SDN for Dense Home Networks

Yiannis Yiakoumis Manu Bansal Sachin Katti Nick McKeown
Stanford University

A large part of the population lives in high-density areas. Only in the US, 27 million households (24%) are located in multi-apartment buildings sharing resources with neighboring home networks. It's expected to see ~25 listed APs in an urban area, and such high density can be a bad indicator for network performance. Despite advancements in WiFi rates over the years, users often experience poor performance, deviating from what protocols promise. High interference and congested channels is commonplace, while misconfiguration often leads to poor channel and power allocation. Even though a plethora of access points are available, users can access only theirs, occasionally leading to poor coverage which in turn degrades the channel for everyone. A number of factors contribute to this: lack of coordination between individual homes, no expertise from users, and poor manageability of WiFi itself.

In this paper, we present an SDN framework for designing a dense WiFi network which aims to provide users with a **personalized, fast and reliable network service**.

Design Principles. We identify three main properties to characterize the design of a WiFi network: i) density and spatial deployment of APs, ii) infrastructure configuration (e.g. channel and power allocation, and iii) network access. For example, in an apartment building, each user chaotically deploys and configures his own AP, which serves all his traffic. On the other end, the network for a university dorm is typically deployed by an IT team which configures all the infrastructure providing an enterprise-like environment. Users (and their devices) choose which AP to connect to, through a complex and driver-specific process (and using a number of criteria such as channel load, SNR, previous history etc).

For our architecture, we make the following decisions :

- **Personal network abstraction:** Each user can configure and customize his own network service (e.g. define SSID name and password, prioritize traffic, add devices). This personal network may follow the user wherever he goes within the same administrative domain (within the building, at a coffee-shop, or on an ISP-wide infrastructure).
- **Sufficient infrastructure control:** To improve performance we require sufficient visibility and control to the infrastructure from a global perspective. This includes configuration control (channel-power allocation, WiFi properties), as well as access control (which client connects to which AP at what channel).
- **Overprovisioned physical infrastructure:** To provide users with fast and reliable service, we want an infrastructure with high enough density to to ensure good coverage throughout the spectrum and sufficient redundancy. As planning a wireless network is notoriously hard, we suggest overprovisioning the deployment and decoupling it from the actual operation. APs which are not necessary to serve the active set of clients can be dynamically "turned-off" to avoid unnecessary interference and overhead.

Comparing these decisions to our original goal, one can observe a clear division of labor between users and the infrastructure: users should only deal with *personalizing* their network service, and let the infrastructure do the rest, i.e. ensuring that this service is *fast and reliable*.

Today's WiFi home networks fall short to meet these requirements. Users' policies are statically integrated into a physical AP, and they include both high-level policies and low-level wireless configuration (e.g. channel, power). When the infrastructure is open and accessible, users (and their devices) decide where to connect to, while the operator maintains very little control over the final state of the network. This becomes worse with increased density, as it introduces higher overhead (e.g. beacons) and less predictability.

WiFi Virtualization. To overcome these limitations, we suggest WiFi virtualization as a mechanism to decouple infrastructure control and user customization. On a virtualized architecture each user sees only his personal AP that follows him everywhere. Besides traditional AP characteristics (SSID, encryption, etc) a user can define additional primitives enforced elsewhere in the network (e.g. traffic prioritization, tunneling). By managing the mapping of personal APs to the underlying physical infrastructure, we can enforce a variety of strategies to improve the performance of our network. For instance, capable clients can be directed to the 5GHz band to make more efficient use of the available spectrum. Older devices can be limited to one channel, allowing the rest of the spectrum to run on a green-field mode, without the need for slow-rates and other inefficiencies for backwards-compatibility. Personal APs can be dynamically moved across the infrastructure to ensure that clients always experience a sufficiently good SNR; and only the necessary number of physical APs can remain active to keep interference and contention low.

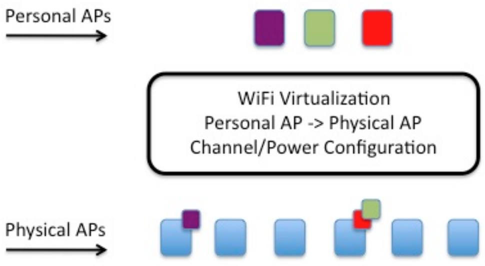

Figure 1: Virtualized WiFi architecture. Each user configures and access his own personal network. The network controller configures the APs, and based on its strategy maps personal APs to the physical infrastructure to optimize performance.

Implementation and Deployment. To test and evaluate our ideas, we are building BeHop, a dense WiFi network at a Stanford dorm. We develop a prototype AP using commodity hardware and software (NetGear AP, OpenWRT, OpenVSwitch) and our own SDN WiFi extensions. Using our AP and SDN controller, we can programmatically configure channel and power, add/remove clients, and handle WiFi management packets for discovery, authentication and association from a centralized controller. Ongoing work includes scaling our deployment, iterating over useful abstractions for admission control, channel selection, and client monitoring, and experimenting with different policies for improving network performance and customizing users' experience.

Related Work. The chaotic nature of home networks was first studied at [3], suggesting self-management techniques for power allocation and rate control. We assume that the physical infrastructure is under the same administrative domain (e.g. an ISP or building owner) and look at coordination instead of stand-alone methods. Getting control over the AP-client association graph has been the focus of recent work on enterprise networks, both in industry and academia [4, 1, 2]. Our work is targeted towards home deployments, taking into account the chaotic and dense nature of deployed APs as well as user-defined policies.

References

[1] CAPWAP RFC. http://tools.ietf.org/html/rfc5415.

[2] Meru Networks Whitepaper. http://www.merunetworks.com/collateral/white-papers/2012-wp-wireless-lan-virtualization-twice-the-network-at-half-the-cost.pdf.pdf.

[3] Aditya Akella, Glenn Judd, Srinivasan Seshan, and Peter Steenkiste. Self-management in chaotic wireless deployments. *Wireless Networks*, 13(6):737–755, 2007.

[4] Lalith Suresh, Julius Schulz-Zander, Ruben Merz, Anja Feldmann, and Teresa Vazao. Towards programmable enterprise WLANs with Odin. In *Proceedings of the first workshop on Hot topics in software defined networks*, pages 115–120. ACM, 2012.