Bandwidth Control and Regulation in Mobile Networks via SDN/NFV-Based Platforms

Thomas Anderson, thomande@cisco.com; Peter Bosch, pbosch@cisco.com;
Alessandro Duminuco, aduminuc@cisco.com
for GSMA / IAB workshop, September 2015

***Abstract* — We explain why Software Defined Networking (SDN) and Network Function Virtualization (NFV) play an important role in evolving the mobile packet core and the systems that are deployed at the boundary between the mobile packet network and data networks such as the Internet and enterprise networks. These systems (DPI, video optimization, content caching, etc …) are precisely those most affected by the pervasive use of encryption in mobile networks. This position paper describes a use case for a platform that employs SDN and NFV concepts that is used to mitigate the effects of encryption and address the mobile operator needs for regulating and managing traffic for better QoE.**

1 INTRODUCTION

The fraction of encrypted traffic traversing (mobile) networks is rapidly increasing. The main driver for this phenomenon is the adoption of TLS/SSL protocol by many content owners and providers, either in conjunction with HTTP/1.1 or as a base requirement in HTTP/2.0/SPDY. The encryption trend leads to a significant impact on the (mobile) service providers' ability to provide reasonable network management mechanisms in their networks. As their networks are increasingly traversed by opaque data flows, service providers are no longer able to use traditional packet inspection techniques to analyze and regulate this traffic for improved network performance and user Quality of Experience (QoE).

For (mobile) service providers to participate in the changing data-networking world where the majority of mobile traffic is encrypted, (mobile) service providers need to change their strategy regarding network traffic management. In particular mobile service providers must focus on new ways to manage their network by better leveraging their unique position in the end-to-end network chain: (1) (mobile) service providers are access gatekeepers and thus are topologically close to the edge of the network and (2) (mobile) service providers maintain an existing trust/commercial relationship with end subscribers. This translates into specific new network models which include:

1. Foster cooperative partnerships with third-party application providers and associated aggregators to expose and monetize (mobile) network functionalities and information. Such functionalities and information include channel condition information, QoS settings, subscriber identity, and other subscriber dependent information;
2. Make better use of subscriber opt-in techniques to offer value-added services to (mobile) service provider subscribers;
3. Enable content owners and content providers to securely run their value-added services in the (mobile) service provider's network itself. These services include content caches, web-servers, optimization engines, etc …; and
4. (Mobile) service providers to become content providers themselves to enable their own service offerings to content owners.

This paper focuses in particular on the first three points and argues how NFV and SDN technologies play a key role in providing the necessary flexibility and control granularity needed to implement them.

2 RAPID INCREASE OF ENCRYPTED TRAFFIC IN OPERATOR NETWORKS

The underlying reasons for the rapid increase of carrying web and (smart-phone) application traffic in encrypted forms are as follows:

- Subscribers increasingly demand privacy and authentication in web transactions, especially for highly sensitive applications such as e-banking and e-commerce, but it is also critically important for any kind of application that handles personal information such as emails, social networks, instant messaging, etc. Given today's public opinion on privacy, it has also become a significant business risk for companies to leak customer-private data or as being perceived as callous with such data. Indeed, in many jurisdictions world-wide privately identifiable information is protected by law.
- Content owners need full and exclusive control over the content they serve. These content owners need to avoid any middle-box service that handles, inspects or modifies their content, and as such, these companies need to avoid "middle-boxes" to derive value from content owner's data.

While the reasons above explain why subscribers and content providers are willing to encrypt their conversations, the factor that is currently driving most of the increase in TLS adoption is the introduction of HTTP alternatives, such as SPDY/HTTP2.0 [1][2]. Moreover, smart-phone application traffic deploys secure communication channels as well. These protocols have been conceived to reduce latency of web-content delivery over the TCP protocol and include by default TLS based encryption. In addition, smart phone applications increasingly use encrypted channels to communicate between the mobile device and the (cloud-based) applications.

SPDY proxies further hide regular HTTP traffic by creating an encrypted conversation tunnel between a collaborative client device (with its browser properly configured) and the SPDY proxy. This tunnel carries all web/SPDY requests generated by said device. The SPDY proxy extracts the requests from the tunnel, opens and maintains regular HTTP(S) sessions tunnels to the final Internet destinations, retransmits the original web requests, and re-aggregates the web-server's responses into the SPDY tunnel back to the client. Such a scheme prevents middle boxes from even detecting the final destination of the HTTP traffic. Thus, in addition, SPDY proxies can also negatively impact CDN and caching performance since the proxy itself may not be optimally located for CDN performance as compared to the option where the device goes direct to a CDN / cache.

3 CHALLENGES FOR MOBILE SERVICE PROVIDERS

Traditionally mobile service providers manage traffic in their network by applying "service functions" through middle boxes and other inline appliances and by placing these functions between the mobile packet core and the Internet/enterprise networks. All data transmitted from and to the mobile device is additionally routed *through* the middle boxes. These service functions are virtual or physical *boxes* deployed and chained into what is commonly referred to as Gi-LAN infrastructure. This is named the Gi-LAN infrastructure after the 3GPP specified (S)Gi-Interface.

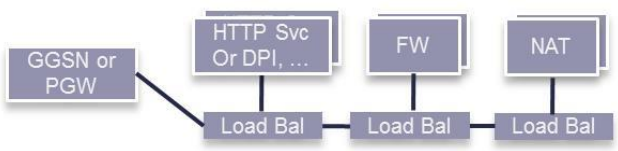

Figure 1 Traditional 3GPP Gi-LAN Architecture

Most of the services included in current Gi-LAN deployments need to access and/or modify data traversing the network. These include:

- Content-optimization boxes: video transcoders can optimize videos to the specific target device; image compressors can adapt the image size and quality to the radio access conditions; HTTP(S) proxies can reformat HTML to be tiny screen friendly, etc.
- TCP optimization proxies: TCP is known to operate poorly in a mobile access network and special TCP proxies can be adopted to mitigate the existing inefficiencies.
- Caching functions: frequently accessed data can be cached at the edge of the network achieving both reduced latency and reduced peering costs.
- Content-based filters: URL-based filtering can implement parental controls, and DPI based traffic detection can enforce fair-use capping or blocking.
- Security-based intrusion detection/mitigation appliances: scan traffic for malicious traffic.
- Charging functions: implement special charging relationships with 3rd parties to allow certain classes of customer traffic to be billed to the 3rd party rather than the subscriber (contingent on country and local regulations).
- Ad-insertion engines: HTTP proxies are able to insert targeted advertisements.
- Header-enrichment proxies: Exposing mobile network information allows content providers to optimize content.
- Analytics engines: Monitors collect and monetize user behavior statistics.

Most of these services are severely constrained if not infeasible when data flows are encrypted end-to-end. This is a side effect of protecting user privacy but also an explicit intent of content providers advocating for encryption.

4 Possible Mobile Service Providers Strategies

The scenario described earlier clearly demands a strategy evolution in mobile service provider networks to re-enable the network management and subscriber benefits that may be lost with pervasive encryption. As access providers, mobile service providers still hold a key position that cannot be easily circumvented by so called "over the top" and 3rd party providers:

- Mobile service providers hold commercial/billing relationship with end customers.
- Mobile service providers manage their access networks, i.e., mobile service providers are gatekeepers of the mobile Internet and/or enterprise networks, which includes the ability to monitor traffic and manage congestion, to control subscribers network access methods and to influence methods for consumption and payment for data access.
- Mobile service providers are topologically as close as possible to the data consumers.

The mobile network maintains subscriber information and information on the access network that can be useful to content companies. These include:

- Subscriber identity, which with the agreement of the end user could be exposed to the content owner to enforce more robust authentication mechanisms;
- Subscriber meta-information, such as precise geographic location, billing category, usage patterns, mobility patterns, etc. Such information can be used to provide more targeted services or ads; and
- Access-channel information, such as radio-link quality, channel congestion, radio-access technology. Access to such information enables content providers to better adapt content to the current access capabilities.

Moreover the mobile network implements functionalities that subscribers and content companies are willing to pay for.

These functionalities include:

- Ability to upgrade/downgrade the access QoS. For example, in 4G networks the mobile network operator can create a dedicated bearer with particular QoS settings that carry specific flows [6]. This can be used to prioritize and improve the quality of experience of certain content consumption;
- Ability to offer advanced parental control and security scanning services to mobile subscribers;
- Ability to use the billing relationship with the mobile customer to pay third-party services (with user consent); and
- Allowing third parties to sponsor the mobile data delivery, i.e., content companies can pay the bill for the delivery of certain content.

5 How SDN/NFV Gi-LAN Platform Helps

Effectively implementing earlier described services and capabilities in an encrypted networked world can benefit from a new *virtualized* Gi-LAN infrastructure. Such an infrastructure leverages SDN technology and ETSI NFV-based function delivery by way of deploying services through *virtual machines*[1] generally called ETSI NFV *Virtual Network Function-Components (VNF-Cs)*. This new infrastructure combines virtual function delivery with service chains e.g., by way of NSH-based service chains [10]. Key elements of this new virtual Gi-LAN platform include:

- A subscriber-aware policy function that can provide subscriber specific guidance on how traffic flows may be differentially handled within the platform on a per-subscriber and per flow basis. This can be considered a subscriber-aware SDN controller;
- A classification function to classify traffic based on the above referenced subscriber-aware policy function into specific service chains dynamically. Changes in subscriber policy can be reflected into changes in service path assignments in real time. Each specific service path includes a specified set of service functions required to manage traffic assigned to the specific service path;
- A switching function to efficiently support service path switching (e.g. IETF SFC enabled);
- New service functions designed to better monitor and manage encrypted traffic; and
- All on an ETSI NFV compliant virtualization platform that enables dynamic growth of service capacity of the service platform. The virtualization platform's role is to track the liveliness of deployed VNF-Cs, to auto-scale VNF-C capacity to demand, and to programs service chains through the SDN infrastructure.

This platform is flexible and elastic such that it can support a wide variety of use cases and services addressing the encrypted and non-encrypted network environment. Specific use cases include allowing Gi-LAN services to expose service provider functionalities and information to third parties, or in enabling third party content providers to install their own services in a mobile service provider's Gi-LAN platform.

[1] Please note that *virtual machines* is used in the broadest sense here: these can be bare-metal deployments, containers, Qemu-based virtual machines, or any other type of *virtual* deployment.

6 Gi-LAN Multitenancy For Third Parties

As described earlier, many of the mobile core services cannot provide their services when exposed to encrypted data flows. However, some of them, such as content caches, are most effective when run closer to the edge of the network. This is because (1) these caches can provide lower latency experience for end-users; and (2) they allow for the maximum savings in terms of (Internet) peering costs.

Although the most convenient place for content cache services to be deployed in a mobile network is the Gi-LAN infrastructure, the opacity of encrypted flows prevents mobile service providers from running these Gi-LAN services on their own.

Instead, we propose mobile service providers to provide content caches as-a-service and allow content companies, i.e., those companies that hold content and the associated encryption keys, to control the content caches hosted by the mobile service providers. Moreover, mobile service providers can also allow content companies to install their own services, thus enabling 3rd parties to host a mix of service provider functions and 3rd party functions in a common virtual Gi-LAN infrastructure.

The mere fact that Gi-LAN service infrastructures can be offered through an as-as-service offering with ETSI NFV and SDN technologies at the heart of the virtual deployment, enables such over-the-top and 3rd party service deployments inside the mobile service core. When compared to a traditional Gi-LAN infrastructure, typically implemented as a bespoke, physical network element solution, deploying such 3rd party services in a ETSI NFV-based environment greatly enhances the a 3rd party's ability to offer enhanced services close to the edge of the network – in a bespoke, physical deployment, over-the-top and 3rd party providers can only provide for their services in the mobile network by way of physically installing a *box* with the service in the mobile network.

The key benefit for the mobile service provider is that the mobile service provider can monetize its access networks through new methods: the mobile service provider can create a service offering from over-the-top and 3rd party content providers. Since virtual services are deployed in service chains, e.g. by way of IETF SFC, a mobile service provider can even provide a concatenation of over-the-top and 3rd party services in their networks.

For these optimization scenarios to be viable, the content companies need to secure their content from the mobile service provider for legal or business reasons and maintain the end-to-end security relationship between the subscriber and their services. Mobile service providers must offer secure hosting capabilities in the "Gi-LAN service area" to enforce privacy for content companies in the service provider's infrastructure through existing and novel hosting techniques. While absolute privacy cannot be guaranteed in cloud systems[2], cloud-orchestration systems can manage secure and private hosting. In addition, novel techniques can be used in case 3rd party service functions need to be chained in such cloud systems.

To encourage content companies to acquire virtual Gi-LAN hosting services, mobile service providers can make the services described in the previous section available only locally within the mobile service provider network. This approach can also increase the manageability and security of the services.

[2] At least, with today's cloud-computing hardware.

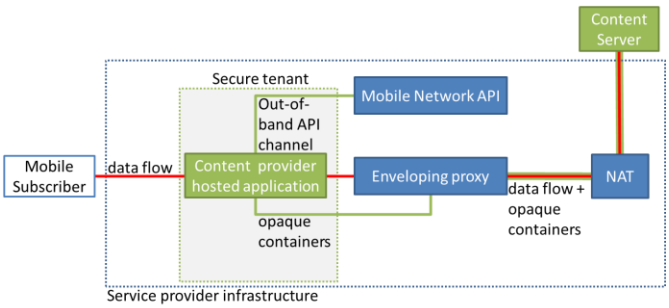

Figure 2 Gi-LAN multitenancy architecture

Content provider services hosted in a virtual Gi-LAN system likely need to exchange information with the origin content servers, for example: information collected by the mobile network, session encryption keys, or other data flow meta-information. This exchange can be provided for by way of an out-of-band or tunnel-based channel. This means that a mobile service provider needs to enable direct communication between the over-the-top/3rd party service provider and their services operating within the confines of the mobile service provider's cloud systems. This requirement places specific networking and scaling constraints for over-the-top/3rd party service provider operating inside the mobile service provider's network. Moreover, specifically on scaling functions, there needs to be a closed-control loop between the mobile service provider's ETSI NFV and SDN solutions and the over-the-top/3rd party control center to manage the virtual deployments securely and effectively.

7 CONCLUSION

The growing rate of encryption of data traversing mobile network requires mobile service providers to evolve the way they manage their network.

This paper argues for a strategy evolution in mobile service provider networks to re-enable the network management and subscriber benefits that may be lost with pervasive encryption, specifically leveraging the privileged position mobile service providers have.

Such involvement can be implemented in many different ways and would greatly benefit from a new, subscriber/policy aware, dynamic, NFV/SDN enabled Gi-LAN architecture.

8 REFERENCES

[1] SPDY white paper (http://dev.chromium.org/spdy/spdy-whitepaper)

[2] M. Belshe, R. Peon, M. Thomson, A. Melnikov, Hypertext Transfer Protocol version 2.0, IETF draft https://datatracker.ietf.org/doc/draft-ietf-httpbis-http2/

[3] State of the Mobile Service Provider: "Middleboxes" and SPDY, Cisco White Paper, 2013

[4] Jeffrey Erman, Vijay Gopalakrishnan, Rittwik Jana, K.K. Ramakrishnan, Towards a SPDY'ier Mobile Web?, In ACM CoNext 2013

[5] United States Courd of Appeals, No. 11-1355, Jan-2014 (http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf)

[6] 3GPP TS 24.301 V12.3.0, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 12)

[7] ATIS-020010, ATIS standard on CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment, Alliance for Telecommunication Industry Solutions, 2012

[8] K. Leung, Y. Lee, Content Distribution Network Interconnection (CDNI) Requirements, IETF draft https://datatracker.ietf.org/doc/draft-ietf-cdni-requirements/ , 2013

[9] ATIS, An Analysis of the SPDY Protocol and the SPDY Proxy, 2014

[10] P. Quinn, U. Elzur, Network Service Header, IETF draft, https://tools.ietf.org/html/draft-ietf-sfc-nsh-00/