II Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software y Salud Electrónica y Móvil
AmITIC 2018
12 al 14 de septiembre de 2018
David, Chiriquí, República de Panamá

Evolución y Contribución para el Internet de las Cosas por las emergentes Redes Definidas por Software

Evolution and Contribution for the Internet of Things by the Emerging Software-defined networking

Carlos Gonzalez [1*], Olivier Flauzac [2], Florent Nolot [3]
[1] *Vicerrectoría de Investigación y Postgrado UNACHI, Panamá,* [2,3]*Université de Reims Champagne-Ardenne, CReSTIC, Francia*
[1]carlos.gonzalez-santamaria@etudiant.univ-reims.fr, [2]olivier.flauzac@univ-reims.f, [3]florent.nolot@univ-reims.fr

RESUMEN– *Las últimas décadas han tenido una enorme evolución de las tecnologías de la computación y la comunicación, lo que ha llevado a un desarrollo y despliegue continúo de las infraestructuras de redes informáticas en términos de dimensión y complejidad. Una de las tecnologías que se ha convertido en una parte integral de la vida cotidiana es el Internet de las Cosas (IoT). Sin embargo, existe un consenso en que las nuevas arquitecturas de redes deberían rediseñarse e implementarse pruebas para mejorar muchos problemas técnicos y mejorar el rendimiento. Hoy en día, con el crecimiento exponencial de dispositivos conectados a Internet, la administración y configuración de la red es uno de los desafíos más difíciles para los administradores de red. En este contexto, con la aparición de las redes definidas por software (SDN) y funciones de redes virtualizadas (NFV) como dos nuevos paradigmas de redes, ofrecen muchas oportunidades para superar estos desafíos, ya que permiten gestionar con flexibilidad, configurar, proteger y optimizar la red recursos usando programas de software dinámicos. Este artículo presenta los aportes de la virtualización de funciones de red y arquitecturas que se pueden utilizar para mejorar el rendimiento basado en el protocolo OpenFlow y SDN, desde una perspectiva IoT.*

Palabras claves– *Administración de redes de computadoras, Internet de las cosas, Openflow, Redes definidas por software, Virtualización*

ABSTRACT– *The last decades have a tremendous evolution of computing and communication technologies, which has led to a continuous development and deployment of computer networks infrastructures in terms of dimension and complexity. A technology which has become an integral part of everyday life is the Internet of Things (IoT). However, there is a consensus that new network architectures should be redesigned and deployed in practice to address many technical issues and improve the network performance. Nowadays, with the exponential growth of devices connected to the internet, managing and configuring the network is one of the hardest challenges for network managers. In this context, with the emergence of software defined networking (SDN) and Network Functions Virtualization (NFV) as new networking paradigms, many opportunities have become available to overcome those challenges since they allow to flexibly manage, configure, secure, and optimize the network resources using dynamic software programs. This paper presents the benefits of network function virtualization and architectures that can be used for enhancing the network performance based on the OpenFlow protocol and SDN, from an IoT perspective.*

Keywords– *Computer network management, Internet of Things, Openflow, Software-defined networking, Virtualization.*

1. Introducción

Con la proliferación actual de dispositivos conectados a Internet, aumenta la complejidad para administrar la seguridad y el despliegue de redes a gran escala. Unas de las más importante las tecnologías emergentes es el Internet de las Cosas o Internet of Things (IoT) [1]. Con la aparición de este nuevo paradigma digital de comunicación, los objetos están programados para monitorear y controlar de forma autónoma muchos aspectos de nuestra vida cotidiana en sectores como el transporte, las ciudades inteligentes, el medio ambiente, la educación, salud, entre otras áreas. Estos dispositivos generan grandes volúmenes de datos, creando una fuerte demanda de gestión de flujo de datos y un nivel de gestión de seguridad difícil de administrar. Debido a la complejidad y la heterogeneidad para el desarrollo de una arquitectura adaptable a este tipo de red, una solución es proporcionada por otra tecnología emergente

denominada Redes definidas por software, *Software-Defined Networking* en inglés (SDN) [2].

En la arquitectura SDN, la función de control de red es separada de la función de plan de transferencia de datos. A su vez, las funciones de control de red pueden ser centralizadas en uno o más controladores de SDN. Este nuevo paradigma cambia por completo la noción del funcionamiento de una red tradicional con equipos y programas proporcionados por un proveedor con sistemas propietarios, lo que hace difícil la innovación y el despliegue de redes gran escala. El SDN permite superar estas limitaciones proporcionando un entorno de código abierto programable y personalizable.

En este artículo se presenta una plataforma de prueba para redes a gran escala incluyendo dispositivos integrados con capacidad de IoT, utilizando técnicas de virtualización de sistemas y SDN.

2. Antecedentes

En los últimos años, la comunidad de científica se ha centrado en investigar dos nuevos paradigmas de redes IoT y SDN. En el punto de partida de esta investigación se realizó un estudio de ambas arquitecturas para comprender su funcionamiento, y así poder describir los aportes de las redes virtualizadas para el IOT. Adicionalmente este trabajo permitió la elaboración de una plataforma de prueba para poder realizar experimentaciones y ver la fiabilidad del sistema.

2.1 Arquitectura de IoT

El desarrollo reciente de una gran cantidad de aplicaciones para el IoT proporciona una amplia gama de oportunidades para crear valor agregado en diversos sectores de la industria y usuarios finales. En una de las estadísticas publicadas por Cisco pronostica que había alrededor de 25 mil millones de objetos conectados en todo el mundo en 2015, y este número de objetos puede duplicarse para el año 2020 [3]. Además, se proyecta unos 6,5 dispositivos *per-capita* conectado y aproximadamente 49 *exabytes* de tráfico de datos por mes superando de esta manera la mitad de 1 *zettabyte* anual.

Actualmente no hay consenso sobre un solo modelo de arquitectura referencial aplicable para todo el IoT. Existen diferentes modelos en curso de desarrollo, como lo son NIST para Smart Grid, ITU-T, M2M para ETSI o el modelo de referencia arquitectural para la Unión Europea, el proyecto IoT-A, entre otros modelos IETF, W3C, etc. La estandarización de una arquitectura para el IoT va a evolucionar a través del tiempo con diversas contribuciones e ideas, como fue desarrollado el Internet.

La arquitectura IoT más comúnmente utilizada para definir la idea principal consta de tres capas: capa de percepción, capa de red y capa de aplicación [4].

- Capa de percepción: esta capa consiste en objetos físicos y sensores. La tarea principal de la capa de percepción es recopilar datos e identificar objetos utilizando diferentes dispositivos como tarjetas inteligentes, RFID y redes de sensores.
- Capa de red: esta capa también se denomina capa de transporte, que al mismo tiempo es responsable de transmitir los datos a la capa de percepción y a la capa de aplicación. Para garantizar la transferencia de datos, la capa de red utiliza diferentes tipos de tecnologías y protocolos, por ejemplo, 2G, 3G, bluetooth, zigbee, gateway, ad-hoc, red inalámbrica/cableada o infrarroja, entre otros.
- Capa de aplicación: la capa de aplicación permite la interacción directa con los usuarios finales. Las aplicaciones se pueden implementar para diferentes tipos de servicios e industrias, por ejemplo: domótica, ciudades inteligentes, logística, comercio, medio ambiente, seguridad pública, salud. En esta capa, todas las decisiones de control, seguridad y administración de aplicaciones se realizan a este nivel.

2.2 Arquitectura de SDN

En redes tradicionales, el plan de control y el plan de datos es gestionado de manera individual en cada dispositivo de interconexión de red (enrutador o conmutadores). El proceso de despliegue de nuevos protocolos y políticas de seguridad individualmente puede resultar extenso y complejo debido a sistemas propietarios cerrados. La arquitectura de SDN simplifica la administración de la seguridad y la gestión de redes al separar el plan de control del plan de datos.

El plan de control es centralizado incluyendo todas las funciones de administración en un nodo externo denominado controlador de SDN. El plan de datos gestiona la transferencia de paquetes desde equipos de red tales como conmutadores y enrutadores a través de tablas de enrutamiento, con las decisiones que recibe desde el plan de control.

La arquitectura SDN, como muestra en la Fig. 1, está compuesta de tres capas: capa de aplicación (Application layer), capa de control (Control layer) y capa de infraestructura (Infrastructure layer).

- La capa de aplicación es constituida por un conjunto de aplicaciones que comunican sus requisitos de red a la capa de control SDN.
- La capa de control consiste en uno o un grupo de dos o más controladores SDN que coordinan las políticas de administración, así como la comunicación con las otras capas de la arquitectura de SDN usando interfaces y protocolos específicos.
- En la capa infraestructura se incorporan los equipos de red y si implementan algunas decisiones de transferencia de datos para reenviar el tráfico o procesarlo.

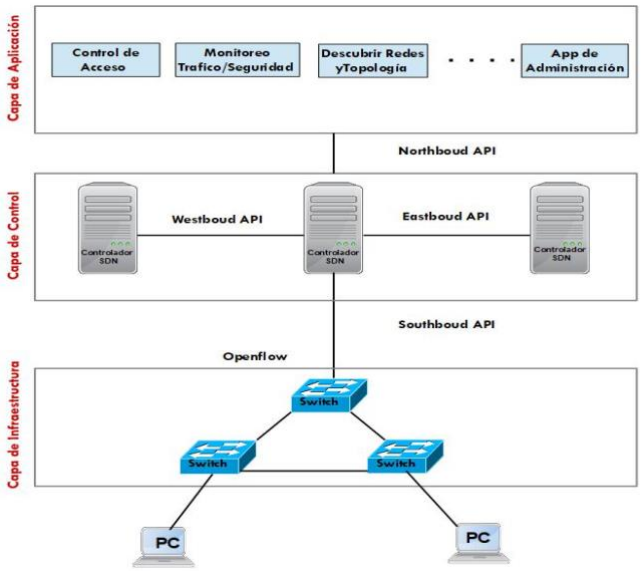

Figura 1. Arquitectura SDN.

El protocolo más utilizado para la comunicación entre los equipos de red y el controlador SDN es OpenFlow [2]. OpenFlow está estandarizado por Open Networking Foundation y es adoptado por muchos proveedores equipos de red con capacidad SDN. Además, este protocolo permite a través del controlador la administración y configuración de manera remota de los conmutadores, con el fin de leer los estados cada dispositivo de red, recopilar la información y estadísticas.

3. Beneficios de SDN para el IoT

El desarrollo de las nuevas tecnologías emergentes como lo es el IoT y los ambientes inteligentes requieren de infraestructuras de redes que pueden soportar la administración grandes niveles de escalabilidad, tráfico de datos, movilidad y amenazas de seguridad. La continua evolución y el crecimiento de Internet representa un enorme desafío para los desarrolladores y las compañías de telecomunicaciones. Una solución alternativa para solventar este gran desafío es presentada por otra tecnología emergente como el SDN. Los beneficios de SDN para administrar el IoT se describen a continuación.

- La ***centralización*** de la información en el controlador SDN provee una visión global completa de la red, habilitando la automatización a través de la interfaz de programación de aplicaciones (API) y un control continuo de demandas masivas de conexión. Esta centralización simplifica la administración a gran escala de dispositivos IoT.
- La ***flexibilidad*** de administrar el almacenamiento de datos para analizar, procesar y para maximizar continuamente el rendimiento del flujo de la información entre dispositivos IoT. Los entornos de IoT están compuesto por diversos tipos de dispositivos finales en el cual toda la información generada puede ser tratada localmente utilizando la computación en los bordes evitando el congestionamiento del tráfico de red. Como resultado, la administración de la red puede ser incluso más crítica con el uso de los entornos de aplicaciones y protocolos actuales. La capacidad de configuración flexible de SDN, permite cambiar dinámicamente el comportamiento de la red en función de los patrones de tráfico, los incidentes detectados y los cambios de políticas de seguridad sobre todos los dispositivos conectados en un entorno de IoT.
- Debido al gran número dispositivos IoT conectados requieren de infraestructuras de redes capaces de soportar la ***Escalabilidad.*** Desde un punto centralizado, con SDN es posible crear una automatización de sistema con protocolos que permitan una gestión macro de los flujos de datos. También se puede predefinir las políticas de comunicación y seguridad para los dispositivos que se conecten a la red, e incluso definir estas políticas antes de la solicitud de conectividad, lo que básicamente permite una administración dinámica sin tener en cuenta los

nuevos dispositivos conectados. SDN permite incluir una escalabilidad inherente debido a su concepción centralizada para la administración de aplicaciones y protocolos el cual permite dar respuesta a expansiones de redes escalables según sea necesario.

- Con la ***abstracción*** de equipos de redes tales como conmutadores, enrutadores y dispositivos intermediarios permite una reducción de costo importante. Estos equipos en redes tradicionales utilizan sistemas propietarios programados con reglas específicas y protocolos complejos de establecer en tiempo real. Por lo tanto, la configuración de políticas adecuadas para cumplir con los requisitos específicos de aplicaciones IoT es un desafío que puede ser solucionado aplicando las redes definidas por software.
- La arquitectura de SDN permite una ***Programabilidad*** completa de todos los dispositivos conectados en una infraestructura debido a la visión global de la red. SDN ofrece la oportunidad de desarrollar nuevas funcionabilidades y aplicaciones de red sin la necesidad de configurar individualmente cada dispositivo o esperar que los fabricantes de equipos de red las desarrollen. Esto permite una adaptación dinámica a cambios en topologías de redes, daño material de equipos, configuraciones dinámicas e implementación múltiples políticas de redes ideales para entornos IoT.

Actualmente los diversos escenarios de pruebas que permitan la utilización de SDN para el IoT están aún en desarrollo. Sin embargo, existen herramientas y protocolos adaptables en ambientes de pruebas que pueden ser utilizados para analizar la funcionabilidad y adaptabilidad de ambas tecnologías.

4. Plataformas de pruebas para SDN

Los prototipos y las plataformas de prueba tienen una gran importancia para la validación de una investigación. Es importante realizar experimentos en un entorno real o similar al de producción. Para realizar estos experimentos se debe tener en cuenta muchos factores, como lo es el costo, el tamaño y la flexibilidad para elaborar la plataforma. Actualmente existen herramientas como Ns2 y Opnet [5], proporcionando una alternativa para realizar experimentos de redes. Sin embargo, estas herramientas no ofrecen escalabilidad y adaptabilidad a posibles escenarios prácticos realistas. Con la aparición de las nuevas técnicas de virtualización, aislamiento y segmentación, permiten la construcción de entornos de prueba flexibles y personalizables.

Motivados por la idea de realizar experimentos en una red de producción, los investigadores de la Universidad de Stanford propusieron un *test bed* denominado OpenRoads [6]. El prototipo elaborado permite a los investigadores utilizar esta plataforma de pruebas de manera simultánea para sus experimentos y para que los estudiantes creen sus propios controladores SDN inalámbricos. La red consta de 30 puntos de acceso WiFi y estaciones base WiMAX. Una de las funcionalidades incluida es FlowVisor, el cual permite separar y enviar la información específica a cada uno de los dispositivos interconecten las redes inalámbricas.

Mininet [7], es otra herramienta que permite realizar prueba de redes a pequeña escala. Su entorno de diseño de topologías y sus configuraciones proporciona una interfaz de redes programables bastante realista. Mininet permite crear redes SDN interactivas y personalizables que pueden compartirse una vez se ha desarrollado el prototipo. Pero debido a su enfoque de virtualización liviano, Mininet no puede soportar múltiples kernels sistemas operativos simultáneamente y no ofrece el mismo rendimiento para la transferencia de datos que un sistema de hardware real.

Para superar el impedimento de establecer topologías virtuales por sectores independientemente de la infraestructura física el cual es considerada una limitación de FlowVisor [8], se ha desarrollado un nuevo componente denominado *ViRtual TopologIes Generalization in OpenFlow* (VeRTIGO) [9]. Este nuevo componente de redes es una extensión de FlowVisor, que permitir elaborar instancias de redes virtuales y mejorar el nivel de abstracción de la capa de virtualización de red a través de la separación de los conmutadores. Además, VeRTIGO ha sido implementado en el proyecto OFELIA [8], otro entorno experimental para diseñar y hacer pruebas de redes SDN, demostrando su eficacia y flexibilidad en entornos de redes reales y a gran escala.

OpenGUFI [10], es una plataforma de pruebas SDN el cual provee una interfaz gráfica de usuario. Esta plataforma permite visualizar la topología de red, las asociaciones entre los clientes móviles y el tráfico de los

puntos de acceso inalámbrico en tiempo real. Basado en ODIN (*Open Data Center with an Interoperable Network)*, una plataforma SDN para redes WLAN empresariales, con un control sobre los clientes móviles conectados y los equipos de red a través del controlador SDN.

En [11], presentamos una arquitectura en clúster de controladores SDN para comprobar la escalabilidad y el rendimiento de OpenDaylight. Uno de los principales inconvenientes de SDN es la centralización del plan de control. Es por esta razón, que es necesario la clusterización de controladores SDN para evitar potenciales ataques como la denegación de servicio (DoS) o daños materiales en alguno de los nodos. Las técnicas utilizadas actualmente para realizar clúster de controladores SDN no son las adecuadas para soportar la nueva generación de internet como lo es el IoT. Una solución para solventar este desafío es la utilización de un protocolo de comunicación intra-cluster en la arquitectura SDN.

5. Diseño de una plataforma SDN-IoT

Luego de analizar las diferentes plataformas y herramientas que existen actualmente, ninguna se puede adaptar a un escenario realista de experimentación SDN-IoT. Es por este motivo que se diseñó una plataforma de pruebas en un ambiente virtualizado, el cual permite crear flujo de datos entre dispositivos, monitorear las peticiones enviadas al controlador SDN, decidir las políticas y reglas de seguridad sobre cada dispositivo conectado a la red. La plataforma desarrollada consiste en una red externa para la administración remota de cada servidor y una red interna para el flujo de comunicación solo OpenFlow. Esta plataforma cuenta con 5 servidores Linux, 1 servidor para la instalación del controlador SDN y 4 servidores para la virtualización de los dispositivos finales con capacidad de IoT.

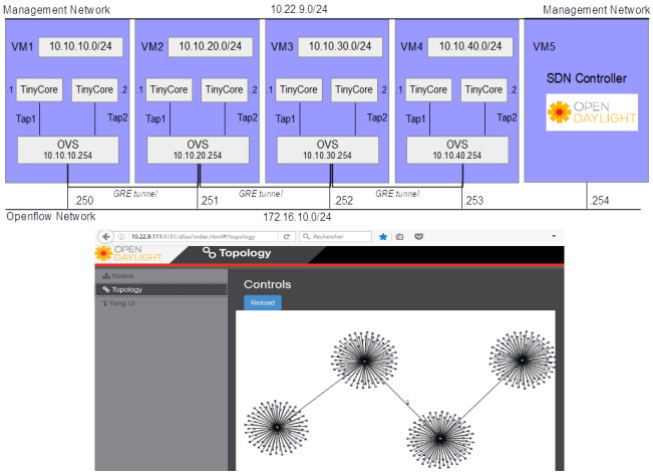

Figura 2. Diseño de la plataforma de prueba.

La gestión de la infraestructura es realizada en un ambiente de computación en nube, basado en VMware vSphere. Por medio de este software se puede administrar, instalar y configurar, múltiples máquinas virtuales simultáneamente en un solo servidor. La emulación de la arquitectura de un dispositivo con capacidad IoT, se realiza con el software de código abierto qemu. Este emulador permite adaptar según requerimiento el tipo de procesador, interfaces de redes, disco duro, la memoria RAM entre otros. El sistema operativo para cada uno de los dispositivos IoT conectados consiste en sistemas Linux basados en TinyOS. Existen otros sistemas operativos para simular dispositivos con recursos limitados tales como, Contiki, RIoT, LiteOS entre otros. TinyOS contiene diversas funcionabilidades diseñadas para permitir la escalabilidad e integridad en una arquitectura IoT.

La plataforma de prueba SDN está constituida por herramientas de código abierto como el controlador SDN OpenDaylight (ODL) y conmutadores Open vSwitch (OVS). El proyecto ODL tiene el soporte de la fundación Linux, así como de los más importantes desarrolladores de Internet. El canal de comunicación entre el controlador y los conmutadores OVS se realiza a través del protocolo OpenFlow. Las funciones de control y las decisiones de transferencia de datos son gestionadas mediante table de flujos organizadas por OpenFlow. El controlador ODL tiene integrado un complemento de tipo *plug-in* que permite la automatización del flujo de datos para el proceso de conmutación en IPv4. No obstante, el

proceso de enrutamiento es más complejo para lograr una escalabilidad óptima. Para ello es necesario tener un amplio conocimiento en el funcionamiento de tabla de flujos incluyendo segmentación de instrucciones con OpenFlow, como también programación en Python, C o Shell scripting que permitan la automatización de redes escalables SDN.

En la evaluación del escenario experimental se pudo constatar el buen rendimiento de OpenFlow para la administración de redes escalables. Este caso de uso se utilizó OpenFlow 1.3 ya que la última versión 1.5 no está adaptada al controlador ODL. Una observación importante es que OpenFlow no dispone de los mecanismos adecuados para agregar políticas de seguridad a nivel de aplicación. Solo permite administrar la transferencia de datos y flujo de comunicación entre dispositivos. Una vez las reglas de flujo de datos son establecidas por el controlador, todos los procesos de conmutación y enrutamiento se realizan a nivel del OVS. Esto expone vulnerabilidad en todo el sistema, por ello es importante desarrollar una estrategia que permita la comunicación hasta el nivel aplicativo entre OpenFlow y otros protocolos como Opflex, Group Based Plociy (GBP) o mecanismos de seguridad de redes en el controlador.

Una experimentación trascendental con arquitecturas SDN es la organización en clúster. El uso de clúster permite limitar el número de dispositivos conectados en una zona, reduciendo la cantidad de información a administrar. El intercambio de información entre clúster se realiza a través de la interconexión de controladores SDN. Dentro de la plataforma desarrollada efectuar simulaciones con más de 1,000 dispositivos conectados al mismo tiempo.

6. Conclusiones

En este artículo presenta los principales aportes que brinda la virtualización de redes para el IoT. El número de dispositivos con conectividad heterogénea aumenta cada día, por lo que es necesario crear arquitecturas de redes orientadas hacia la nueva generación de Internet. SDN ofrece un alto grado de escalabilidad, dependabilidad, seguridad y rendimiento. La centralización de la inteligencia de la red en el controlador SDN permite el control, la configuración y la administración de redes complejas de una manera más eficiente.

Referencias

[1] S. Li, L. D. Xu, and S. Zhao. “The internet of things: A survey, Information Systems Frontiers.” vol. 17, pp. 243-259, Apr. 2015.

[2] Open Networking Foundation. “Software-Defined Networking: The New Norm for Networks", White Paper, [Online]. https://www.opennetworking.org/images/stories/downloads /sdn-resources/white-papers/wp-sdn-newnorm.pdf, [Apr. 2011].

[3] D. Evans, “The internet of things: How the next evolution of the internet is changing Everything.” White Paper, [Online]. http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, [Apr. 2011].

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu. “Security of the internet of things: Perspectives and challenges.” Wireless Network, vol. 20, pp. 2481-2501, Nov. 2014.

[5] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar. “An integrated experimental environment for distributed systems and networks.” SIGOPS Syst. Rev., vol. 36, pp. 255-270, Dec. 2002.

[6] K.-K. Yap, M. Kobayashi, D. Underhill, S. Seetharaman, P. Kazemian, and N. McKeown. “The stanford openroads deployment.” in Proceedings of the 4th ACM International Workshop on Experimental Evaluation and Characterization, WINTECH '09, (New York, NY, USA), pp. 59-66, ACM, 2009.

[7] B. Lantz, B. Heller, and N. McKeown. “A network in a laptop: Rapid prototyping for software-defined networks.” in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Hotnets-IX, (New York, NY, USA), pp. 19:1-19:6, ACM, 2010.

[8] M. Gerola, R. D. Corin, R. R. F. D. Pellegrini, E. Salvadori, H. Woesner, T. Rothe, M. Sune, and L. Bergesio. “Demonstrating inter-testbed network virtualization in ofelia sdn experimental facility.” in 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 39-40, April 2013.

[9] R. Doriguzzi Corin, M. Gerola, R. Riggio, F. De Pellegrini, and E. Salvadori. “Vertigo: Network virtualization and beyond.” in Software Defined Networking (EWSDN).” 2012 European Workshop on, pp. 24-29, Oct 2012.

[10] J. Schultz, R. Szczepanski, K. Haensge, M. Maruschke, N. Bayer, and H. Einsiedler. “Opengufi: An extensible graphical user flow interface for an sdn-enabled wireless Testbed.” Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, pp. 770-776, Oct 2015.