Demo: Programming Enterprise WLANs with Odin

Lalith Suresh
INESC-ID/Instituto Superior Tecnico
Lisbon, Portugal
lalith.puthalath@ist.utl.pt

Julius Schulz-Zander
Telekom Innovation Laboratories/TU Berlin
Berlin, Germany
julius@net.t-labs.tu-berlin.de

Ruben Merz
Telekom Innovation Laboratories/TU Berlin
Berlin, Germany
ruben.merz@telekom.de

Anja Feldmann
Telekom Innovation Laboratories/TU Berlin
Berlin, Germany
anja@net.t-labs.tu-berlin.de

ABSTRACT

We present a demo of Odin, an SDN framework to program enterprise wireless local area networks (WLANs). Enterprise WLANs need to support a wide range of services and functionalities. This includes authentication, authorization and accounting, policy, mobility and interference management, and load balancing. WLANs also exhibit unique challenges. In particular, access point (AP) association decisions are not made by the infrastructure, but by clients. In addition, the association state machine combined with the broadcast nature of the wireless medium requires keeping track of a large amount of state changes. To this end, Odin builds on a light virtual AP abstraction that greatly simplifies client management. Odin does not require any client side modifications and its design supports WPA2 Enterprise. With Odin, a network operator can implement enterprise WLAN services as network applications.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Network communications; C.2.1 [**Network Architecture and Design**]: Wireless communication; C.2.3 [**Network Operations**]: Network management

Keywords

Odin, SDN, Enterprise WLANs

1. INTRODUCTION

Deployments of modern IEEE 802.11 [1] enterprise wireless local area networks (WLANs) serve today a multitude of client devices such as smart-phones, laptops or tablets. Large deployments provide resilience, fault-tolerance and fail-over capabilities. Scalability in this context is paramount. Independent of the size, what most enterprise WLAN deployments have in common is the support for features such as authentication, authorization and accounting (AAA), policy management, mobility management, interference management with dynamic channel reconfigurations, load balancing and providing QoS guarantees. Their management is usually centralized. These systems are also proprietary, with each vendor offering its own closed-source platform.

In this paper, we demonstrate Odin[1], a software defined networking (SDN) framework for enterprise WLANs. The objective of Odin is to empower network operators to program and deploy typical enterprise WLAN services and features as network applications. In this context, WLANs exhibit specific challenges. The 802.11 standard lets clients make AP association decisions on the basis of locally made decisions. The infrastructure has no control over these decisions made by the client. In addition, the association state machine at the AP, combined with the dynamic, broadcast and time-varying nature of the wireless medium can require to keep track of state information changes continuously. Furthermore, not only associated, but also all interfering 802.11 devices need to be taken into account.

To effectively express applications that implement high-level services in enterprise WLANs, the programmer needs simple and powerful abstractions. This is essential if the programmer operates on a central view of the entire network. Hence, a design goal of Odin is to prevent the programmer from keeping track of changes to the authorizer, authenticator and client state machine. Indeed, the programmer cannot make assumptions about the endpoints of the link between the client and the infrastructure (MAC and IP address). To shield the programmer from this burden and to simplify the programming model, a central component of Odin, is the light virtual access point (LVAP) abstraction. LVAPs virtualize association state and separate them from the physical AP. Multiple clients connected to a single physical AP are treated as a set of logically isolated clients connected to different ports of a switch. The LVAP abstraction enables Odin to offer a straighforward programming model. Typically, an application running on Odin does not need to directly handle the association state. But LVAPs also greatly facilitate mobility management, allowing for the infrastructure to handoff clients without triggering the client's re-association mechanism.

[1]Odin is a major god in Norse mythology.

SIGCOMM'12, August 13–17, 2012, Helsinki, Finland.
ACM 978-1-4503-1419-0/12/08.

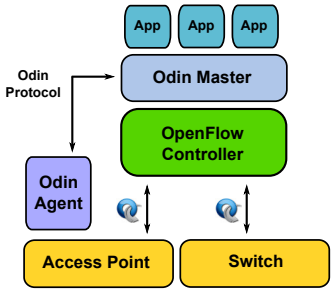

Figure 1: Architecture of Odin. The Odin Master (an OpenFlow application), speaks OpenFlow to the switches and the APs, and uses a custom protocol to talk to each Odin Agent running on APs. Odin applications use Odin's primitives to implement enterprise specific services.

Odin is work in progress, under heavy development and operates under the following assumptions: It targets fully centralized and reasonably sized deployments with one controller. It does not expect any client side modifications and supports WPA2 Enterprise by design. It is fully transparent to clients, which connect to it as regular IEEE 802.11 stations in infrastructure mode.

2. ODIN: AN SDN FRAMEWORK FOR ENTERPRISE WLANS

2.1 Architecture of Odin

Odin's architecture consists of a single master, multiple agents and a set of applications (Figure 1). The master itself is an application on top of an OpenFlow [2] controller. It has a global view of flows in the network, clients connected to the network, and the infrastructure that comprises the network. Odin agents run on the APs. Together, the master and agents implement a Wi-Fi split-MAC.

2.2 Light Virtual AP (LVAP)

LVAPs are a central primitive within the Odin framework. When Wi-Fi clients in managed mode scan APs, probe request messages are generated. APs responding with probe response messages become potential association candidates. A client then proceeds to perform a connection handshake with a locally selected AP. The LVAP abstraction enables to take control on association decisions from client and leads to a logical isolation of clients with respect to the 802.11 MAC. With LVAPs, every client receives a unique BSSID to connect to, i.e, every client is given the illusion of owning its own AP. In Odin, the LVAP is the client specific AP. Each *physical* AP hosts an LVAP for each connected client. Removing a client LVAP from a physical AP and spawning it on another achieves the effect of handing off a client without the client performing a re-association, generating additional layer 2 or 3 messages, and most importantly, without requiring any special software or hardware at the client. Thus, Odin always provides clients a consistent link to the network, and the programmer of an Odin application needs not be concerned with *how* the client's link to the network changes. The end-point of a link always corresponds to the client's IP and MAC addresses and the unique BSSID assigned by Odin.

3. DEMO PLAN

The demo setup will comprise three APs connected via a switch to a laptop. The APs are x86 based Alix 3D2 boards running OpenWrt with Wistron DNMA92 802.11n interfaces (Atheros AR9220 chipset). Each AP runs an Odin agent and the laptop runs the Odin master with a set of Odin applications. In addition, the laptop will run necessary services for the demo. Namely, a visualization interface and, depending on the local availability, an upstream connectivity through NAT.

Our demo of Odin will display various aspects of a typical enterprise system.

- A complete Odin deployment with WPA support where demo attendees can use their own devices as clients.
- Using a visualization interface, we will demonstrate the inner working of the LVAP concept. It will show at which physical AP each client is associated by means of LVAPs. In addition, the visualization interface will display the various statistics that are collected by the measurement collection component of Odin. For instance, the received signal strength of different clients as observed at the APs, the noise, and data rates.
- We will demonstrate various Odin applications. In particular, the mobility manager and the load balancer.
- Demonstration of network slicing based on policies, such as separation of a guest WiFi network, isolation of malicious nodes or traffic restrictions.
- Demonstrate connection restorations in light of AP failures using LVAP migrations.
- In order to show the ease with which Odin applications can be written, we will provide another laptop to let demo attendees program their own Odin applications. We will support them and help them to run their application on our Odin deployment.

4. SUMMARY

There is a large body of work on enterprise WLAN architectures and system, see for instance [3, 4] and the references therein. For Odin, these works contain typical applications that we expect to eventually support.

5. REFERENCES

[1] *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, 2007.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38:69–74, March 2008.

[3] V. Shrivastava, N. Ahmed, S. Rayanchu, S. Banerjee, S. Keshav, K. Papagiannaki, and A. Mishra. CENTAUR: realizing the full potential of centralized wlans through a hybrid data path. In *ACM Mobicom 09*, 2009.

[4] R. Murty, J. Padhye, A. Wolman, and M. Welsh. Dyson: an architecture for extensible wireless LANs. In *USENIX ATC 10*, 2010.