Computer Networks 66 (2014) 94–101

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Software defined networking for security enhancement in wireless mobile networks

Aaron Yi Ding [a,b], Jon Crowcroft [b,*], Sasu Tarkoma [a], Hannu Flinck [c]

[a] University of Helsinki, Finland
[b] Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge, United Kingdom
[c] Nokia Solutions and Networks, Finland

ARTICLE INFO

Keywords:
Software defined networking
Security
Wireless mobile networks

ABSTRACT

In recent years we have seen a fast change in the networking industry: leading by the Software Defined Networking (SDN) paradigm that separates the control plane from the data plane to enable programmability and centralized control of the network infrastructure, the SDN design not only simplifies the network management but also accelerates the innovation speed of deploying advanced network applications. Meanwhile, the landscape of the wireless and mobile industry is changing dramatically as well. Given the advance of wireless technologies such as 4G and WiFi offering a pervasive Internet access, the traffic growth from the smartphone-alike devices has placed an increasing strain on the mobile network infrastructure and infringed the profit. Since the demand is increasing together with the growth of mobile users, the incumbent legacy infrastructure is already calling for an upgrade to overcome its existing limitations in terms of network management and security. In this paper, we advocate that the way forward is to integrate SDN and fully utilize its feature to solve the problem. As the security issue has raise serious concern in the networking community recently, we focus on the security aspect and investigate how to enhance the security with SDN for the wireless mobile networks.

1. Introduction

The Software Defined Networking (SDN) is a disruptive and innovative force in the networking industry that affects almost every player including network operators, equipment vendors, Internet service providers and cloud service providers. With SDN, the low-level device configuration and management can be handled by the centralized software controller which facilitates the upgrade of functionality and debugging. By managing and distributing the network state with a system perspective, SDN frees the administrators from mining the complex protocol specifications with agility and flexibility to control the networks. The SDN-enabled Network Functions Virtualization (NFV) also makes it possible for the Internet and cloud service providers to deliver their differentiation advantage in the market through service improvement in terms of Quality of Service (QoS) and security.

Behind the SDN paradigm that separates the control and data plane, SDN delivers four visible features to the networking field:

- Central control and coordination – the logically centralized control model is a key part of the SDN architecture which mitigates the overhead from the traditional distributed mechanisms based on protocols. Although the centralized approach is often questioned for its scalability, it can deliver the state and policy changes more efficiently than the distributed methods in a managed

[*] Corresponding author.
E-mail address: jon.crowcroft@cl.cam.ac.uk (J. Crowcroft).

http://dx.doi.org/10.1016/j.comnet.2014.03.009

domain. The coordination feature also makes it possible that when one of the controllers fails, other standby ones can take over the management tasks to avoid service breakage, which poses a great challenge for the distributed approach.

- Programmability – for both the control plane and the data plane, SDN makes implementation and deployment of the new functionality faster and easier, and hence speeding up the innovation at both hardware and software level. This agility can reduce the cost for service and network providers in terms of Operational Expenditure (OPEX) as the management can be powered by SDN applications in an automatic manner. By avoiding the unnecessary replacement of the underlying hardware through software update, it can also bring down the Capital Expenditure (CAPEX) and facilitate the adoption by the cloud providers.
- Virtualized abstraction – the layered design of SDN hides the complexity of hardware devices from the control plane and SDN applications. Through virtualized abstraction, SDN allows the managed network to be divided into virtual networks that share the same infrastructure but are governed by different policy and security requirements. Such flexibility greatly promotes the sharing, aggregation and management of available resources and enables dynamical reconfiguration and changes of policy.
- Openness – the open standards of SDN such as OpenFlow help build and develop open sourced communities that attract brain power and speed up the innovation. Such openness combined with programming APIs can promote the networking research by allowing researchers to experiment with novel ideas through fast prototyping and testing. It also benefits the interoperability with the legacy infrastructure and allows different operators and providers to collaborate through the SDN framework.

Since SDN allows a granular control of network and services through its abstraction of the underlying hardware, it meets the urgent need from the mobile networks that are going through a fast change to simultaneously operate over multiple wireless technologies (e.g., 4G and WiFi) in order to accommodate the radical growth of data traffic. There are several studies and proposals [1–7] exploring the potential of SDN in wireless mobile networks. As illustrated in Fig. 1 of an envisioned SDN-enabled wireless mobile networks, the current trend of convergence in such networks can benefit from SDN to enhance resource utilization, network management and security in the multi-service and multi-vendor environment.

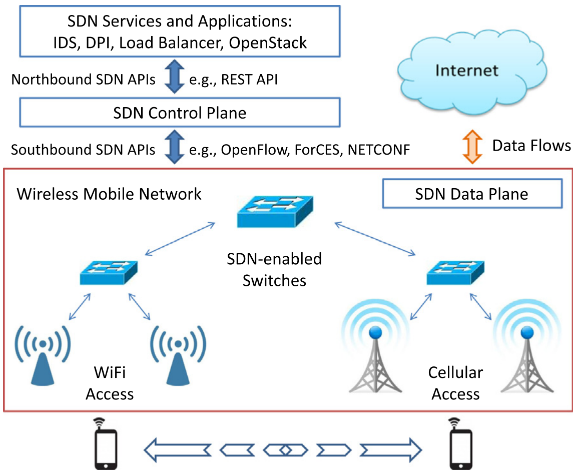

Fig. 1. SDN-enabled wireless mobile networks.

As discussed in [8,15], the security of SDN deserves our special attention for the challenges it brings and also the opportunities to enhance the network security. In this article, we review the recent work on SDN for wireless mobile networks and discuss how SDN solutions can improve security in such a dynamic environment. By surveying the SDN-based security solutions, we identify the design goals and describe our approach of utilizing SDN for security enhancement in wireless mobile networks.

2. SDN for wireless mobile networks

As wireless mobile networks are becoming the major channel to access Internet services, there is an urgent need to keep up with the pace of user growth and the scale of services. For instance, the recent demand of network capacity for mobile data traffic is far exceeding the supply of incumbent networks. At the same time, services also evolve in both variety and complexity. Since operators are limited by the commercial budget and the operation cost, it is extremely hard, if not impossible, to keep up with such speed while still cost-effectively upgrading the infrastructure, delivering service updates, and improving the end user experience under the existing infrastructure.

As highlighted in Table 1, we describe in this section the latest SDN solutions for wireless mobile networks that aim to address the challenges. The range of discussion covers the cellular and the WLAN environment, from the angle of core infrastructure and edge access.

Table 1
SDN solutions for wireless mobile networks.

	WWAN cellular environment	WLAN campus/enterprise environment
Core infrastructure	CellSDN [1]: Cellular SDN architecture design SoftCell [2]: Scalable core network design	OpenRoads [5]: Open wireless infrastructure on campus Odin [6]: Programmable platform for enterprise WLANs
Edge access	SoftRAN [3]: SDN control plane for radio access OpenRadio [4]: Programmable wireless data plane	OpenAPI [7]: Open SDN APIs for access network virtualization OpenRadio [4]: Programmable wireless data plane