Part V

Security and Economic Aspects

17

Software Defined Mobile Network Security

Ahmed Bux Abro
VMware, Palo Alto, CA, USA

17.1 Introduction

Telecommunication has transformed rapidly into Infocommunication [1] in a short period and has forced us to digitalize our life and further derived changes for how we communicate, entertain, work, and socialize with other human beings.

This transformation to digital life has brought many opportunities as well as offers great challenges for how to protect our valued data, keep our privacy, and secure our Infocommunication networks that are used to provide access to billions of users, devices, and things. Cyberattackers have frequently challenged the telecommunication industry and put company's reputation at risk. Increased use of mobile data has also introduced new security challenges and threat vectors.

Enhanced visibility, intelligence, and network wide control are required to protect from such threats while making sure mobile services are not compromised and always on.

Available vulnerabilities in an all-Internet-Protocol (IP)-based mobile network have made it easy for the attackers to use it as an attack Launchpad. Traditional security models were used to apply security on selected domains and place in the network (PIN) while keeping the rest of the network wide open.

Software defined mobile network (SDMN) has the potential to leverage the network as a tool to provide enhanced visibility, converged intelligence, centralized policy control, and real-time threat mitigation. Traditional security models may not address the needs for SDMN and the next generation of the mobile network. We need to think out of the box by leaving bolt-on security model and develop an inclusive and intrinsic security model across the mobile network.

Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture, First Edition.
Edited by Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila.

17.2 Evolving Threat Landscape for Mobile Networks

Phone hacking (also called as phreaking) was first spotted somewhere between the 1960s and 1970s when phreakers demonstrated their skills to manipulate the functions of a telephone network. Methods to attack telecommunication systems had evolved since then and have changed its shapes from war dialers to viruses, to worms, and to modern-day advance persistent threats (APTs). Tools to protect our telecommunication systems have also evolved from physical access control to antivirus to modern application and context-aware firewalls.

Increased use of smartphones for data services and applications has exposed these devices to the same security threats that were once known and dedicated to personal computers (PCs). Mobile devices have replaced legacy system and have changed our ways to learn, work, entertain, shop, and travel. Bring your own device (BYOD) and cloud technologies have further diminished the enterprise boundaries and often challenged security experts to work out-of-the-box strategies.

Motivations for attacking networks have also changed from fun-loving immature script kiddies to organized cybercrime rings and hacktivists with clear political and financial objectives. In this age of digitalization, after connecting humans using the Internet and mobile, we are talking about connecting things and machines. Mobile has not yet completely replaced the PC but has become an ideal place where personal information can be found for nefarious use.

Security needs to be architected to not only protect from the current threats but to address the increased and evolving threat landscape. Adequate security should include threat intelligence, visibility, and real-time protection.

17.3 Traditional Ways to Cope with Security Threats in Mobile Networks

Mobile network has always been the target for security attacks. Legacy techniques to protect mobile networks from ongoing security threats are nothing but introducing new and unplanned security control for selected network segments, focusing perimeter security while leaving inside networks wide open, and finally building complex security systems that later cause impact to overall network operations and performance.

These techniques on one side were able to address selected threats but proved to be less efficient for new and advance threats where hackers follow a systematic and collaborative approach. The following figure demonstrate an ongoing attack or an attack vector that can consist of multiple attacks and what traditional security tools are used by a security admin to protect the mobile network. We can see how a collaborative attack can cause a network wide impact, while the security tools placed for selected PINs can be limited and less efficient to protect the network.

Let us review some of these legacy security tools and techniques that are applied in mobile network today (Fig. 17.1).

17.3.1 Introducing New Controls

Security is often deployed in a reactive manner. Separate security controls are deployed on various PINs to protect the mobile network and its services. Mobile network security includes various security controls such as firewalls, packet filters, network address translation (NAT),

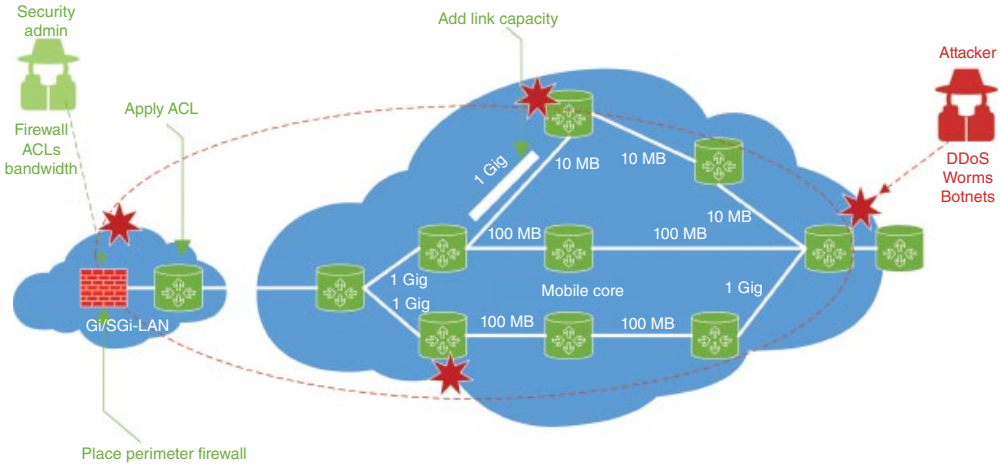

Figure 17.1 Mobile IP Core and Gi/SGi Network attack simulation and response.

packet inspections, antivirus, etc. Managing such controls remains a challenge and requires expensive technical resource involvement.

Most of the security controls are placed in a distributed fashion with a limited territory to protect. One of the major drawbacks of these security controls is that they all work in silos and offer close to none collaboration. A holistic and centralized control system is hard to imagine in today's mobile networks.

Software defined network (SDN) technology centralizes the network control plane and signaling using "controller" software. The controller sits in a central place and all network nodes communicate with and share network state and flow information with that controller. The SDN model also offers centralized policy and visibility to the entire network.

17.3.2 Securing Perimeter

Perimeter is an edge or a boundary where a mobile network can interface with an external network that can be another mobile or data network. Security for a mobile network has been most of the time heavily focused around securing the perimeter as it has been considered the most vulnerable point of the network. Access control is the major security tool to protect the mobile network perimeter. Perimeter security has traditionally been applied by placing network firewalls or packet filters that use IP address and protocol information to filter access to network. Perimeter firewalls or packet filters are usually placed on SGi and S8 (partner facing) interfaces.

Firewalls have served decades as the preferred technology to protect against network attacks on the perimeter and inside networks, but we have seen this technology as limited against the new era of coordinated and advance persistent threats.

Firewalls have proved to be successful in controlling traffic and protecting from certain network attacks, but it brings its own limitations, such as limited visibility and point protection.

Debate can go on and on for firewalls and their effective role in the modern Infocommunication world with evolving cyberthreats. It is still an effective tool to apply access control on the perimeter, but we definitely need more than that. What is needed is an advance, intelligent, and collaborative security system to detect, protect, and mitigate new threats inside and on the network perimeters.

17.3.3 Building Complex Security Systems

Building an effective as well as simple security system in a mobile network has remained a dream by many telecommunication security experts. Like mobile networks, security has also been applied in an evolving method and introduced to the network on as-needed basis. As we cannot predict how exactly we will be communicating after 25 years or how will our telecommunication networks look like, so is the case with mobile network security. We did not imagine that mobile network security will be facing IP packet-based network attacks in once time-division multiplexing (TDM)-based circuit-switched networks.

Some of the major factors driving complex security systems in telecommunication networks are:

- Interworking of various legacy (2G, 2.5G, and 3G) and new Long-Term Evolution (LTE) systems
- Convergence of voice, video, data, and other services
- Evolution of IP end-to-end network.

17.3.4 Throwing More Bandwidth

IP Core of the mobile network is used to provide faster backbone access between Evolved Packet Core (EPC) and other mobile network segments. One of the many schools of thoughts for security experts follows the strategy to keep the IP Core network clear from any security technology as this may impact the speed to delivery packets. We will not go into a debate on which school is better, but we will discuss the possible impact of one approach over the other.

The traditional method used by the operators to protect the core of the mobile network (also called mobile core) was to oversize the network capacity and overpopulate the resources to avoid services disruption.

That technique had proved successful in some situations, but it had its own drawbacks from a cost perspective and proved to be a short-term resolution.

17.4 Principles of Adequate Security for Mobile Network

Mobile networks need to adopt a security model that is not just based out of the common confidentiality, integrity, and availability (CIA) triad but also extended to address new security principles for centralized policy and enhanced visibility to offer better security and protect customer data (Fig. 17.2).

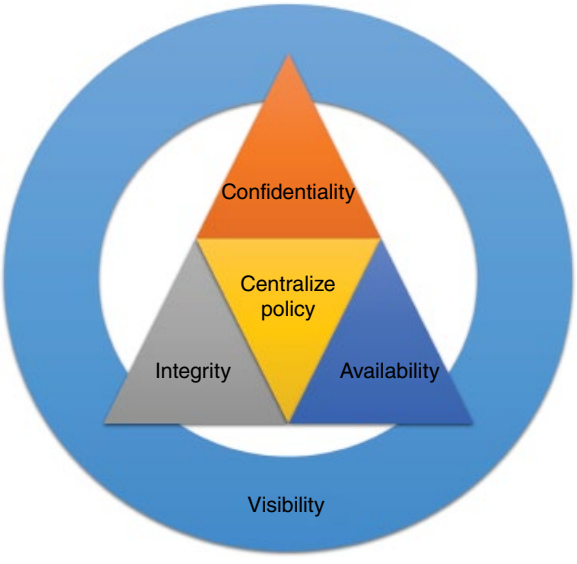

Figure 17.2 Mobile network security model.

17.4.1 Confidentiality

Confidentiality is to make sure that the least privileges are assigned and access is controlled for authorized applications and clients while denying any unauthorized access request. Principle needs to be equally applied on northbound and southbound traffic.

17.4.2 Integrity

It is critical to ensure that the information is not tempered and removed and remains integrated while transferred between different points inside the mobile network. Network can be compromised and data integrity can be lost if required security controls are not implemented on each layer.

17.4.3 Availability

Availability principle assures that the network components, services, and information are available as and when needed. Most of the mobile network offers service-level agreement (SLA) with 99.999% availability. Attacks such as distributed denial of service (DDoS) can cause damage to services and limited services for legitimate mobile users.

17.4.4 Centralized Policy

Centralized policy management and enforcement make it easy to control access to the network resources, services, and applications. It also helps to organize, manage, and associate security policies in a central location.

17.4.5 Visibility

Mobile networks need end-to-end visibility to the network control plane to monitor, optimize, and better troubleshoot network issues. Visibility not only helps secure the environment but also profile traffic to offer new services, plan network capacity, and introduce analytical capabilities. SDN-based model provides global visibility across all base stations.

17.5 Typical Security Architecture for Mobile Networks

Mobile networks with evolution to LTE technology have been transformed and built on all-IP-based network architecture that means IP end to end from radio access network (RAN) to core to data center. Having a flat architecture simplifies the mobile network but at the risk of increased vulnerabilities and threats. A flat architecture introduces challenges to design an effective security defense in depth model that can offer necessary fault isolation as well as protect the interwork of legacy and non-3rd Generation Partnership Project (3GPP) networks.

Mobile operators are accustomed to the traditional way to design security in a reactive manner by having separate security controls for RAN, aggregation (back haul), core, and data center.

3GPP has defined a security architecture that covers security features, mechanisms, and procedures for Evolved Packet System (EPS), EPC, and E-UTRAN. A detailed document for that security architecture can be found in the Refs. [2, 3]. Mobile network operators use this architecture to build a security layer around the access network, EPS/EPC, user authentication, application security, and finally security configuration.

The 3GPP security architecture (Fig. 17.3) is divided into five domains as below.

- Network Access Security (I): Defines security for users using USIM to securely access EPC resources and further protect RAN against various attacks
- Network Domain Security (II): Provides security features to offer secure communication over a wired network between different EPC nodes to protect user and signaling data

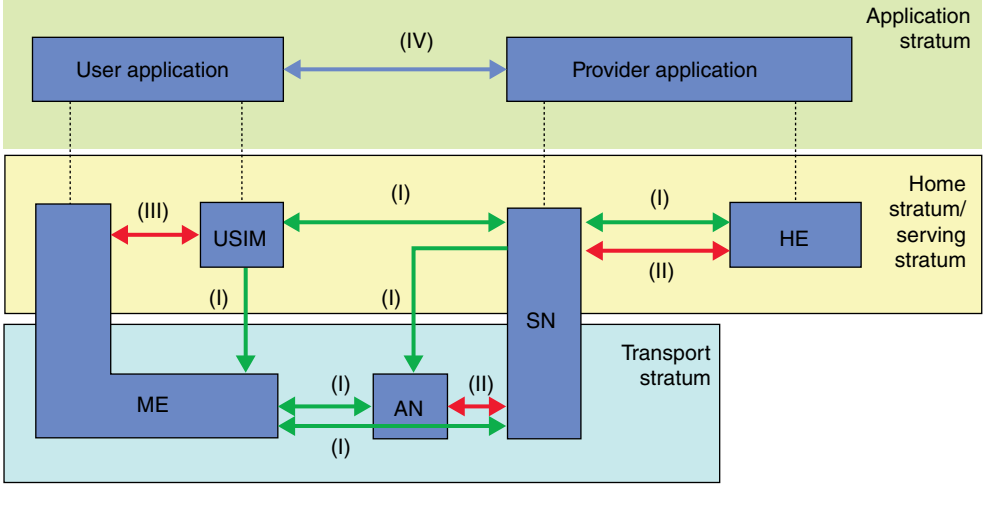

Figure 17.3 3GPP security architecture.

- User Domain Security (III): Covers the mutual authentication between a user equipment (UE) using USIM and mobile equipment (ME)
- Application Domain Security (IV): Includes necessary security features to protect user and provider application communication with the rest of the network
- Visibility and Configurability of Security (V): Offers users the visibility to their current security posture.

The 3GPP architecture covers security for different network types such as RAN and EPC network, secure communication for inter- and intranetwork nodes, and security for various interfaces (S1, S8, SGi, etc.) Inside mobile network is usually categorized into three domains:

- S1 Interface Security: To protect RAN-to-EPC communication
- SGi Interface Security: To protect the Internet facing links and interfaces
- S8 Security: To protect partner facing interface for secure roaming.

Various security controls are applied in this architecture to secure these interfaces (Fig. 17.4). The following figure maps the security controls with different PINs.

As seen in the above figure, security controls to protect these interface types are usually based on:

- Firewalls: Separate interface-specific firewall is installed for each domain, that is, S1 firewall installed between RAN and EPC to protect GPRS Tunneling Protocol (GTP) communication, a Gi firewall deployed near the Internet border to protect from Internet threats, and S8 firewall installed to protect communication with the roaming partners.
- Authentication and Authorization: Strong authentication and authorization are applied for the S1 interface to ensure only authorized evolved nodeB (eNB) is allowed access to the packet core network. Authentication and key management area has been well addressed by 3GPP by incorporating Authentication and Key Agreement (AKA). AKA offers mutual authentication along with integrity protection. Its variations are used to authenticate trusted non-3GPP clients. For trusted non-3GPP access, Extensible Authentication Protocol AKA (EAP-AKA) can be used for authentication.
- Encryption/IPSec: Encryption is applied to protect RAN-to-EPC communication and to ensure the network is protected from rogue and insecure eNBs.
- NAT: This is used to hide network core addresses while interfacing with the outside and partner world.
- Malware and Antivirus Protection: This is used to protect the network from viruses, worms, and other threats.

The abovementioned typical security architecture and security controls offers its own security benefits but has some limitations as well:

17.5.1 Pros

- Domain-specific security
- Strong authentication for UE
- Protects vulnerable points in the network.

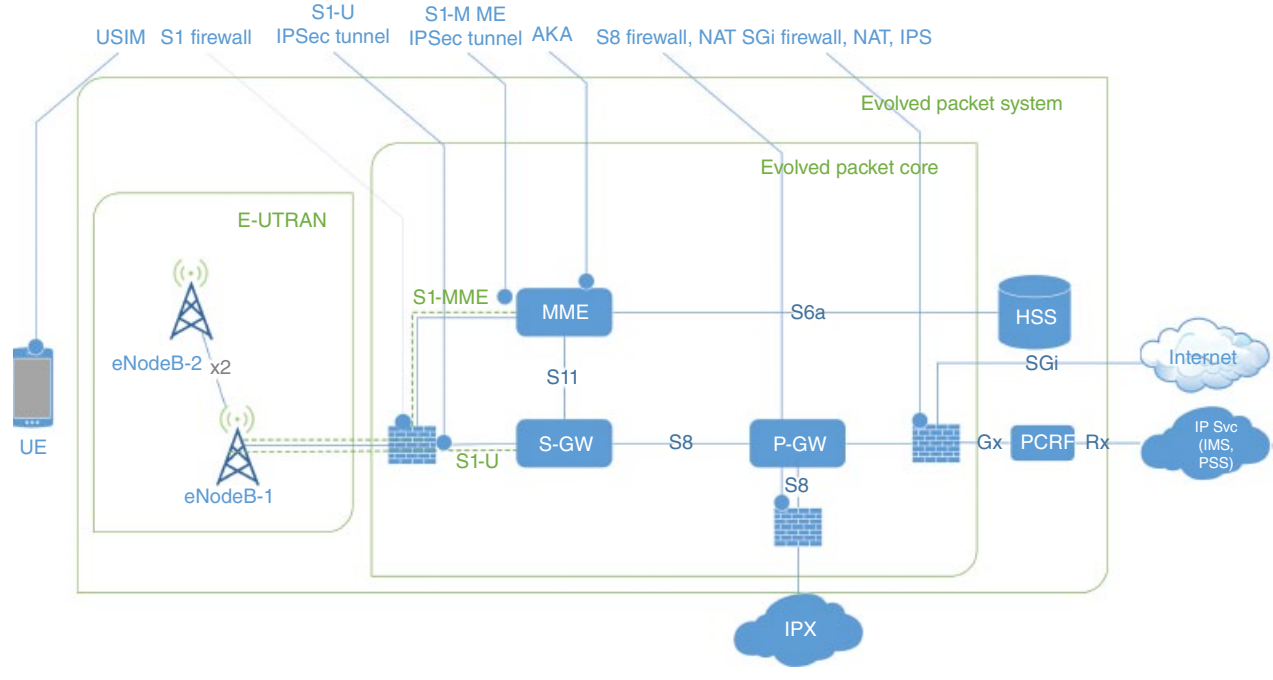

Figure 17.4 Typical security architecture for mobile network.

17.5.2 Cons

- Complex and fragmented security model
- Limited visibility
- Decentralize control
- Distributed security
- Lack of collaborative security model.

17.6 Enhanced Security for SDMN

An all-IP-based mobile network architecture has exposed us to new IP-centric threats on all layers of a mobile network. Threats such as IP spoofing, man-in-the-middle attack, and DoS have increased probability of attack success in this new environment.

At the time of the writing of this book, SDN is not fully embraced by the major telecommunication operators, but we are seeing a trend toward SDN and we also witness telecommunication operators starting to adopt cloud, orchestration, and virtualization technologies that are enablers for SDMN. SDN standardization organizations such as the Open Network Foundation (ONF) have dedicated groups for wireless and mobile network that are actively working on SDMN use cases and standards.

A traditional security model may not work with SDMN and may require consideration of an integrated security architecture. Security should not be restricted to selected components but should be equally applied to all layers of an SDMN architecture such as infrastructure, SDN, management, orchestration, automation, and applications.

A security architectural approach for SDMN will help gain better visibility and control. Security for individual layers is discussed in the following sections.

17.6.1 Securing SDN Controller

The SDN controller is an important component of the SDMN architecture and requires necessary security hardening to protect it from any threat that can affect its availability. Hackers can leverage its position of the central control and visibility for their nefarious objectives. Gaining unauthorized access to control can enable hacker to manipulate network functions, capture packets, divert traffic, and misuse the network functions.

A controller is usually installed on the top of an operating system (OS) platform such as Linux. Like any other OS, we can harden the underlying OS for the controller by installing necessary patches and fixes, enabling role-based access control (RBAC), enabling accounting and logging, and disabling unnecessary services, ports, and protocols.

A controller software usually ships with basic security management protocols such as SSH, HTTPS, and a proper RBAC to manage controller resources.

17.6.2 Securing Infrastructure/Data Center

SDMN separates the control and data plane. The control plane is centralized in a controller software, while the data plane resides on hardware devices such as Serving Gateway (S-GW) and PDN Gateway (P-GW) or network components such as routers and switches. Depending

on what SDN model (basic SDN, hybrid SDN, or full SDN) is used in the environment, necessary security controls can be enabled on the infrastructure devices that are controlled by the SDN. It is common to keep the management plane and data plane function on the device, while the control plane function can be placed on box or off box per the SDN model.

Security controls for infrastructure supporting SDMN include authentication, authorization, and accounting (AAA), secure management protocols, logging, and monitoring controls. Data plane-specific security controls such as port security, access control lists, and private VLANs can be enabled to protect the data plane.

17.6.3 Application Security

SDMN offers an open interface for software applications to call or manage different control plane functions; such interfaces are called Application Programming Interfaces (APIs).

It is required to ensure that applications accessing the SDMN environment are authenticated using a digitally signed code and certification process. Such applications should be developed following secure application development lifecycle and principles of least privilege and fail safe and tested against possible threats such as buffer overflow and resource leakage. A code analysis is performed to ensure applications are secure.

17.6.4 Securing Management and Orchestration

Management and orchestration are the key components of the SDMN architecture, and it is required to apply necessary security controls to protect these components. It is preferred to put management and orchestration in a secure zone that is protected by a firewall and a proper role RBAC system is in place to ensure least privilege and access to authorize users and to monitor and account activities.

17.6.5 Securing API and Communication

As discussed previously, SDMN offers an open interface for applications to call or manage control plane functions; such interface is also called as an API. Access to an API needs to be properly authenticated and authorized. API access also needs to be monitored and revoked as needed. Encryption is required when an open communication channel is used to send and receive API access requests.

17.6.6 Security Technologies

The SDMN environment can be further protected through physical or virtual security technologies such as firewalls, security gateways, deep packet inspections, and intrusion prevention systems.

SDMN can also be used to provision these security technologies as a service for customer tenants or create security service chain for mobile applications.

17.7 SDMN Security Applications

SDMN helps solve security issues in mobile networks. It not only simplifies the network and services provisioning in a mobile network, but it can also be used to solve security problems in a mobile network such as encrypting selected traffic, creating on-demand network segmentation, applying necessary access control, protecting infrastructure in real time, mitigating security threats, and enhancing visibility and telemetry for the network (Fig. 17.5).

ONF [4] has shared two use cases of OpenFlow-based SDN in LTE network. One of the use cases discusses how SDN can be used to centrally manage the radio resources and resolve the interference issues that are traditionally resolved using techniques applied in a distributed fashion.

A similar approach can further be leveraged to apply end-to-end security policies from the eNB all the way up to the EPC using a centralized SDN controller.

17.7.1 Encryption: eNB to Network

In the new all-IP-based mobile network architecture, it is difficult to protect traffic between the eNB and EPC, especially when the eNB can be installed in an untrusted environment or when H(e)NB is located at a customer premise. It is not that difficult to intercept control plane or user plane communication between the eNB and EPC. User and control traffic is at risk without an encryption in place. IPSec is used today to protect eNB-to-EPC communication, but it has its limitations of introducing scalability and complexity to the network.

SDMN can be leveraged to encrypt traffic for all or selected eNBs residing in a trusted or an untrusted environment. A selected traffic identification, policy, and encryption can be applied from an SDN centralized controller.

An SDN controller with centralized policy and control to a mobile network can be used to verify and enforce necessary control and encryption for user plane data. It can also be used to further encrypt traffic from the eNB to EPC, which is unencrypted today.

17.7.2 Segmentation

During a security event such as malware and DoS, DDoS network gets paralyzed. Access to all parts of the network is affected including the critical assets. During such a network state, the security administrator wants to have their critical assets reachable during a network attack; meanwhile, it needs to make sure that no one can access the critical asset until the incident is handled and the attack is mitigated.

An SDN-based application can make sure that critical assets (i.e., Home Subscriber Server (HSS) DB) are accessible during a breach or network attack. System can also make sure that only authorized people can access the assets until the incident is fully resolved.

Such SDN applications can build a tier, a zone, or a network segment in real time by doing a requirement analysis (application criticality, classification, network trust level, risk focused) and create an appropriate type segment.

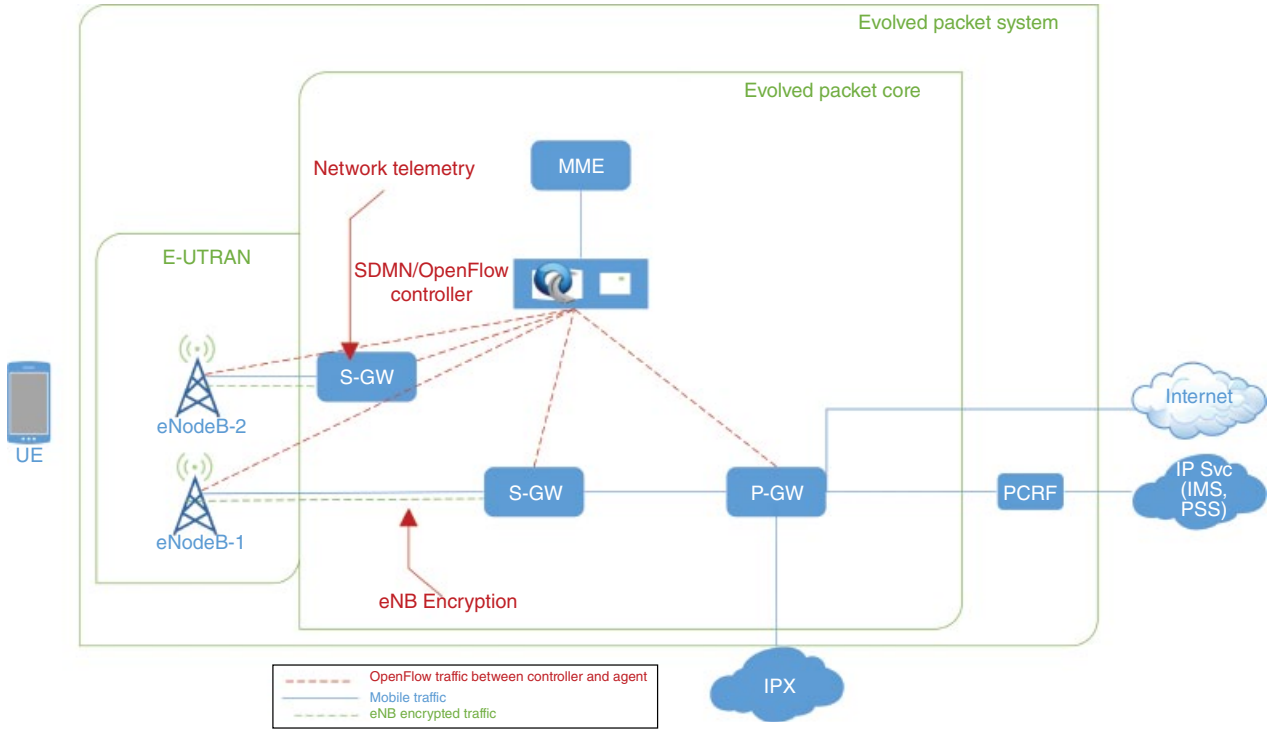

Figure 17.5 SDMN/OpenFlow security applications.

17.7.3 Network Telemetry

Network intelligence can be developed by enabling network visibility and knowing your network. An effective threat protection and mitigation are not possible without having capability to see what is going inside your network.

A network telemetry system can provide information about the origin, destination, nature, and other attributes of the traffic from various network components and help identify and mitigate an ongoing threat.

SDN technology can leverage its capabilities to develop a telemetry system of mobile components in a mobile network where eNBs, S-GW, and P-GW can collaborate and develop an intelligent network telemetry system. This will help introduce network intelligence and visibility capabilities to take informed security decisions.

References

[1] Wikipedia Infocommunication. Available at http://en.wikipedia.org/wiki/Infocommunications (accessed February 18, 2015).

[2] 3GPP. 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401. Available at http://www.3gpp.org/DynaReport/33401.htm (accessed February 18, 2015).

[3] 3GPP. 2G Security; Security architecture. TS 33.102. Available at http://www.3gpp.org/DynaReport/33102.htm (accessed February 18, 2015).

[4] Open Network Foundation. OpenFlow™-Enabled Mobile and Wireless Networks document. Available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-wireless-mobile.pdf (accessed February 18, 2015).