Handbook of Research on Progressive Trends in Wireless Communications and Networking

M.A. Matin  
Institut Teknologi Brunei, Brunei Darussalam
Chapter 3
IP-Based Virtual Private Network Implementations in Future Cellular Networks

Madhusanka Liyanage  
University of Oulu, Finland

Mika Ylianttila  
University of Oulu, Finland

Andrei Gurtov  
Aalto University, Finland

ABSTRACT

Virtual Private Network (VPN) services are widely used in the present corporate world to securely interconnect geographically distributed private network segments through unsecure public networks. Among various VPN techniques, Internet Protocol (IP)-based VPN services are dominating due to the ubiquitous use of IP-based provider networks and the Internet. Over last few decades, the usage of cellular/mobile networks has increased enormously due to the rapid increment of the number of mobile subscribers and the evolvement of telecommunication technologies. Furthermore, cellular network-based broadband services are able to provide the same set of network services as wired Internet services. Thus, mobile broadband services are also becoming popular among corporate customers. Hence, the usage of mobile broadband services in corporate networks demands to implement various broadband services on top of mobile networks, including VPN services. On the other hand, the all-IP-based mobile network architecture, which is proposed for beyond-LTE (Long Term Evolution) networks, is fuel to adapt IP-based VPN services in to cellular networks. This chapter is focused on identifying high-level use cases and scenarios where IP-based VPN services can be implemented on top of cellular networks. Furthermore, the authors predict the future involvement of IP-based VPNs in beyond-LTE cellular networks.

DOI: 10.4018/978-1-4666-5170-8.ch003
INTRODUCTION

Global marketing strategies increase abilities of a firm to conduct its business in various locations across the world. However, the secure communication among these sites is also mandatory to perform a smooth operation of the organization. Many firms use advance communication services such as VPN services to interconnect these geographically distributed branches to headquarters. A VPN service is the first choice of many organizations since it is the most prominent communication methodology to provide a secure inter-site connectivity.

The notion of VPN or Virtual Network (VN) services has been around for last four decades which is almost the same as the life span of data networks. The usage of VPN services is constantly improving due to various factors. Primarily, the implementation cost of VPNs is drastically decreasing with the use of low cost network equipments and communication devices. Furthermore, the competition between different network service providers causes to reduce subscription fee for a VPN service. On the other hand, the technological advancement of VPN technologies in terms of enhanced security, high speed connectivity and high reliability are motivating many organizations to use VPN based services.

The usage of mobile network based broadband services has drastically increased over the past few years. The number of mobile subscribers is increasing rapidly and the total mobile broadband traffic volume is growing faster than the fixed Internet traffic. Furthermore, the steady development in telecommunication techniques causes to provide almost the same level of broadband services as fixed Internet in terms of bandwidth, reliability and Quality of Service (QoS). The recent surveys showed that the number of worldwide mobile broadband subscribers has already exceeded the number of fixed broadband subscribers (Cisco, 2010). Moreover, a telecommunication network is able to provide anytime anywhere broadband connectivity regardless of the mobility pattern or the location of the subscriber. This is the most prominent advantage of a mobile broadband service. For instance, many organizations often have “road warriors” who equip with portable computing devices such as laptops, smart phones and various tablet devices. These road warriors need to work from anywhere without being physically present in the office. The integration of virtual networks and mobile broadband services is a promising solution to provide efficient and secure connectivity for these road warriors. Furthermore, there are large numbers of mobile network operators than fixed network service operators. Thus, the competition among the mobile network operators is very high and it drastically decreases the mobile broadband charges. These facts fuel corporate customers to choose mobile broadband over wired network services.

The LTE specification introduces all-IP network architecture and beyond LTE networks will operate on top of IP infrastructures. Thus, we focus only on IP VPNs in this chapter. We present high level use cases and scenarios of IP based VPN services which are implemented on top of cellular networks.

VIRTUAL PRIVATE NETWORK

A virtual network is a communication network which contains virtual network links. In other terms, it is a collection of virtual links which are established on top of a physical network. These virtual links are implemented by using methods of network virtualization and they are transparent to end users.

There are two commonly used methods of network virtualization; namely protocol based virtual networks and virtual device based virtual networks (Metz, 2003). However, protocol based virtual networks are easy to implement and globally ubiquitous than virtual device based virtual networks. For instance, VPNs, VLANs (Virtual Local Area Networks), VPLSs (Virtual Private
LAN Services) are the widely used protocol based virtual network implementations (Rosenbaum et al., 2003).

A virtual network which extends a private network across public networks is called Virtual Private Network (VPN). It allows a remote host or site to be a part of the private network with all the functionality by communicating data across a shared or a public network.

These are several building blocks of a VPN.

- **Customer (C) Device:** A C device is a legacy device which is owned by the customer. Customer devices are not aware of the presence of a VPN.
- **Customer Edge Equipment (CE):** CEs are located at the edge of the customer’s network. It might be a host equipment or a router or a switch which is located at the customer’s premise. Furthermore, CE is the interface device between the customer and provider networks.
- **Provider Edge Equipment (PE):** PEs are located at the edge of the provider network and connects to customer sites through CEs. Hence, PEs are aware of the existence of VPNs and contain all the VPN intelligence.
- **The Core Network:** The core network is the backbone network of the VPN. It belongs to the network service provider. This core network can be operated based on several network protocols, such as IPv4, IPv6, MPLS (Multiprotocol Label Switching).
- **Provider Device (P):** A P device is located inside the core network. They are not directly interfacing to any customer network. Hence, the P devices are not VPN-aware and maintaining any VPN states. Its principal role is to support the traffic routing and aggregation functions of the core network.

Figure 1 Illustrates a topology of a simple VPN.

### History of Virtual Private Networks

The history of VPNs spans as long as the history of the data communication networks (Metz, 2003). The first generation of VPNs was based on X.25 carriers. In early 1970’s, VPNs were consisted of privately operated network devices which are connected by using the dial-up or dedicated leased lines over an operator network. In the late 1970s, the development of X.25 introduced the virtual connection concept for data networks. The connection-oriented networks were capable to logically separate customer communication channels for virtual connections. Then, operators were capable of multiplexing various virtual connections which are interconnecting users from the same customer cooperation, through a single switched network infrastructure. TCP/IP protocol was introduced to data networks in the 1980s (Rosenbaum et al., 2003). In the early 1980s, X.25 carriers began to offer VPN services to early adopters of TCP/IP protocol stack.

The second generation of VPNs was the virtual connection oriented VPNs based on frame relay and ATM (Asynchronous Transfer Mode) switching. The advancement of frame relay and ATM switching technologies were allowed to provide high speed virtual connection based services. In the 1990s, the connectivity speed of virtual network connections grew up to 155 Mbps (Knight & Lewis, 2004).

The third generation of VPNs was IP based VPNs. During the mid-1990s, the traditional connection oriented VPNs services such as ATM and frame relay were in the decline stage of the product lifecycle. Simultaneously, Internet began to popular in communication networks. Thus, network service providers began to build new network infrastructures to support IP based services. These migrations fuel the adaptation of IP based virtual networks as well. IP based VPNs were attracted by various customers since they provide significant economic advantages and better service functionalities than the connection oriented VPN.
services. Meantime, service providers started to offer IP VPNs as a Value Added Service (VAS) for customers. It was the initiation of the provider provisioned VPN concept.

The fourth generation of VPNs aims to extend IP based Layer-2 VPN (L2VPN) solutions over WAN (Wide Area Network) connectivity through an IP or MPLS network. Especially, Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS) are becoming popular as a cost effective alternative to Layer-3 VPN (L3VPN) solutions.

**IP-BASED VIRTUAL PRIVATE NETWORK (IP VPN)**

IP VPN is a virtual network which is deployed over a shared IP based network infrastructure. It connects customer sites by using IP VPN tunnels. These IP VPN tunnels offer the packet based VPN connectivity. It forwards the customer data, packet by packet basis. A separate tunnel header is imposed on the VPN data packet at the source site and disposed it at the destination site. It allows to opaque ly forwarding the VPN data packets through the provider network or the Internet (Carug & Clercq, 2004).

IP VPNs are widely used in corporate organizations since they provide various benefits to the customer (Harris, 2002).

- **Global Ubiquitous Availability:** IP based networks are widely available all over the globe. All most all the network operators provide IP based network connectivity for customers. Literally, the IP VPN services can be implement in anywhere in the world.
- **Any-to-Any Connectivity**: IP VPNs allow establishing a full mesh of VPN tunnels over the provider network. Hence, the customer can achieve any to any connectivity.

- **Secure, Scalable, Flexible, Robust Network Architecture**: IP based network technologies such as MPLS and IPsec, have been developed thought out the last two decades and matured in terms of technology. They have already addressed the most of the scalability and security issues. Further, various versions of IP based technologies are available in the market and the customer has the flexibility to select any of the technology according to his requirements.

- **Classes of Service and Traffic Aggregation**: IP VPNs can accommodate and optimize traffic belong to various classes. It allows traffic prioritization and extra bandwidth allocations according to requirements of different traffic classes. On the other hand, it is possible to integrate various traffic types and delivers them in a single network infrastructure due to the packet based VPN connectivity.

- **Economic Advantages**: IP based VPNs have lower implementation and maintenance cost than traditional virtual connection based VPN services.

IP VPNs can be categorized in to two main classes (Rosenbaum et al., 2003).

1. Network based IP VPN
2. Premises based IP VPN

**Network Based IP VPN**

The service provider is responsible for all operational and management tasks of a network based IP VPN. Hence, the customer does not need to consider about the implementation aspects on the VPN service over the public network. The customer and the provider exchange several Service Level Agreements (SLAs) to define the required service level such as bandwidth, the number of connected sites, traffic priorities and the classes of service quality (Venkateswaran, 2001; Callon & Suzuki, 2005).

Several versions of network based IP VPNs are available in the market (see Figure 2).

Network based IP VPNs attract more corporate customers due to several reasons. It is estimated that revenues for the network based IP VPN market in 2009 will be double in 2014 (XO, 2010).

There are several market drivers and advantages of network based IP VPNs (Daniel, 2004).

1. **Lower the VPN implementation and maintenance cost**: The customer’s capital cost is low since he is not responsible to implement or manage the VPN devices. He can purchase on the shelf VPN services without changing anything in his private network infrastructure. Moreover, the customer needs a very small number of technical staff to manage the VPN since the routing, maintenance and operational functions are outsourced to the provider. On the other hand, the customer has opportunity to tailor-made his VPN service at any time just by exchanging few SLAs with the provider.

2. **Converged network services**: In contrast to other VPN services, network based IP VPNs can transport traffic belong to various applications such as VoIP, data, video and multimedia applications, in a single VPN services.

3. **Traffic prioritization**: Network based IP VPNs support traffic prioritization which allows the provider to tailor the bandwidth according to the requirement of each customer traffic type.

4. **Global ubiquitous availability**: Network based IP VPNs are widely available all over the globe. Many network operators provide IP VPNs as an additional broadband service for their customers.
The market restraints of network based IP VPNs include:

1. **Sunken investments on ATM & Frame Relay networks**: ATM & frame relay networks are still dominating the access network space. Many of the network operators still use ATM & frame relay networks. Thus, they are reluctant to deploy IP based infrastructures due to the sunken investment to deploy these old technologies. It delays the process of adaptation of new network based IP VPN technologies.

**Premises Based IP VPN**

The customer is responsible for all the operational and management tasks of a premises based IP VPN. The network operator only provides the connectivity among the customer sites and he is not aware the existence of premises based VPNs. Hence, the customer must have expertise in the implementation of VPN service over the public network. Furthermore, premises based IP VPNs require to install intelligent devices at the customer premises which can provision VPN services over the provider backbone or the Internet. Firewalls or VPN tunnel termination devices are installed at the edge of the customer network. Usually, premises based IP VPNs are developed based on IPsec (Internet Security Protocol) or SSL (Secure Sockets Layer) protocols (Cisco, 2004).

There are several market drivers and advantages of premises based IP VPNs (Rosenbaum, 2003).

1. **Advanced security features**: Both IPsec and SSL protocols ensure the confidentiality, integrity, and authenticity of the VPN traffic. Furthermore, it is possible to integrate additional security mechanisms such as firewalls, URL (Uniform Resource Locator) filtering, and virus scanning to premises based IP
VPNs. Hence, they provide the security features which are far beyond the features of a traditional IPSec or SSL connection.

2. **The global connectivity**: Premises based IP VPNs required only the broadband connectivity from the network operator. Literally, a simple Internet connection is enough to implement a premises based IP VPN service.

3. **Simple implementation**: The implementation of both IPsec and SSL is quite simple and a limited number of devices are required.

The market restraints of premises-based IP VPNs

1. **Lacking of interoperability**: There are various IPsec and SSL protocol versions available in the present IP networks. Especially, IPsec has imprecise standards. Thus, it is required to select compatible versions for implementation of a premises based IP VPN service.

2. **Lacking of scalability**: Both IPsec and SSL VPNs do not utilize any auto discovery mechanism. Also, it is not possible to utilize the provider’s auto discovery mechanism in premises based IP VPNs. Thus, the manual configuration is still required. Hence, the large scale premises based IP VPNs are highly complex to implement and maintain.

3. **The issue of lawful interception**: Authorize personals have right to intercept the communication data to investigate any communication that may threat to national security or support potential terrorist attacks. This process is known as the lawful interception. However, the lawful interception is not possible at the provider network for premises based IP VPN traffic since the customer data is encrypted. Therefore, some countries and service providers prevent the transfer of encrypted premises based IP VPNs data over their networks and gateways.

4. **Problems in QoS management**: Most of the QoS management schemes are based on layer 3 header attributes. The encryption of customer data prevents the access of layer 3 header information at the provider network. Thus, it is not possible to use QoS management mechanisms at the provider network for premises based IP VPNs.

5. **Higher VPN implementation and maintenance cost**: The customer has a higher capital cost since he has to implement and manage devices in the VPN network. Moreover, the customer needs technical staff to manage the VPN. On the other hand, the customer has to change his infrastructure including the VPN devices, each time he wants to tailor-made his VPN service.

**CELLULAR NETWORKS**

A cellular network or a mobile network is a radio network which provides wireless network services for mobile users. The radio network is consisted of cells. A cell is a small geographical area which is served by at least one base station. A base station is a fixed location transceiver which provides wireless connectivity for mobile users. These cells jointly provide the radio coverage over a wide geographical area. The cellular network allows a mobile user to make or receive network services from almost anywhere within its radio coverage. Furthermore, the user is receiving uninterrupted network services even while on the move within the radio coverage.

Initially, cellular networks were designed to provide only voice call services. However, these cellular networks have experienced rapid technological advancement during past three decades. Today, millions of people around the world are using mobile networks for various network services including voice call, video call, broadband access, multimedia, VPN and mobile cloud services. The
cellular network technologies have passed four generations.

- **The first generation (1G):** The first generation of cellular networks was operated based on analog telecommunication technologies. The first analog telecommunication standards were introduced in the 1980s. 1G telecommunication networks provided the connectivity speed up to 56 Kbps.

- **The second generation (2G):** The second generation of cellular networks was operated based on digital telecommunication technologies. In 1991, the first 2G cellular telecom networks were commercially launched on the GSM (Global System for Mobile Communications) standard in Finland. Digital TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access) technologies are used in the 2G telecommunication networks to increase the network capacity.

- **The third generation (3G):** The first 3G cellular telecom networks were commercially launched in South Korea in January 2002. 3G telecommunication networks provide the data transfer at a minimum speed of 200 Kbps. However, many 3G telecommunication networks provide higher speed than the minimum data transfer speed of a 3G service. These various 3G releases often denoted as 3.5G and 3.75G. They provide the mobile broadband access at a speed of several Mbps. Furthermore, 3G introduces various network applications such as wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV.

- **The fourth generation (4G):** The first 4G cellular telecom networks were commercially launched in the USA in 2008. A 4G system provides mobile ultra-broadband Internet access to laptops with USB (Universal Serial Bus) wireless modems, to smartphones, and to other mobile devices. The advance version of 4G networks is introduced as LTE in 2009. LTE cellular networks offer conceivable applications including amended mobile Web access, IP telephony, gaming services, high definition mobile TV, video conferencing, 3D television and cloud computing.

**Long Term Evolution (LTE)**

Long Term Evolution (LTE) is a wireless communication technology that allows operators to provide higher data rate and broadband connectivity than the previous 2G/3G network technologies. Even an earliest LTE network can offer very fast data speeds up to 100 Mbps in the downlink and 50 Mbps in the uplink. LTE is belonging to the fourth generation mobile networks which is marketed as 4G LTE. The overall objective for LTE is to provide an extremely high performance radio access technology that offers full vehicular speed mobility and that can readily coexist with earlier mobile networks. The first commercial LTE networks were launched by TeliaSonera in Norway and Sweden in December 2009. Since then, the LTE networks are becoming popular all around the globe. There were 119 commercial LTE networks in over 50 countries by November 2012.

**Integration of IP VPNs in LTE Networks**

The implementation of IP VPNs in cellular networks is not motivated until the availability of the IP based LTE mobile architectures. Especially, the architectural differences between the data network and the cellular networks prevent IP VPN implementations in earlier 2G/3G architectures. Initially, cellular networks provide only the network connectivity for IP VPNs. Mobile network operators did not participate in the service provisioning of VPNs. Later, mobile network operators were
interested to offer provider provisioned IP VPN services by actively participating in VPN service provisioning functionalities. They generated additional revenue by providing the IP VPNs as a Value Added Service (VAS) and it is the main motivation factor for them to offer provider provisioned VPN services (Shneyderman et al., 2000).

However, the deployment of IP VPNs in cellular network environment is not matured enough as wired IP VPN architectures. Only a very few number of mobile VPN architectures are proposed so far. Many IP VPN architectures for wired networks have been developed during past few decades. Many of these wired IP VPN architectures are properly implemented and keep using for a long period of time. However, it is not feasible to directly implement the existing wired IP VPN architectures in cellular networks. The availability of resources, network topology, data transmission media and behavior of end users are completely different in a cellular network environment. Thus, a cautious consideration on these factors is required while implementing IP VPNs in cellular networks. Several mobile IP VPN architectures are proposed by considering these factors (Shneyderman & Casati, 2003; Benenati et al., 2002; Feder et al., 2003). In this chapter, we investigate the feasibility of such proposals and possible applications based on these mobile IP VPN architectures. Furthermore, we present the adaptation efforts of existing wired IP VPN architectures into cellular networks.

APPLIEDS OF IP VPNS IN CELLULAR NETWORKS

IP VPNs can offer various services by integrating them with cellular networks. Since the LTE architecture is proposed an all-IP mobile architecture, this chapter mainly focuses only on LTE and beyond LTE cellular networks. On the other hand, it is the future of present telecommunication networks. Main applications of IP VPNs in LTE cellular network are as follows (see also Figure 3):

1. Service provisioning of conventional IP VPN services as a value added service.
2. IP VPN based backhaul traffic transportation architectures for LTE networks.
3. Securing the LTE backhaul traffic by using IP VPN techniques.
4. IP VPN based traffic architectures for Mobile Virtual Network Operators (MVNO).

Service Provisioning of Conventional IP VPN Services as a Value Added Services

The mobile Internet usage has increased during the past few years. Hence, service providers are eager to provide various services in addition to the traditional voice communication. The conventional VPN services over telecommunication networks or Mobile VPNs (MVPNs) are also newly embraced as a VAS by mobile network operators (Shneyderman & Casati, 2003; Benenati et al., 2002; Feder et al., 2003). They expand their role in VPN context from a simple connectivity provider to a VPN service provider.

The MVPN concept has fundamentally changed the method of communication and network access of a traditional VPN service. Especially, many of enterprises have road warriors who equipped with mobile devices. MVPNs provide a location independent connectivity for these road warriors to access the customer’s private network. Hence, the remote workers and road warriors can reach the private network regardless of the location and the time. Furthermore, MVPNs provide the seamless mobility for users. For instance, a customer can use the VPN services even while he is travelling in a high speed train or a bus. Moreover, mobile Internet tariffs are decreasing day by day. Hence, MVPNs are becoming an affordable and cost effective solution for users.

The architectural framework for MVPNs is defined in several research articles and standards. Furthermore, various forms of MVPNs are currently in (Shneyderman & Casati, 2003; Benenati et al., 2002; Feder et al., 2003). It is possible to
categorize these VPN implementations over the telecommunication networks into three categories based on the tunnel establishment mechanism; namely, end to end tunnel mode, network based tunnel mode and chained tunnel mode.

**End to End (E2E) Tunnel Mode MVPNs**

The E2E tunnel mode is considered as the most widely used VPN mode over the globe. In the E2E tunnel mode VPN scenario, remote user establishes a direct VPN connection to the customer private network by using the telecommunication network. The user can connect either a single device such as PDA (Personal Digital Assistant), laptop, smart phone or a complete customer network site by using a mobile communication capable CE device. The most of these VPN tunnels are IPsec tunnels. The administrative staff of the customer network is responsible to implement the security mechanism such as user authentication functions, access control mechanisms, firewalls and confidentiality protection schemes for these VPNs. Hence, E2E tunnel mode VPNs can be categorized as premises based VPN.

Figure 4 illustrates an end-to-end tunnel mode VPN over a LTE network.

The operation of an E2E tunnel mode VPN is as followed. First, the user device set up a dial up access connection over the telecommunication network to gain the Internet access. Then, it built a VPN tunnel (IPsec tunnel) with the VPN gateway which is residing at the customer private network by using this dial up connection. Hence, the part of the tunnel is built across the telecommunication network and the rest over the Internet. The mobile operator has no knowledge on the presence of these VPN tunnels. However, the tunnel establishment is temporal and it exists as long as the mobile user is connected to the Internet.
IP-Based Virtual Private Network Implementations in Future Cellular Networks

**Network-Based Tunnel Mode**

In the network-based tunnel mode scenario, the mobile operator is responsible for the establishment and maintenance of VPN tunnels. The customer assumes that the mobile operator has a network infrastructure with the intelligence and features to operate VPN services based on mutually exchanged SLAs (Figure 5).

In this scenario, VPN tunnels terminate at the entry point of the mobile network. Several tunnel establishment mechanisms such as IPsec, GRE (Generic Routing Encapsulation), MPLS can be used to establish these VPN tunnels. The operator and the customer exchange the VPN information and SLAs to establish the VPN service. Since the operator is responsible for the access control and the denial of unauthorized users, the customer has to trust the operator to provide the confidentiality of the private data.

**Chained Tunnel VPN**

The third type of VPN mode is the chained tunnel VPN. It establishes a VPN connectivity between the remote mobile user and the VPN gateway of customer network by using a set of concatenated tunnels (Figure 6).

There are many forms of chained tunnel VPNs. Similar to the network based VPN, operator builds a VPN tunnel between the border GW of the operator network and the customer network. This tunnel can be built by using various establishment mechanisms such as IPsec, GRE, MPLS. Then, the operator builds VPN tunnels within his mobile network to interconnect the remote mobile users. These tunnels have different forms and different expendabilities. The provider can deploy either a single tunnel or a set of concatenated tunnels within his network. On the other hand, these tunnels can be extended up to the mobile user device or only up to the base stations/eNodeBs. Furthermore, the operator can build some tunnels with foreign operators to facilitate the secure transmission for roaming users. These VPN tunnels within the operator network can be built by using different tunneling protocols such as GTP (GPRS Tunneling Protocol), IPsec, HIP (Host Identity Protocol).

**Traffic Transportation Architecture from LTE networks**

The virtual network based traffic transportation is also a major use case of virtual networks in telecommunication network domain. Two scenarios have been identified. Namely, transport models to transmit the traditional traffic over IP/Ethernet based networks during the migration phase and general backhaul traffic transportation architectures for LTE networks.
Virtual Network Based Transport Model to Transport the Traditional Traffic During the Migration Phase

The truly affordable broadband bandwidth from GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System) and HSDPA (High-Speed Downlink Packet Access) is saturating due to the rapid increment of the mobile broadband usage. Hence, all telecommunication operators have to migrate for the LTE and LTE-A (LTE Advanced) architectures to satisfy future demands. Ethernet based networks provide higher bandwidth and scalability which are necessary features to accommodate future evolutions. The LTE architecture proposes a new Ethernet based all-IP network infrastructure. Hence, operators have to build a new Ethernet based network infrastructures at the backhaul level (Ronai & Officer, 2009; Dahlman et al., 2011). However, the present GSM and UMTS networks are operating based on TDM (Time-division multiplexing) or ATM technologies and operators are not ready to abandon these network structure. Several market researchers predict that GSM networks will remain at least until 2020 (Croy, 2011).

On the other hand, it is not feasible to manage multiple backhaul traffic technologies such as TDM, ATM and Ethernet over a single operator network due to high operating costs and compatibility issues. Thus, operators are trying to converge all backhaul traffic into single traffic model.

Several solutions are proposed to achieve this goal. One possible solution is to tunnel the traditional TDM or ATM services over a virtual network...
which overlays on an Ethernet based network. Here, all the GSM (TDM) and UMTS (ATM) traffics transport over an IP-based infrastructure without changing the existing radio equipments at the access network. This can be considered as a part of a long-term strategy towards an all-IP infrastructure. Different VPN technologies are designed for this purpose, namely TDM over MPLS such as Structure Agnostic TDM over Packet (SAToP), Circuit Emulation Service over Packet Switched Network (CESoPSN) and ATM over MPLS such as ATM Pseudowire Emulation Edge-to-Edge (Alvarez et al., 2011; Cisco, 2010). Both L2VPN and L3VPN architectures are feasible to implement. However, the architectural choices will depend on the protocol stack of intermediate nodes in the underlay operator network.

Figure 7 illustrates the deployment and the protocol stack of L2/ L3 VPN architectures which tunnel the conventional traffic over an all-IP-based LTE network.

Initially, operators needed point-to-point connections from cell site routers to controllers such as RNC (Radio Network Controller), BSC (Base Station Controllers). Hence, the E-line (Ethernet pseudowire) is preferred as the L2VPN architecture. Later, E-tree (point-to-multipoint) and E-LAN (multipoint-to-multipoint) services are also acquired to provide the redundancy and scalability. However, these L2VPN solutions have complex operational features and less flexibility on controlling. The complexity of operation is directly proportional to the level of redundancy support and the scalability.

Due to these reasons, operators are motivated to deploy L3VPNs such as MPLS based 2457bis VPNs. These L3VPNs provide various advantages including higher scalability, simpler integration, less operational complexity, better resilience and redundancy. Hence, L3VPN is the preferred choice of implementation for most of operators.

Virtual Network Based Backhaul Traffic Transportation Architectures for LTE Network

The LTE architecture proposed a whole new architecture for telecommunication networks.
Especially, it proposed to use an all-IP based flat backhaul network architecture. Also it defined several new interfaces such as S1, X2 to enhance the performance of the traffic transportation. Furthermore, the flat architecture concept proposes to distribute the centralized controlling entities across the network to optimize the controlling functions.

On the other hand, the traffic architecture is well defined in LTE architecture. It proposed several traffic types namely, S1-U for the user traffic between eNodeBs and the S-GW (Service Gateway), S1-C for the control traffic between the eNodeBs and the MME (Mobility Management Entity), X2-u and X2-c for the traffic between eNodeBs, OSS (Operations Support System) traffic to provide fault, configuration, and performance management and the network synchronization traffic (Alvarez et al., 2011). However, these traffic classes have different operational, controlling and QoS requirements. It is challenging to satisfy these individual requirements in a shared network infrastructure. A VPN based traffic architecture is an ideal solution to provide different levels of services for these different traffic types.

Several VPN based traffic architectures are proposed for LTE backhaul networks (Liyanage & Gurtov, 2012; Cisco 2010; Alvarez et al., 2011; UTStarcom, 2009). These architectures can be categorized into two types based on traffic separation options for VPNs. In the first scenario, the backhaul traffic is divided into two VPNs. One VPN is carrying the traffic between the eNodeBs and core network elements. Several interfaces such as S1-U and S1-C, belong to this VPN. The other VPN is carrying the traffic between eNodeBs. Several interfaces such as X1-U, X1-C belong to later VPN. In second scenario, each backhaul traffic class is divided into a separate VPN. In other terms, each interface has a separate VPN. The first scenario is preferred by the operators due to the lesser operational complexity (Cisco, 2010). In contrast, VPN based traffic architectures again categorize in to two types based on operational network layer. It depends on the underlay network infrastructure. Generally, intermediate routers in LTE backhaul networks support either layer 2 or layer 3 protocols. Therefore, it is possible to implement these VPN-based traffic architectures as L2VPNs or L3VPNs.

Layer 2 VPN Model for LTE/EPC Deployments

The L2VPN traffic architecture is proposed for LTE networks which have layer 2 network nodes. Figure 8 illustrates the deployment and the proto-

![Figure 8. The deployment and the protocol stack of L2VPN traffic architecture for a LTE backhaul network](image-url)
col stack of L2VPN traffic architecture for a LTE backhaul network.

There are two VPNs in Figure 8. VPN1 transmits the X2 traffic and VPN2 transmits the traffic for core applications. VPN1 requires multipoint to multipoint connectivity as eNodeBs are mesh connected in LTE architecture. Hence, VPLS is the preferred VPN technology for VPN1. Furthermore, this VPN can span until several nodes such as pre-aggregation nodes, aggregation nodes, distribution nodes or control elements. VPN2 requires point to point connectivity to transfer the traffic for core network elements. Hence, VPWS is the preferred VPN technology for VPN2.

The L2VPN model has several advantages. L2VPN architectures have a low implementation cost. Furthermore, they can support multiple layer 3 protocols as the implementation is independent of layer 3 protocols. However, L2VPN model has several disadvantages as well. L2VPNs can result for larger broadcast domains at the backhaul network and it may cause to DoS (Denial of Service) and DDoS (Distributed DoS) attacks. Hence, L2VPNs are lacking of scalability. Also, it is not possible to implement higher layer security mechanisms such as IPsec in L2VPNs as IPsec need layer 3 equipments at end nodes of tunnels. Moreover, eNodeB authentication mechanisms such as 802.1x have some incompatibility issues with layer 2 network attributes. The layer 2 attributes based traffic separation is also not efficient. Due to these reasons, L2VPN techniques are not mature and globally ubiquitous as L3 techniques.

Layer 3 MPLS VPN Model for LTE/EPC Deployments

L3VPN traffic architecture is proposed for LTE networks which have layer 3 network nodes. Figure 9 illustrates the deployment and the protocol stack of L3VPN traffic architecture for a LTE backhaul network.

VPN1 transmits the X2 traffic and VPN2 transmits the traffic for core applications. MPLS based 2547bis VPN is the preferred VPN architecture for both VPNs. It is possible to use the same VPN technology for both VPNs as MPLS VPNs provides both point to point and multipoint to multipoint connectivity.

L3VPN model has several advantages. L3VPN architecture is flexible and it can be modified with a minimum effort. For instance, the upper layer

Figure 9. The deployment and the protocol stack of L3VPN traffic architecture for a LTE backhaul network
security mechanisms such as IPSec tunnels can be implemented without modifying the intermediate nodes. Furthermore, the use of a single VPN technology for all VPN instances is reducing the operational cost and the complexity of the architecture. Moreover, the traffic separation and QoS management are managed based on L3 attributes. L3VPN technologies are efficient, matured and globally ubiquitous than L2 techniques. However, there are some issues which are associated with L3VPNs. The L3VPN model cannot be used for a LTE backhaul network with layer 2 nodes. Besides, MPLS based L3VPNs have higher implementation cost than L2VPN technologies.

Virtual Network based Secure Architectures for LTE Network

LTE networks confront several security threats which do not exist in 2G/3G networks. These treats can be originated in different segments such as customer nodes, backhaul network, customer provider interface network and core network (Liyanage & Gurtov, 2012; Alvarez et al., 2011; Alvarez et al., 2012). Hence, 3GPP has defined several security requirements such as user authentication and authorization, payload encryption, privacy protection and IP based attack protection to prevent these security threats (Alvarez et al., 2011; Alvarez et al., 2012). It is necessary to implement segment specific security functions for each segments of the transport network to protect the LTE network. VPN based traffic architectures are promising solution to provide the required level of security for the LTE backhaul network segment.

Three main reasons have identified for security threats in the LTE backhaul network (Alvarez et al., 2011; Alvarez et al., 2012).

First, the LTE architecture proposed all-IP network architecture. Hence, the LTE backhaul network also consists of the IP-based entities such as MME, SGW, eNodeBs and IP based interfaces such as X2, S1. Thus, the backhaul network is now vulnerable to IP based attacks. Also, it is possible to destruct important core elements and gateways directly by compromising nodes in the access network.

Second, the LTE backhaul network has hundreds or thousands of end nodes (e.g. eNodeBs). Hence, an attacker has multiple places to mount an attack to the backhaul network. On the other hand, the flat architecture concept distributes the control functionality over the backhaul nodes. Therefore, an attack on a single node can cause a significant damage in the network.

Third, all the traffic which are transferred through the access and the aggregation networks, are unencrypted in LTE networks. In the previous mobile network architectures such as GSM and UMTS, these traffic were encrypted by radio network layer protocols. However, these radio network layer protocol based encryptions are terminated at the eNodeBs in the LTE architecture. Hence, the backhaul traffic is vulnerable to common security threats such as eavesdropping and man in middle attacks.

Several VPN based secure traffic architectures are proposed to avoid these security threats. Most of these architectures are based on IPsec VPNs (Liyanage & Gurtov, 2012; Alvarez et al., 2011; Alvarez et al., 2012). Figure 10 illustrates a deployment and the protocol stack of IPsec based L3VPN architectures for LTE backhaul network (Liyanage & Gurtov, 2012).

Two modes of IPsec tunnels can be used to develop secure traffic architectures, namely IPsec tunnel mode and IPsec BEET (Bound End-to-End Tunnel) mode (Liyanage & Gurtov, 2012). Both of these architectures have similar properties as previously described L3VPN traffic transportation architecture. The IPsec tunnel mode VPN architecture is built by using Internet Key exchange version 2 (IKEv2) Mobility and Multihoming Protocol (MOBIKE) and the IPsec BEET mode VPN architecture is built by using Host Identity Protocol (HIP). Both architectures fulfill the 3GPP security requirements for the LTE backhaul network and provide additional features such as load
balancing, automatic redundancy, the best path routing in a meshed backhaul network.

**Mobile Virtual Network Operator (MVNO)**

A MVNO is a mobile network service provider who operates his network over a leased telecommunication network. A MVNO obtains bulk access to network services such as radio spectrum, backhaul nodes, network controllers at wholesale rates based on the business agreement with a physical mobile network operator. Then, MVNO uses these leased resources to provide his own operator network. From a customer point of view, there is no difference between the services provided by a MVNO versus a traditional operator. Hence, the MVNO concept is becoming popular across the globe. The first MVNO was created by Tele2 in Denmark, and subsequently rolled out in several European markets. There are 633 active MVNO operations worldwide by October 2012 (MVNO, 2012).

The deployment of the MVNO concept in various countries varied based on different factors. In some countries, the regulatory intervention is the key reason to adapt the MVNO concept for mobile networks. These regulatory interventions are forced to mobile network operators to offer wholesale access to their network to ensure robust competition and provide benefits to the consumer. However, the most of mobile network operators adapt the MVNO concept to sell their excess capacity at wholesale rates to other entities in an effort to bring an incremental revenue which otherwise be regarded as unused network capacity.

The different types of MVNOs are present around the globe. They are categorized based on their participation for each function of the value chain. There are three main types (see also Figure 11) (Balon & Liau, 2012).

1. **Branded Reseller:** The branded reseller is the lightest MVNO business model. The MVNO just operates its brand and distribution channels. The host mobile network operator operates all other functionalities of the network. The branded reseller model requires the lowest investment for a new MVNO. Therefore it is the fastest MVNO type to implement.
2. **Full-MVNO:** The full-MVNO is the most complete MVNO model. Here, the host mobile network operator just provides the
IP-Based Virtual Private Network Implementations in Future Cellular Networks

access network infrastructure. The MVNO operates the rest of functionalities of the network. The full-MVNO model is typically adopted by telecom players who wish to obtain all most all the control functionalities of their network.

3. **Light-MVNO:** The light-MVNO is an intermediate type in between a branded reseller and a full-MVNO. Light-MVNO allows the MVNO to take control over some of the back-office processes and control functionalities while having the full control of the marketing and sales areas. The MVNO can adapt his responsibilities according to his requirement.

Virtual private networks play a special role in a MVNO context. A MVNO itself can be considered as a special kind of VPN customer of the host network operator. A large scale host operator can simultaneously support several MVNOs by selling his network resources. Thus, a secure virtual network architecture is a promising solution to provide traffic separation, bandwidth allocation and privacy protection for these MVNOs. The existing VPN architectures are proposed only for traffic separation. However, primary operators need VPN architectures that not only separate the traffic but also slice the resources at network elements.

On the other hand, a MVNO also provides the traditional VPN services for his customers. Technically, it builds VPNs over another VPN. However, this dual VPN encapsulation wastes the scarce radio bandwidth and increases the operational cost. Hence, it is interesting to discover the novel VPN architectures to avoid these dual VPN encapsulations.

**FUTURE TRENDS OF IP VIRTUAL PRIVATE NETWORKS**

The future of IP VPNs in the telecommunication domain is not easy to predict due to the influence of numerous factors. Especially, VPN architectures and services in telecommunication networks are not stably deployed and widely used to predict a steady future. However, we identified several applications which may be interested in the future.

**The Convergence Different Wireless Technologies**

The LTE architecture proposes to integrate different wireless packet data technologies and systems such as Wireless Local Area Network (WLAN), GPRS, UMTS, CDMA (Code Division Multiple Access) with LTE networks. For instance, the convergence of WLAN with LTE...
systems provides better broadband services. WLAN has a far superior throughput rates than telecommunication networks. Hence, mobile user can achieve a higher throughput by offloading the user traffic to WLAN. On the other hand, WLAN has a cheap connection fee. Furthermore, WLAN equipments are significantly less expensive than telecommunication nodes and they are easy to install and maintain. These factors cause to achieve a significant economic advantage for operators. However, existing VPN architectures have to consider the impact of such a network convergence and modify them accordingly.

**Mobile Cloud Services**

Cloud computing and cloud based services are becoming popular among present communication networks. The main concept of a cloud service is to outsource the computing and storage functions to the service provider. Cloud service users can use mainframe resources which are located at the various places in a network (Sosinsky, 2010). The integration of the cloud computing with mobile devices or mobile cloud computing is accomplished due to the tremendous development of the mobile broadband services. The deployment of mobile cloud computing provides different advantages such as higher scalability, lower overall costs, higher computation power and more storage facility to mobile users. Furthermore, cloud base security is also achievable as a mobile cloud service. Here, the mobile user offloads complex security functions from the device to a virtualized cloud infrastructure. However, mobile cloud computing is still new to the telecommunication domain. There are many scalability and compatibility issues which need to be tackled before worldwide implementations.

The security is considered as a key requirement of a mobile cloud service. Cloud service providers can secure data communication to some extent. However, customers cannot rely only on service providers to provide the privacy, integrity and confidentiality for their private data. VPN based security architectures are promising solutions to solve these issues. While service providers interconnect the customer network with the rest of the world, well advanced and matured VPN security precautions protect the private data from third party users. However, VPN architectures to secure mobile cloud services are not implemented yet. On the other hand, it is possible to define a generalized virtual network platform on top of a telecommunication network. It will provide secure communication not only for mobile clouds but also other network services such as mobile P2P (Peer-to-Peer), multicast services.

**Software Defined Networking (SDN) based Network Virtualization**

As a result of increasing demand in data and the increase in the number of base stations over the telecommunication networks, the backhaul network will face congestion, in a manner similar to data center networks. In order to overcome this problem, Software Defined Networking (SDN) is a very promising solution. Initially, SDN has been defined only for fixed networks (McKeown, 2009). SDN separates the control plane from the data plane in network switches and routers.

Although, the widely discussed marketing applications in SDN is consolidated data centers, the basics of SDN could be extended to any application. These extensions also mean that SDN based network virtualization is applicable in telecommunication network. Several recent research projects (MEVICO, 2010; SIGMONA, 2013) are focused on these aspects. Hence, it is important to study the implementation aspect of IP VPNs in SDN based telecommunication network.

**Person-to-Machine Services**

Initially, telecommunication networks are used only for person-to-person services such as voice call and text message services. However, the recent
IP-Based Virtual Private Network Implementations in Future Cellular Networks

Evolution of telecommunication networks inspires to provide person-to-machine services such as dynamic traffic condition reports, interactive voice response systems, interactive short message systems, online navigation systems. These person-to-machine services are well integrated with the present human life style. It is expecting that the service usage will be increased in the future. Present, virtual networks are playing a vital role in person-to-machine services in wired Internet environment to avoid the unauthorized access, enforce service exclusivity and protect against IP based attacks. Some of these VPN architectures might be applicable up to certain extend in the telecommunication networks. However, it will be interesting to implement novel IP VPN architectures to protect the person-to-machine services over the telecommunication networks.

Conclusion

Virtual private networks are widely used in wide area networks to securely interconnect geographically distributed customer sites through public networks. On the other hand, the tremendous development of the telecommunication technologies causes to increase the number of mobile subscribers and provide almost the same level of broadband services as wired networks. Hence, corporate customers are motivated to use telecommunication networks to obtain the broadband access and it fuels implementations of the IP VPNs on top of the cellular networks.

This chapter contains an extensive survey on these IP VPN implementations in the cellular network domain. In the beginning, we described the history, the evolvement and the classification of VPNs. We identified four main applications of virtual networks in the telecommunication domain; namely mobile VPN services, VPN based traffic transportation models for LTE networks, secure backhaul traffic transportation of telecommunication network and Mobile Virtual Network Operators (MVNO). Finally, we discussed the future trends of virtual networks in telecommunication network context; namely, mobile cloud services, mobile person-to-machine services and Software Defined Networking (SDN) based network virtualization. Hence, we can conclude that the integration of IP VPN technologies with telecommunication networks is a highly demanded requirement and it is a timely context to conduct extensive research works.

References


IP-Based Virtual Private Network Implementations in Future Cellular Networks


**ADDITIONAL READING**


KEY TERMS AND DEFINITIONS

**Cellular Network**: A radio network that provides wireless network services for mobile users.

**LTE (Long Term Evaluation)**: A telecommunication standard for wireless communication of high speed data for mobile phones and data terminals.

**Mobile**: A device, user, technology, or service that has the ability to move or be moved.

**MVPN (Mobile Virtual Private Network)**: A virtualization mechanism that allows mobile devices to access network resources on their home/private network, when they connect via other public mobile networks.

**Telecommunication**: Long distance communication by using technological means such as electrical signals or electromagnetic waves.

**VPN (Virtual Private Network)**: A virtualization mechanism to extend a private network across a public network, such as the Internet.