A New Perspective on Wireless Network Architecture for Mobility and Internet of Things
A White Paper for Future Wireless Cities Workshop

Kuang-Ching Wang, Clemson University

The world today already sees a complex landscape of wireless network systems – cellular networks, wireless LANs, sensor networks, short range radios (DSRC, Bluetooth), etc. Wireless network technologies have clearly gone a long way. IEEE 802.11 (Wi-Fi), for example, had nearly two decades (since 1997) of innovation leading to its current state. Cellular technologies have an even longer history. These technologies together have already supported a rich range of applications for a really large world population today. Nevertheless, with the explosive growth of new wireless needs (e.g., smart devices, connected vehicles, Internet of Things), there is real concern that today's architecture will be unable to sustain their needs.

The top challenges are due to increasing number of wireless endpoints, mobility as a norm for many of them, and increasingly diverse and stringent security and performance requirements. The existing network architecture presents too much friction and too rigid topology and service constraints. Devices undergo non-trivial authentication and access control to obtain network access, often disruptive and via few contractual options. Once connection is established, the network imposes relatively few but rigid and hard-to-change application-specific limtis .

Connected vehicles and Internet of Things are probably two major emerging applications that depend critically on wireless connectivity. Connected vehicles today are typically connecting via a single provider network (including this provider's roaming partners via corporate-level roaming agreements and complex infrastructure for roaming authentication/authorization/accounting (AAA). Deploying Internet of Things (IoT) today is a difficult undertaking – operators must either impose rigid requirements on the network configuration, or impose per device security requirements (driving costs of such devices as smart power meters way high), or restrict devices to not communicate sensitive information. For connections requiring firewalls or VPN gateways, the physical deployment of these appliances restricts the scope, topology, and performance of such services. With discussions of the emerging application driven customization opportunities with software defined infrastructure, the problem is quickly getting beyond manageable.

A new perspective different from contemporary wisdom might shed light on new directions. If friction is the key inhibitor, how about let us begin with removing it. What if all devices are by default accepted to connect to any networks? Foregoing restriction at the lowest layer does not mean losing control. Instead, control can be enforced by services, via *network function virtualization (NFV)* or *virtualized services* over physical appliances, flexibly enacted in the network. With NFV, firewalls, VPN gateways, load balancers, etc. can be deployed as virtual machines anywhere in a network or multiple federated networks. The flexibility implies that either operators or applications can instantiate customized services without topology constraints. Since network connectivity is no longer the choke point, software driven customization of performance and security will have a wider degree of freedom. Control of AAA and deterrence of malicious/unlawful traffic is not lost; instead, NFV allows agility, elastic scalability, and flexibility with more intelligent and novel methods. Essentially, we take away global friction and enable customized properties.

Kuang-Ching (KC) Wang as PI for a series of NSF projects (GENI OpenFlow, GENI WiMAX, GENI Cinema, EAGER on "Mobile Gigabit Wireless Access", CC-NIE, and NSFCloud) has led the Clemson team to deploy GENI SDI on campus and conduct experiments stitching compute and network elements over national and international topologies. Wang holds the joint position as Networking CTO for Clemson IT to advise campus strategies in this era of change. Wang has worked with Stanford ON.Lab and Big Switch Networks during his recent sabbatical developing SDN solutions.