VPMN – Virtual Private Mobile Network Towards Mobility-as-a-Service

Arati Baliga*, Xu Chen†, Baris Coskun*, Gustavo de los Reyes*,
Seungjoon Lee†, Suhas Mathur*, Jacobus E. Van der Merwe†
*AT&T Security Research Center †AT&T Labs - Research
arati.baliga@att.com,chenxu@att.com,baris@att.com,gdelosreyes@att.com,
slee@att.com,suhas@att.com,kobus@att.com

ABSTRACT

In this paper we present our vision for a mobile network infrastructure that embraces advances in virtualization to dynamically create private, resource isolated, customizable, end-to-end mobile networks. We describe an architecture for such a virtual private mobile network (VPMN) infrastructure and present a number of use cases that illustrate the requirements and trade-offs to consider in their realization and the benefits that can be achieved.

Categories and Subject Descriptors

C.2.1 [**Computer-Communications Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Design

Keywords

Virtual Private Mobile Network

1. INTRODUCTION

In this paper, we propose the use of the physical infrastructure comprising a mobile wireless network as a platform that offers *mobility as a service*, much in the same way that servers in a data center offer computing as a service. By applying the principle of virtualization to a mobile wireless network, the owner of a mobile network can open up the network's building blocks, to be controlled, operated, and optimized by other entities, thereby de-linking the physical infrastructure from the services that run on top of it, and hence potentially enabling new types of services.

Server virtualization technologies have enabled and fueled the creation and growth of cloud computing. Cloud computing in turn has radically changed the way data centers are managed and operated, and in fact the way business and casual users alike perceive and interact with compute and storage resources. Specifically, with Infrastructure-as-a-Service cloud abstractions, compute resources can be instantiated on-demand from a seemingly unlimited pool of resources, and can be given "personalities" (e.g., web, database, etc.) depending on the function they are to fulfill. These can then be plumbed together to realize multi-tier compute stacks, or indeed clusters of compute resources targeting data-intensive and compute-intensive workloads. In a nutshell, the effect of cloud technologies has been to liberate compute resources from sets of special purpose components to a flexible pool of resources that are operated in a highly automated fashion and whose function is determined on-demand depending on workload requirements.

Virtualization and its close cousin, resource partitioning, are similarly heavily used in network infrastructures. In enterprise and data center networks, virtual local area network (VLAN) technology is commonplace and continues to evolve. In backbone networks, virtualization in the form of different protocol families utilizing a single multiprotocol label switching (MPLS) core network, virtual private networks (both layer-2 and layer-3) and tunneling technologies (*e.g.*, IPSec) are widely used and allow some degree of sharing of common physical infrastructures.

However, except for a number of research efforts [1, 2, 3], the network community has by and large not attempted to provide the same level of automation, customization and pooling of resources in virtualized network infrastructures that is the hallmark of cloud computing. There are several possible reasons for this state of affairs. First, networks provide connectivity between distributed entities, and so, by their very nature are spread out and hence not amenable to the pooling of resources. Second, beyond the interest of networking researchers to experiment with new protocols, the actual need for customization of network functionality has, in large measure, remained elusive. Finally, because many different services depend on the correct operation of the underlying network, networking operators and vendors typically need to be more conservative in adopting new technology, especially when that technology has the ability to modify the function of the network.

We take the position that the complexities inherent in modern and evolving mobile network infrastructures demand a much more flexible and automated approach to network management. Second, this need is best met by fully exploiting the flexibility provided by network virtualization and partitioning functionality. Third, that such functionality provides for the ability to better protect the network against emerging threats and enable new services, especially when this functionality is combined with emerging cloud computing and mobile device technologies. Finally, we argue that, the evolving nature of both the technology and traffic load of mobile networks, combined with the strong separation between control and data planes inherent in these networks, mean that they present a unique opportunity within the networking domain to apply network virtualization.

In this paper we present our vision for Virtual Private Mobile Networks (VPMNs). In its most complete form, VPMN uses virtualization and partitioning technologies to dynamically create pri-

MCS'11, June 28, 2011, Bethesda, Maryland, USA.

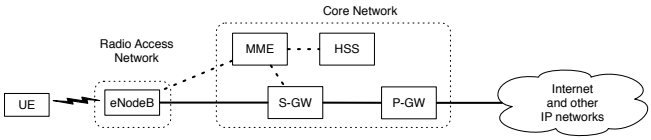

Figure 1: Simplified LTE architecture

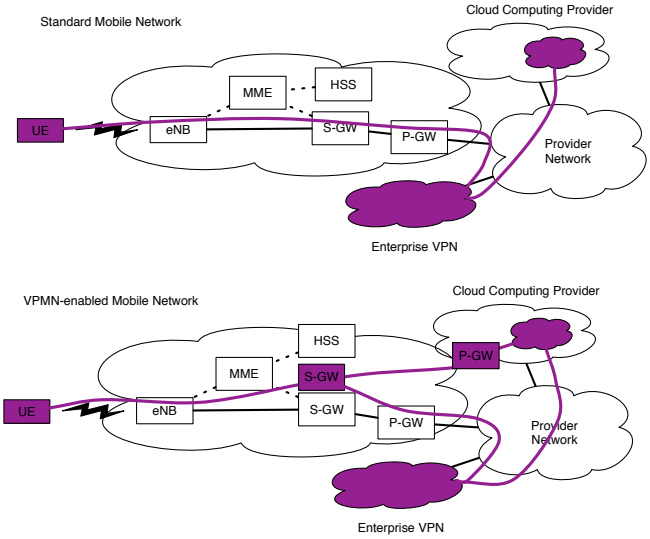

Figure 2: VPMN optimized VPN/Cloud access

vate, resource isolated, customizable, end-to-end mobile networks on a shared physical mobile network. We present an architecture for such an end-to-end VPMN framework based on long term evolution (LTE) and evolved packet core (EPC) mobile technology.[1] However, we recognize that more modest versions of this vision, i.e., VPMNs that are not fully end-to-end, might be more practical and indeed provide useful functionality. We illustrate this by describing a number of VPMN use cases and how they might be realized using LTE/EPC selection functions.

2. BACKGROUND

To provide context for our discussion, we briefly describe the architecture for long term evolution (LTE) mobile networks, and the evolved packet core (EPC) below.

2.1 LTE/EPC Architecture

We provide a brief description of the LTE (Long Term Evolution) and Evolved Packet Core (EPC) system [4] in this section.[2] LTE/EPC is an "All IP Network", and both packet data and voice services use IP. As depicted in Figure 1, LTE/EPC packet system consists of three components: User Equipment (UE) (i.e., the cell phone or other mobile device), Radio Access Network (RAN), and Core Network. LTE RAN consists of eNodeB (enhanced NodeB), which communicates with mobile devices (i.e., UEs) through the radio link and then forwards user packets to a S-GW. eNodeB also performs radio resource control and cooperates with MME (Mobility Management Entity) for mobility management (e.g., location update, handover). LTE packet core consists of MME, S-GW (Serving Gateway), and P-GW (PDN Gateway). MME is on the LTE control plane (shown as dotted line in Figure 1) and interacts with HSS (Home Subscriber Server) for user authentication and mobility management. It also interacts with S-GW for data session establishment/release. S-GW and P-GW are on the data path, and their main function is packet routing/forwarding, traffic management, and traffic accounting for billing. S-GW is also the interface point for legacy cellular data systems (e.g., UMTS (or 3G)). P-GW acts as a gateway to the external network (e.g., the Internet) and supports policy enforcement and charging.[3] To provide large geographic footprint and high quality service, a typical cellular service provider deploys multiple eNodeBs, MMEs, S-GWs, P-GWs, while the exact numbers may vary from one provider to another.

Suppose a UE wants to connect to a server in the Internet. First, the UE sends an eNodeB a session establishment request, which includes an APN (Access Point Name) to specify the type of service (e.g., corporate VPN, Internet service). Then, the eNodeB contacts an MME, which in turn looks up the subscriber information and finds which S-GW to contact for data session establishment for the requested APN. The contacted S-GW establishes a service session context with a P-GW. As mentioned above, the P-GW acts as a gateway to the Internet for the UE, and all the data packets from the UE go through the P-GW. To achieve this, the eNodeB uses a logical point-to-point link to the S-GW by encapsulating all data packets from the UE using GTP (GPRS Tunneling Protocol), which typically runs on top of UDP/IP. Similarly, the S-GW uses another GTP tunnel to the P-GW. Note that these logical point-to-point links can span a large geographic area (e.g., using OSPF routing in the provider's IP backbone) or even multiple continents (e.g., in case of roaming). Upon receiving the GTP encapsulated packets, the P-GW decapsulates the GTP header and further forwards the original packets towards the final destination (e.g., using routing information learned via BGP). The return traffic takes similar steps in the reverse order.

3. A MOTIVATING EXAMPLE

In this section we consider a specific use case to illustrate different requirements of the VPMN architecture. The use case is depicted in Figure 2 and involves an enterprise which has a mobile workforce who needs to access resources in the enterprise VPN while they are traveling, e.g., sales data from a corporate database. In a more extreme case, the mobile workforce might, for security reasons, be equipped with disk-less notebooks which rely on the enterprise VPN for all file accesses.

In our scenario, the enterprise also, on occasions, needs to make use of compute resources from a cloud computing provider. We further assume that the mobile workforce need to utilize the functions that the enterprise hosts in the cloud. The top part of Figure 2 shows the data path such accesses would follow in a "standard" mobile network infrastructure: from the mobile device, traffic would flow through the mobile network, out of the P-GW to a provider network, before reaching the enterprise gateway; once inside the enterprise, traffic would immediately exit again on route to the cloud provider datacenter; return traffic would follow the same path in reverse. This convoluted data path is clearly sub-optimal, and depending on the application, might make it infeasible for the enterprise to use cloud computing resources in this manner, *e.g.*, thin-client applications.

The bottom part of Figure 2 shows a VPMN-based solution to

[1]The architecture would also readily apply to UMTS (3G) environments.

[2]Technically LTE is only a radio access network (RAN) technology and other RAN technologies can make use of EPC. However, it has become common practice to refer to the LTE/EPC combination simply as LTE.

[3]For this, P-GW interacts with PCRF (Policy and Charging Rules Function), which is not shown here for simplicity.

this problem. In this case we assume that the VPMN consists of a P-GW co-located with the cloud infrastructure, and an S-GW (or more likely a number of S-GWs to ensure geographic coverage). Traffic between mobile devices and the cloud infrastructure can now follow the more direct path. However, it is quite possible that mobile devices would require simultaneous access to resources in both the cloud infrastructure as well as the enterprise VPN. We therefore assume that the VPMN S-GW has slightly modified functionality from a regular S-GW in that it could route traffic to either the enterprise VPN or the cloud infrastructure.[4]

While perhaps somewhat contrived, this example is sufficient to identify a number of requirements for the VPMN architecture:

VPMN control framework: VPMN requires a control framework which has access to all potential VPMN locations, via a private out-of-band network. This control framework would export an interface through which a trusted application and/or service, e.g., similar to the cloud control function in our example, can specify the functionality, placement and connectivity of VPMN nodes. Through such an interface the application would also be able to query the network in order to request realistic placement decisions.

Virtual network elements: The network elements associated with a VPMN should be virtualized and/or partitioned versions of physical network elements.

Specialized network elements: The S-GW in our example was assumed to have non-standard functionality.

Dynamic VPMN manipulation: Our example assumes that VPMN creation would be coupled with the enterprise network moving compute functions in the cloud. When the cloud resources are removed, the VPMN should likewise be released.

VPMN selection function: There is a need to intercept and/or modify normal mobility signalling so that mobile nodes associated with a specific VPMN would be identified and associated with the VPMN. In our example, this might have happened during the S-GW selection process, so that the (normal) eNodeB would be instructed to connect to the VPMN S-GW (rather than the "normal" S-GW).

VPMN Inter-node connectivity: To allow VPMN network elements to communicate requires IP level connectivity between them. While such communication can function across any IP network, it would be best provided by some type of VPN technology.

Note that the VPMN described in this example is a partial VPMN, i.e., the VPMN network elements and resource isolation is limited to S-GW and P-GW functions. In the next section we will generalize these requirements to develop a VPMN architecture.

4. VPMN ARCHITECTURE

A conceptual picture of the Virtual Private Mobile Network (VPMN) architecture is shown in Figure 3. Central to this picture is a *VPMN controller* that accepts VPMN related requests, such as creation and manipulation, and interact with the infrastructure to fulfill them. The controller relies on a set of element create/destroy mechanisms to dynamically spawn mobility elements with dedicated resources. Then the controller stitches the individual elements together via a set of selection control mechanisms, which are also responsible for pinning the UEs into the associated VPMNs (or the regular mobility network that co-exists with the VPMNs.)

[4]Note that other options are possible for realizing this use case. E.g., the VPMN P-GW could be made to split the traffic destined to the cloud and VPN respectively and be placed closer to the VPMN S-GW location to ensure low latency to both. Such variations do not fundamentally change the resulting VPMN requirements.

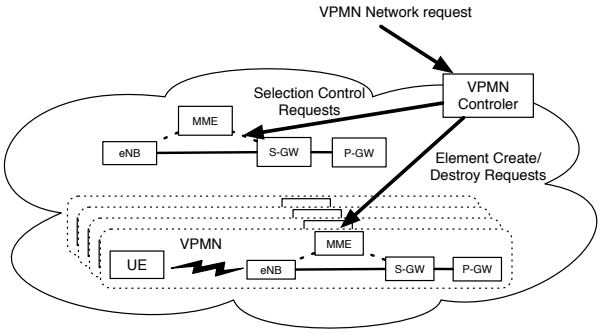

Figure 3: VPMN Architecture

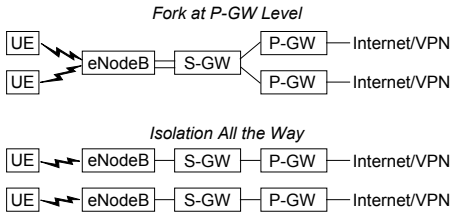

Figure 4: Data-path Isolation in VPMNs

Virtualization and Partitioning Mechanisms: A simple form of partitioning is to have separate physical resources dedicated to different VPMNs. For example, a mobility provider may run two P-GWs on two separate servers, each acting as the anchor point for a particular APN (as shown in the top of Figure 4). Note that in this case the two VPMNs share physical resource up to a S-GW and fork into different P-GWs. The bottom of the same figure shows a more aggressive separation of enforcing isolated resource all the way.

With the advance of virtualization technologies and the tendency of using commodity hardware to host mobility infrastructure (*e.g.*,, S-GW and P-GW in LTE could be realized through software implementation), we envision the encapsulation of mobility functions into virtual machines.[5] Running mobility functionality in VMs has the following benefits: i) It allows us to dynamically spawn individual pieces and tunnel them together to create VPMN instances, or mobility network functionality in general, satisfying the requirements of virtual network elements and dynamic VPMN manipulation mentioned in the previous section. ii) It simplifies the optimization and customization of VPMN instances, for example moving P-GW VMs closer to cloud resources or integrating a modified S-GW, as shown in Figure 2

Virtualized packet core network elements (MME, S-GW, P-GW) can be placed anywhere in the infrastructure, as long as IP-level connectivity (and transport capacity) is provided. This is very attractive for VPMN as it allows network resources to be considered a single pool from which core network elements can be instantiated as needed based on capacity and functionality requirements, *i.e.*, in a similar manner as virtual machine allocation in cloud computing. The same is not true for network elements in the radio access network, which are relatively more difficult to virtualize/partition. These network elements, i.e., eNodeB, manage resources at a specific geographic location and typically utilize specialized hardware

[5]In an early prototype of the VPMN functionality in a UMTS environment, we have been running a UMTS GGSN implementation in a virtual machine and integrated it with our production-grade mobility lab.

to realize radio access control. In this case, we can resort to techniques to ensure the isolated usage among different users. For example, via modified radio resource control [5] radio resources can be partitioned for allocation to different VPMNs.

Selection Control Mechanisms: Both 3G and LTE networks are heavily relying on signaling among the mobility components [4]. There are plenty of opportunities to intercept or modify the selection procedures and thus inject the logic to realize VPMN separation. If we consider the top of Figure 4 to be a partial realization of VPMN, the selection of which P-GW to use depends on the S-GW performing a DNS resolution of the access point name (APN) provided by the UE. In fact, almost all network element selection in LTE is done through DNS lookups [4], thus by hooking into the DNS resolution function, we can flexible control both the control plane and data plane elements used by a UE. To realize the bottom part of Figure 4, we might need to place some identify information on the UE, so that it can only be admitted to a subset of cell towers. For example, we can modify the eNodeB's implementation such that a UE's attachment request is only accepted if the HSS has the information of the UE being part of a particular VPMN.

5. VPMN USE CASES

We envision that, in a manner analogous to how server virtualization radically changed data center management, ease of management and the ability to use resources in a more flexible manner will be a driver for mobile network virtualization, thus enabling VPMN. However, noting the accelerated utility of server virtualization once it enabled cloud services, in this section we consider further use cases enabled by VPMN.

5.1 Mobility-as-a-service

The capital-intensive infrastructure required to build a large scale mobility network can be made available in the form of a virtual network to organizations that wish to have a network of their own but do not want to spend the required capital. Resources needed by such a virtual network can be allocated in an always-available manner or dynamically, as and when/where needed. There are at least two distinct advantages to this:

Secondary mobility networks: Mobility virtual network operators (MVNOs) are companies that employ the infrastructure of a primary operator to offer mobility services directly to end-users. Most MVNOs share only the radio access portion (RAN) of the primary mobile network operator and operate the rest of the mobile network elements on their own. The reason for this is that the cost of market entry for a new mobile service provide has been dominated by the cost of spectrum and the cost of installing cellular base stations with back-hauls to provide adequate coverage. While the cost of the remaining part of the mobile network is still smaller than that of building a country-wide RAN, handling large and ever-increasing volumes of data requires non-trivial resources for operations and management in the rest of the mobility network. The high cost of a country-wide network also keeps government agencies (law enforcement, emergency response, etc.) from building out a dedicated network of their own from scratch, even though they have a real need to have their own mobile network. The VPMN framework promises to lower the barrier to entry by allocating resources to the secondary operators (or government agencies) *as and when needed*, thereby allowing us to view the mobility network as a cloud platform providing mobility as a service.

Customizing network parameters: In certain scenarios, application service providers may wish to modify parameters inside the mobility network to better suit their service offering. As an example, consider the radio resource control state-machine in 3G cellular systems, which runs inside the radio network controller (RNC) and controls the power usage and bandwidth states of each connected mobile device. A static set of parameters can be highly suboptimal for certain types of streaming applications but if the parameters of the state-machine are allowed to be modified, they can be better tuned to a service, thereby improving battery life and performance of mobile devices. For example, the authors in [6, 7] performed an optimization of the radio resource control state-machine for the popular audio-streaming application, Pandora and found that the changes made to the state machine made the battery utilization on a mobile device streaming from Pandora much more efficient. The VPMN framework can be used to create network slices that include all or some of the components of the mobility network, in which third party application service providers are granted control over the parameters of the slice, without interfering with the rest of the network. This may be particularly helpful in customizing the behavior of the network for various type of other cellular-connected devices other than mobile handsets, such as sensors.

5.2 Sandboxing

As mobile devices become more sophisticated, they have started to emerge as prime targets for Internet perpetrators. Several types of malware designed for mobile devices have been discovered over the past few years [8] [9]. Such mobile malware can potentially be used for a wide range of malicious activities, such as stealing sensitive user information, distributed denial of service attack against network infrastructure, etc. Therefore, it is crucial for mobile network operators to detect and track infected mobile devices in their networks. Similarly, mobile operators may want to track various untrusted or vulnerable devices (i.e., jailbroken devices, devices with specific OS version, etc.) due to their potential to harm other users and the network infrastructure.

One appealing strategy to achieve this is by using the VPMN architecture to create sandbox environments for infected or untrusted mobile devices. More specifically, a network operator can provide service to such untrusted devices through a VPMN slice which serves as a sandbox. By isolating and tightly-controlling such a sandbox environment, mobile operators would be able to protect the rest of their networks of potentially harm from untrusted devices. For instance, a group of infected mobile devices attacking the network infrastructure would only affect the VPMN slice that they are in without disturbing the rest of the network. For protection at a finer granularity, network operators may choose to create a different sandbox environment for different kinds of untrusted devices. That way, malicious activities of the devices infected by a specific malware would only affect the devices which have the same infection. Alternatively, an operator might want to more closely monitor devices that has been identified as taking part in an emerging network attack and/or threat. In this case the devices might be served by a VPMN equipped with specialized monitoring equipment.

5.3 Latency Reduction

Despite the rapid pace of adoption of data-centric services on mobile devices, mobility networks are often primarily used as an unintelligent transport to ultimately reach a gateway that connects to the Internet (the P-GW in the case of LTE - see Figure 1). Routing of packets within the mobility network is based on the topology of elements within the mobility network with respect to the location of the user, rather than the type of application a mobile user is accessing. This approach is suboptimal for applications that are latency sensitive in that there is no awareness within the mobility network of the services that are being utilized and consequently

the network provides no support for the possibility of enhancing those services. This situation is further exacerbated by the fact that current mobile networks are a monolithic closed systems that cater best to the common services (voice, web-browsing, etc.) based on industry wide standards, but do not allow sufficient control over the building blocks of the mobility network that is needed for differentiation or innovation to provide support for services/applications with specialized requirements. Latency-sensitive services are one such class of services.

The VPMN framework can be used to dynamically instantiate a slice in the mobility network that allows for redirection to specialized nodes in the network, allowing for reduction in latency. Further, since a separate virtual network is instantiated for a given service, control mechanisms and parameters of the virtual network can be dynamically optimized by the third party service provider that provides the latency sensitive service. Examples of latency sensitive applications that would benefit from latency reduction offered by the VPMN infrastructure include:

Content distribution – One possibility is placing content servers closer to mobile users, within the mobility network.

Gaming – The VPMN framework can help here by allowing for redirection to special dedicated mobility network elements (S-GW, P-GW, etc.) that are topologically positioned to minimize latency between gaming endpoints.

Offloading computation – Interactive applications that require computation to be offloaded from a mobile device onto computing infrastructure (see for example [10, 11]) can benefit from latency reduction. Indeed this was implied by our motivating example in Section 3. In this case performance can be improved, or new applications enabled, if the computing resource is made part of the mobility network, placed as close as possible to the mobile user (e.g. one extreme case would be to have a small server at each base station) and made accessible inside a separate slice.

6. RELATED WORK

Virtualization of network resources has been used before in wired networks and to a lesser extent in wireless networks.

Wired networks: Planetlab [12], a global scale experimental overlay network, uses network virtualization to allow several users to share the same infrastructure. The ShadowNet framework [1] consists of dedicated nodes comprising carrier grade equipment (routers, switches, servers) attached to an operational tier-1 backbone, that enables testing of new network operational and management functions. VINI [2] is a virtual network infrastructure built on top of Planetlab. Emulab [3] is a centralized testbed that emulates topologies and also utilizes virtualization for concurrent sharing between experiments.

Wireless networks: Virtualization of the mobile network's radio resources has recently been studied in the context of WiMax [5]. Here, the authors have focused on virtualizing the spectrum resource at the radio interface of a WiMax network, using a flow-based scheduling system in which slices are provisioned by the time-scheduler. Other work has focused on providing fair share of the downlink resources in WiMax to the different virtual slices [13] and providing a virtual WiMax base station for use with different virtual slices within the WiMax network [14]. While all the above approaches focus on virtualizing the radio resources and devices, our work focuses on virtualizing all the elements in the core mobility network including the radio resources.

Our work leverage and extend these approaches and we specifically focus on the operational efficiencies and new service abstractions that might be realized.

7. DISCUSSION AND CONCLUSION

We presented the concept of Virtual Private Mobile Networks (VPMNs) as a means to dynamically create private, resource isolated, customizable, end-to-end mobile networks. From an operational perspective this approach allows network resources to be considered a flexible pool of assets which can be dynamically utilized as needed. Perhaps more importantly, however, we envision the VPMN approach to enable new service abstractions, especially where services or application need to interact with the network more closely, or customize network behavior.

We note that some of the use cases we presented can be readily achieved with relatively small modifications to standard approaches. Indeed using such standard functionality is an integral part of our approach. The key open question we are investigating at the moment is whether there is a "sweet spot" in terms of the extent or coverage of the VPMN approach. For example, virtualizing and customizing the radio access network might be technically feasible and would enable new functionality and services (protection against subtle radio access or control plane attacks, or radio access protocols specialized for specific services). However, realizing such functionality at scale might not be economically feasible. On the flip side, applying the VPMN approach to packet core components is eminently doable. Exploring these trade-offs and the detailed mechanism to realize VPMN are topics of our ongoing research.

8. REFERENCES

[1] X. Chen, Z. M. Mao, and J. Van der Merwe, "ShadowNet: A Platform for Rapid and Safe Network Evolution," in *USENIX ATC*, 2009.

[2] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: realistic and controlled network experimentation," in *SIGCOMM*, 2006.

[3] 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," in *OSDI*, 2002.

[4] M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, *SAE and the Evolved Packet Core - Driving The Mobile Broadband Revolution*. Amsterdam, Boston Elsevier LTD., 2009.

[5] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "NVS: a virtualization substrate for WiMAX networks," in *MOBICOMM*, 2010.

[6] F. Qian, Z. Wang, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck, "Characterizing radio resource allocation for 3g networks," in *IMC*, 2010.

[7] F. Qian, Z. Wang, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck, "Top: Tail optimization protocol for cellular radio resource allocation," in *ICNP*, 2010.

[8] P. A. Porras, H. Saidi, and V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," in *MobiSec*, 2010.

[9] "Android Threats Getting Steamy." http://www.symantec.com/connect/blogs/android-threats-getting-steamy.

[10] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing," in *IEEE Pervasive Computing*, November 2009.

[11] E. Cuervo, A. Balasubramanian, D.-k. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, "Maui: making smartphones last longer with code offload," in *MOBISYS*, 2010.

[12] L. Peterson, A. Bavier, M. E. Fiuczynski, and S. Muir, "Experiences building planetlab," in *OSDI*, 2006.

[13] G. Bhanage, R. Daya, I. Seskar, and D. Raychaudhuri, "VNTS: a virtual network traffic shaper for air time fairness in 802:16e slices," in *IEEE ICC - Wireless and Mobile Networking Symposium*, 2010.

[14] G. Bhanage, I. Seskar, R. Mahindra, and D. Raychaudhuri, "Virtual basestation architecture for an open shared wimax framework," in *ACM SIGCOMM Workshop on Virtualized Infastructure Systems and Architectures*, 2010.