CELTIC Project Number:	**C2012/2-5**
Project Title:	SDN Concept in Generalized Mobile Network Architectures – SIGMONA
Confidentiality:	PU / RE / CO[1]

Document Identifier:	<D4.1>
Document Title:	**Secure Mobile Architecture**
Authors:	NEXTEL S.A.
Participants:	Aalto University, NEXTEL, ENEO, INNOVALIA, CWC, MONTIMAGE, EXFO
Work Package:	WP4
Version:	1.0
Date of last changes:	31/01/2016
File Name:	Secure Mobile Architecture.

Abstract: This document presents state-of-the-art in security of Software Defined Mobile Networks (SDMN). Starting from brief discussion of SDN and SDMN the security challenges that could exist in SDN and SDMN are elaborated. Then various approaches for strengthening SDMN security are discussed. SIGMONA research partners have provided their contribution in the security area of SDMN and their use cases and research topics are included towards the end of the document.

Keywords: Security in SDN, Network security, SIEM, Intrusion Detection Systems, Deep packet inspection, Customer Edge Switching.

[1] Dissemination level:
PU = Public
RE = Distribution to a group specified by the consortium
CO = Confidential, only allowed for members of the consortium

Table of contents

Authors

Aalto University	Jesús Llorente Santos
	Phone: +358 466 222 336
	E-mail: jesus.llorente.santos@aalto.fi
	Hammad Kabir
	Phone: +358 451 965 275
	E-mail: hammad.kabir@aalto.fi

NEXTEL S.A.	Oscar López Pérez
	Phone: +34 94 403 55 55
	E-mail: olopez@nextel.es
	Mikel Uriarte Itzazelaia
	Phone: +34 94 403 55 55
	E-mail: muriarte@nextel.es
	Etxahun Sanchez Basterrechea
	Phone: +00 34 94 403 55 55
	E-mail: esanchez@nextel.es

INNOVALIA	Asier Valtierra
	Phone:
	E-mail: avaltierra@innovalia.org

ENEO	Jaime Nebrera
	Phone:
	E-mail: jnebrera@eneotecnologia.com

Montimage	Edgardo Montes de Oca
	Phone: +33 1 53 80 35 77
	E-mail: edgardo.montesdeoca@montimage.com

EXFO	Kari Hyväri
	Phone: +358 40 3010 317
	E-mail: kari.hyvari@exfo.com

CWC	Madhusanka Liyanage
	Phone: +358 44 988 5353
	E-mail: lliyanag@ee.oulu.fi
	Ijaz Ahmed
	Phone: +358 45 330 1160
	E-mail: iahmad@ee.oulu.fi

Executive Summary

SIGMONA effort has been focused to provide solutions for evolving mobile communications taking in mind what 5G infrastructures will need. In this scenario of future mobile communications it is expected to deliver ultra-fast, ultra-reliable network access supporting a massive increase of data traffic and connected nodes. Different technologies are emerging to address the requirements of future mobile networks, such as software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing concepts.

SDN aims at decoupling the network control and data planes where the network control and intelligence are logically centralized and the underlying network infrastructure is abstracted from the control. The introduction of centralized controllers, network virtualization, programmability and network function virtualization; the separation of the control plane and the data plane; the introduction of new network functions all have impact on how security needs to be assured and managed.

In the scope of the SIGMONA project, WP4 will demonstrate the topics related to security aspects for future mobile networks. In this WP, SDN, NFV and cloud technologies are analysed and are seen as enablers to enhance security for the new generation of mobile networks where virtual network architectures will be integrated. The ultimate goal is developing methods for better security between the control plane and the data plane, enhancing security in data paths and finally proving the effectiveness of security functions in SDN, NFV and cloud environments to improve detection, better reaction and fast recovery mechanisms.

This deliverable, presents the security challenges these new technologies are facing, inherent to the new telecommunication paradigm. After that a multitier approach to secure Software Defined Mobile Network (SDMN) by tackling security at different levels to protect the network itself and its users, and a proposal for a secure mobile architecture is presented.

Security solutions to provide secure the communication channels between network elements by leveraging Host Identity Protocol (HIP) and IPSec tunnelling are presented. Additional security mechanisms are implemented to restrict the unwanted access to the mobile backhaul network with policy based communications. It also protects the backhaul devices from source address spoofing and Denial of Service (DoS) attacks. Finally, security assessment and awareness it gained with Software Defined Monitoring (SDM) and data collection to detect prevent and react to security threats.

List of abbreviations

ALG	Application Layer Gategay
ANDSF	Access network discovery and selection function
CES	Customer Edge Switching
CETP	Customer Edge Traversal Protocol
CTRL	Controller or orchestrator
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denialof Service
DPI	Deep Packet Inspection
HIP	Host Identity Protocol
HSS	Home Subscriber Server
IP	Internet Protocol
KPI	Key Performance Indicators
LTE	Long-term Evolution; 3GPP standard for wireless communication of high-speed data for mobile phones and data terminals
MME	Mobility Management Entity
NAT	Network Address Translator
NFV	Network Function Virtualization
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
RAT	Radio Access Technology
RGW	Realm Gateway
RTT	Round Trip Time
SDM	Software Defined Monitoring
SDMN	Software Defined Mobile Networks
SDN	Software Defined Networks
SIP	Session Initiation Protocol
SIEM	Security Information and Event Management
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VM	Virtual Machine
VN	Virtual Network slice
VNE	Virtual Network Element
VS	Virtual Switch

1. Introduction

The SIGMONA (SDN Concept in Generalized Mobile Network Architectures) project aims at analysing the network architectures and functions for evolution of the LTE/EPC (3GPP) mobile networks. The target is to innovate and develop new network concepts for meeting the future requirements of the evolving mobile networks. The project aims the specification, evaluation and validation of a Software Defined Mobile Network (SDMN) concept designed onto the software defined networking (SDN), observing network virtualization, and cloud computing principles.

WP4, Security for Future Mobile Networks, addresses the security aspects of future mobile networks while adapting virtual network and SDN architectures into mobile and telecommunication networks. WP4 studies new strategies and concepts regarding the security techniques for SDMN and beyond LTE telecommunication networks. Following the general SIGMONA targets, WP4 security work package will develop secured virtual network architectures. The work package also focuses on obtaining layer 2 and layer 3 virtual network traffic architectures. Thereafter, it will study the correlations and dependencies of such architectures to create a general solution. In other aspects, WP4 seeks to identify economically viable security techniques to provide secure virtual network services in the mobile network environment.

The expected results for this work package will be:

1. Security assessment report on current and future setups
2. Secure virtual network traffic architectures (Layer 2 and Layer 3)
3. Economically viable security techniques for mobile virtual networks
4. Performance and implementation study on IPSec gateway solutions
5. Network services (i.e. mobile clouds, mobile P2P networks, multicast services) using virtual networks
6. Potential contributions to 3GPP in terms of corrections or new contributions for security measures in (virtualized) mobile networks
7. Contributions to standardization of Customer Edge Traversal Protocol and CES legacy interoperability solutions.
8. Definitions of Diameter Extensions for policy control of Collaborative Firewalls.
9. Framework for integrating reputation systems, deep packet inspection, application layer gateways and mobility protocols as part of the Customer Edge Switching architecture.
10. Report on scalability and performance of a Virtual collaborative Firewall using the CES concepts in the SDMN environment

This document describes the proposals developed for each partner in SIGMONA project to contribute to deploy a secure mobile architecture in SDMN. Also, it provides different solutions for a) deploying security between control plane and data planes; b) deploying security implementation in the data paths using a policy based communication; and finally c) providing a security monitoring and control functionality that enable fast detection and reaction against network threats in an SDN deployed network.

2. State of the Art Security in SDMN

2.1 Security Threats in SDMN

The separation of the control and data planes, aggregating the control functionality to a centralized system and running the control functions in a cloud will open new security challenges in SDMNs. For instance, the communication channels between the isolated planes can be targeted to masquerade one plane for attacking the other. The control plane is more vulnerable to security attacks; especially to DoS and DDoS (Distributed DoS) attacks. This is due to its more visible and eventually centralized nature where controllers become single points of failure. Since the networking paradigm in SDMN is converging towards software-based networking, operational malfunctioning or malicious software can compromise the whole network by providing access to the control plane. Some of the known security challenges in SDMN are summarized in Table1.

Table 1: Summary of security threats in SDMN architecture

SDMN Layer	Type of threat	Threat reason and description
Application	Lack of authentication and authorization	Possible huge number of (third-party) applications
	Fraudulent rules insertion	Malicious applications generated false flow rules
	Access control and accountability	Lack of binding mechanisms for applications
Control	DoS/DDoS attacks, Controller hijacking or compromise	Visible nature of Ctrl-plane
	Unauthorized controller access	No compelling mechanisms for enforcing access control on backhaul devices
	Scalability or availability	Centralized intelligence
Data	Fraudulent flow rules	Lack of intelligence
	Flooding attacks	Limited capacity of flow tables
	Controller and DP switch masquerading	Lack of strong authentication
Ctrl-Data Int.	TCP-Level attacks	TLS is susceptible to TCP level attacks
	Man-in-the middle attack	Optional use of TLS and complexity in configuration of TLS
App-Ctrl Int.	Illegal controller access, policy manipulation and fraudulent rule insertion	Limited secure APIs, lack of binding mechanisms between applications and controllers.

2.2 Security requirements for SDMN

Since future mobile networks will expectedly be packet switched, they will inherent the classical weaknesses of the packet-switch networks, such as unwanted traffic, source address spoofing and DoS attacks. Besides, mobile networks will face new challenges from introduction of technologies such as SDN and NFV. The growing popularity of smartphones, rising mobile broadband volume and sophistication of malware exposes mobile-terminals to the attacks of the fixed networks. However, mobile terminals are weakly protected compared to their fixed counterparts i.e. laptops, desktops etc. and are constrained in terms of computing resources, memory and battery lifetime. This de-incentivizes deploying host-based security solutions for resource-constrained wireless hosts. Moreover, host-only security leaves air interface open to the feats of hacks, thefts and unwanted traffic that takes toll on the network performance.

Following the end-to-end principle which states that a function not feasible in the end-hosts shall be left to the network, the new technologies and enhancements in the core network can significantly contribute to the network security. For example, SDMN relying on the principles of SDN can significantly contribute to network security due to global visibility of the SDN controller to the underlying network. This can enable the networks to dynamically react to security threats and mitigate policy conflicts across the network. To address the Internet vulnerabilities, future mobile networks shall:

- Limit the flow acceptance to verifiable sources to tackle unwanted traffic, source address spoofing, and prevent resource exhaustion.
- Shall overcome the classical Internet weaknesses of source address spoofing in order to attribute the evidence of (mis)behavior to the sender identity.
- Evidence attribution shall be aggregated under a stable identity to incentivize deploying mechanisms that build reputation of the communicating entities.
- Under network stress, resources shall be granted to a reputed entity.
- Allow defining dynamic reachability policies for mobile hosts, applications and services. This is in contrast to the current mobile networks where policies are tightly coupled to physical resources and are not scalable to services/applications.
- Analyse and manage the policy configuration of data-plane elements to deploy a robust and stable security policy across the network. The logically centralized controller in SDMN can provide a global view of the configurations of different network devices and hence mitigate conflicts and inconsistencies in the security procedures
- The deployment of new and existing mechanisms to SDMN requires that they are implemented and tested for their compliance to SDN principles. Existing security solutions are difficult to deploy, manage and scale to secure SDMN.
- Deploy security mechanisms that do not require changes to the end-hosts or protocols, to minimize the deployment challenge.
- Leverage the existing investments in network security to harden their security, thus preventing the controller from receiving the flood of malicious traffic.
- Optimize the network resource utilization for security functions

3. SDMN Architecture description

Future mobile network architectures need to be evolved to cope with future demand for high bandwidth, a large and evolving set of services with new specific requirements, high level security, low energy consumption and optimal spectrum utilization. Specifically, the increasing number of mobile users and services will result in the increasing capacity requirements for the mobile network. On the other hand, it is expected that mobile data traffic will grow faster than the fixed Internet during upcoming years. Thus, accommodating this expected traffic growth is an imminent requirement of future mobile networks.

In order to keep with the traffic growth, mobile networks have not only to go through architecture processes to optimize the current resources but also to add new components/technologies which increase the capacity. However, mobile backhaul networks contain remarkably complex and inflexible devices. Although the interfaces of a cellular network are globally standardized, still most of these devices are vendor specific. Thus, mobile operators do not have flexibility to ``mix and match” capabilities from different vendors. In other aspect, the standardization process for mobile networks is a long lasting process. Although, operators find promising concepts, they need to wait years to implement them in their networks. This might bury lots of interesting opportunities due to the lack of support.

On these grounds, Software-Defined Networking (SDN) is one of the promising technologies which are expected to solve these limitations in current mobile networks. SDN provides the required improvements in flexibility, scalability and performance to adapt the mobile network to keep up with the expected growth. Software-defined mobile networking (SDMN) is directing the current mobile network toward a flow-centric model that employs inexpensive hardware and a logically centralized controller. SDN enables the separation of the data forwarding plane from the control planes. The SDN-enabled switches, routers and gateways are controlled through an SDN controller/network operating system, and are seen as virtual resources. The control plane of the mobile networking elements can be deployed onto an operator cloud for computing.

In this paradigm, each operator has the flexibility to develop his own networking concepts, optimize his network and address specific needs of his subscribers. Furthermore, software-programmable network switches in SDMN use modern agile programming methodologies. These software methodologies can be developed, enhanced, and upgraded at much shorter cycles than the development of today’s state-of-the-art mobile backhaul network devices.

The acquisition of virtualization into LTE (Long Term Evolution) mobile networks brings the economic advantage in two ways. Frist, SDMN requires inexpensive hardware such as commodity servers and switches instead of expensive mobile backhaul gateway devices. Second, the introduction of SDN technology to mobile networks allows entering new actors in the mobile network ecosystem such as ISV (Independent software vendor), cloud providers, ISP (Internet Service Providers) and that will change the business model of mobile networks.

Thus, the concept of SDMN would change the network architecture of the current LTE 3GPP (3rd Generation Partnership Project) networks. SDN will also open up new opportunities for traffic, resource and mobility management, as well as impose new challenges on network security. Many academic and industrial researchers are working on the deployment of SDMNs. We believe that ideas stemming from design and experiments with SDMN provide indispensable knowledge for anybody interested in next-generation mobile networks.

SDMN architecture combines the concepts of SDN, NFV and cloud computing to design a programmable, flexible and flow centric mobile network. It offers various benefits such as centralized controlling, improved flexibility, efficient segmentation, automatic network management, granular network control, reduction of operational and equipment cost of backhaul devices, on-demand provision and resource scaling [1]. Therefore, SDMN is considered as the latest innovation in the telecommunication domain [2] [3]. Figure 1 illustrates the consolidated SDMN architecture.

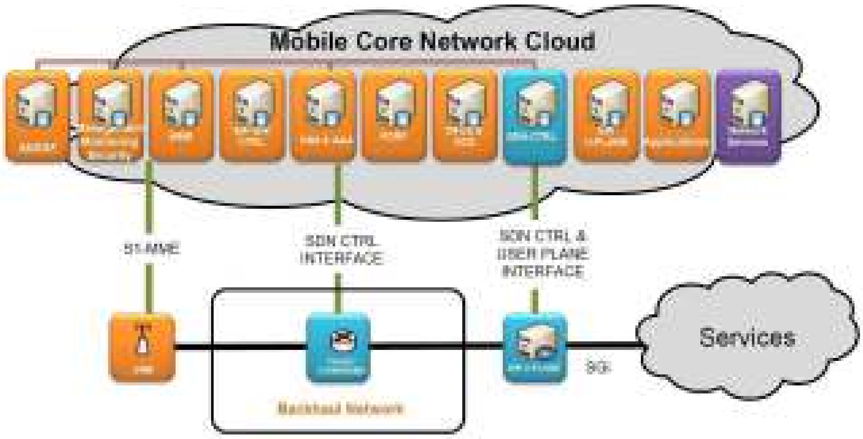

Figure 1: Consolidated SDMN architecture

In SDMNs, the legacy mobile network control functions, i.e., MME (Mobility Management Entity), HSS (Home Sub- scriber Server), PCRF (Policy and Charging Rules Function) and the control planes of S/P-GW (Serving/Packet Gateway) run on the mobile network cloud as SDN applications and enforce the desired function by means of SDN technology. With this approach, the user plane is composed only by strategically located SDN capable switches and devices [4].

The SDMN architecture can be divided in to three layers [2] [4] [9] [10].

1. **Data Plane Layer**

The data plane layer is also known as the infrastructure layer. It is consists of the network elements such as switches and other devices. These switches support packet switching and forwarding functions. Base stations are connected to DP switches at the border. However, the SDMN architecture is transparent to the existing radio technologies. Similarly, boarder switches at the core network are connected to the Internet to offload the mobile subscriber traffic.

2. **Network Controller**

The logically centralized controller provides the consolidated control functionality of the DP switches. The control protocol s used by the controller to communicate with the data plane elements. Basically, the controller uses the control protocol to install flow rules in each DP switch to route the traffic along the mobile network data plane. The boundary between the network controller and the data plane layer is traversed by the southbound API.
The Network Operating System (NOS) is run on top of the controller to support the control functions.

3. **Application Layer**

The application layer consists of all the controlling and business applications of the mobile network. The traditional mobile network elements such as PCRF (Policy and Charging Rules Function), HSS (Home Subscriber Server), MME (Mobility Management Entity) and AAA (Authentication Authorization and Accounting) are now software applications which are running on top of NOS. The boundary between the application layer and the network controller is traversed by the northbound API (Application Programming Interface).

Control elements perform the traditional functionalities and assist NOS to handle mobile network functionalities such as mobility management, resource management and traffic transportation.

Thus, the adaptation of SDN changes the network architecture of the current mobile networks. Moreover, SDN will also open up new opportunities in various sections in the mobile network. Especially, it provides various benefits for traffic, resource and mobility management, as well as imposes new challenges on network security.

3.1 Existing Security Mechanisms in SDMN architectures

3.1.1 Advantages when introducing SDN

SDN allows the separation of the control plane and the data plane, enabling the programmability and centralized control of the network infrastructure. From the security point of view this brings many advantages and disadvantages [11].

One of the main advantages of SDN is that it simplifies network management, and facilitates the upgrade of functionality and debugging. Consequently, introducing SDN in wireless mobile networks allows enhancing security and accelerates innovation in the area. Programmability allows fast and easy implementation and deployment of the new functionality at both hardware and software levels. Automated management reduces Operational Expenditure (OPEX), while Capital Expenditure (CAPEX) can be reduced by making it unnecessary to replace underlying hardware.

SDN enabled centralized control and coordination makes it possible to deliver the state and policy changes more efficiently. SDN introduces vulnerabilities inherent to software based systems, as we will describe in the next sub-section, but at the same time allows improving the resiliency and fault tolerance of centralised controllers using well known techniques such as automated failovers. Reaction to vulnerabilities and attacks is also improved by giving the ability to quickly assess the network from a centralized viewpoint and making it possible to apply fast dynamic changes and automate mitigation actions.

Another aspect is that it enables Network Functions Virtualization (NFV). In this way Internet and cloud service providers can differentiate themselves and propose improved solutions in terms of Quality of Service (QoS) and security. By introducing virtualized abstraction, the complexity of hardware devices is hidden from the control plane and SDN applications. Furthermore, managed network can be divided into virtual networks that share the same infrastructure but are governed by different policy and security requirements. SDN and NFV makes possible the sharing, aggregation and management of available resources, enables dynamical reconfiguration and changes of policy, and provides granular control of network and services through the abstraction of the underlying hardware.

The introduction of open SDN standards, such as OpenFlow, not only promotes research and collaborations between different operators and providers, but improves the possibility of interoperability in multi-service and multi-vendor environments, and with the legacy systems [11].

3.1.2 Disadvantages when introducing SDN

One of the main security issues introduced by SDN is that the controllers act as centralized decision points and, as such, become potential single points of attack or failure. Also, the southbound interface (e.g., OpenFlow) between the controller and data-forwarding devices is vulnerable to threats that could degrade the availability, performance and integrity of the network [11].

Controllers become a security concern and where they are located and who has access to them needs to be managed correctly. Communications between the controllers and network elements needs to be assured by encryption techniques (e.g., SSL) and the keys need to be managed securely. But these techniques are not sufficient to assure high availability because denial-of-service (DoS) attacks remain difficult to detect and counter. Controllers are vulnerable to these types of attacks and guaranteeing that they are available at all times is a complex task that requires guaranteeing resilience using redundancy and fault tolerance mechanisms. Furthermore, every change and access needs to be monitored and audited for troubleshooting and forensics; and this is more complicated in virtual environments where visibility is often reduced. Thus, the following challenges need to be addressed [10][11]:

- Secure the Controller: Contrary to traditional networks architectures where the security functions and mechanisms are orchestrated in a distributed manner, the controller in SDMN architecture is the centralized decision point. Access to such controller needs to be tightly secured and monitored to avoid that an attacker takes control of the network elements.

- Protect the Controller: if the controller goes down (for example, because of a DDoS attack), so goes the network, which means the availability of the controller needs to be maintained.
- Establish Trust: protecting the communications throughout the network is critical. This means ensuring the controller, the applications loaded on it, and the devices it manages are all trusted entities that are operating as they should.
- Create a Robust Policy Framework: what’s needed is a system of checks and balances to make sure the controllers are doing what you actually want them to do.
- Conduct Forensics and Remediation: when an incident happens, you must be able to determine what it was, recover, potentially report on it, and then protect against it in the future.

4. Proposed SDMN Security Architecture

Most of the telecom-specific requirements are tightly coupled with control and data planes than the application plane [1] [4]. At the first stage, the proposed security architecture is focused on securing the security issues related to the control plane, data plane and Ctrl-Data interface only. The proposed security architecture for SDMN networks is presented in Figure 2 [10].

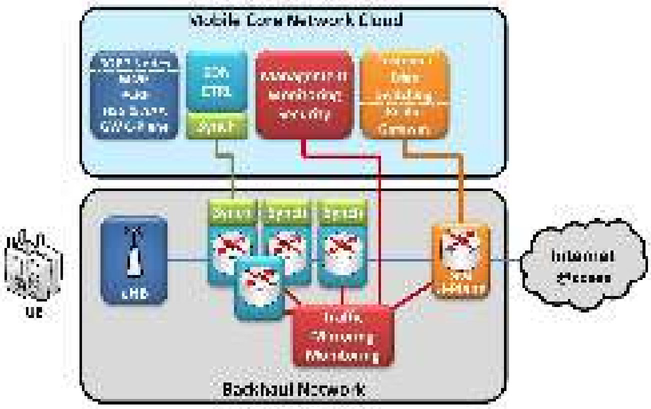

Figure 2: Proposed architecture for SDMN

The Proposed Security Architecture for SDMN is a multitier security approach with six components. 1) Secure Communication (SC) Component, 2) Policy Based Communication (PBC) Component, 3) Security information and event management (SIEM) Component, 4) Security Defined Monitoring (SDM) Component 5) DPI (Deep Packet Inspection) Component and 6) Synchronized Network Security and Traffic (Synch) Component.

4.1 Components of proposed SDMN architecture

4.1.1 Secure Communication (SC) Component

The SDMN architecture has two communication channels: control and data channels. The control channel transports the vital control/signalling data between the control and data planes. The user communication data is transported via the data channel. The key security issues of SDMN communication channels are the lack of IP level security and lack of strong authentication between backhaul devices. Existing SDMN communication channels rely on higher layer security mechanisms, such as TLS/SSL. For instance, widely used Open Flow protocol utilizes a TLS/SSL based control channel [6]. However, higher layer security mechanisms do not protect the IP-level information. As a result, communication sessions are vulnerable to IP based attacks such as IP spoofing, TCP SYN DoS and TCP reset attacks [5][7][8]. Moreover, TLS/SSL authentication mechanism is vulnerable to IP spoofing and Compression Ratio Info-leak Made Easy (CRIME) attacks [5]. Therefore, SDMN architecture requires secure communication mechanisms to prevent these security threats.

We propose a HIP (Host Identity Protocol) based secure IPsec tunnelling architecture to secure SDMN communication channels [8]. It establishes secure HIP tunnels between the DP (Data Plane) switches and the controller.

4.1.2 Policy Based Communication (PBC) Component

The current Internet has struggled to find appropriate solutions for weaknesses in its architecture, such as address spoofing, unwanted traffic and DoS. As a result, these attacks often interrupt legitimate access, induce computing downtime and launch DoS. Future mobile networks that are packet switched will inherit these vulnerabilities in addition to challenges from introducing new technologies. Since mobile terminals and other battery-powered wireless devices are constrained in terms of computing power and battery times, deploying host-based security drains the available resources. Besides, host-only security leaves the air interface open to the feats of hacks, thefts and malicious traffic that can take toll on the network performance. Following the end-to-end Internet principle which states that a certain functionality that cannot be implemented in the end nodes shall be left to the network, we advocate a particular approach towards security based on certain role of network-based firewall, namely Customer Edge Switching (CES)[14] [15].

CES is an extension of traditional stateful firewall functionality into a cooperative firewall. The solution is a proposed replacement of NATs at network edges, separating the customer network from the public Internet. It acts as a connection broker for the hosts/applications that it serves and exchanges their policy offers and requirements encoded in Customer Edge Traversal Protocol [14]. Compared to traditional stateful firewalls that either accept or drop an inbound packet, the policy negotiation procedure enables the destination to issue additional queries to the sender: i.e. to eliminate spoofing, authenticate sender and ensure policy compliance. The policy-based communication architecture enables network administrators to dynamically adjust and negotiate their security policies. CES offers the necessary set of security or authentication methods as policy-controlled features for network administrators, such that flow admission is limited to verifiable sources only. In addition, CES supports Realm Gateway functions for incremental adoption of the technology, such that the solution is inter-operable with legacy IP networks.

4.1.3 Security information and event management (SIEM) Component

Network monitoring solutions come in different variants depending on what they measure and how they collect the data. These are, for instance: (1) Active Probing: service-centric approach that collects data based on synthetic measurements such as ICMP Echo Requests, HTTP GET requests or specially crafted packets. Often these measurements try to measure properties of the network that would be impossible to obtain from pure passive measurements and are arguably the only way to measure service availability. (2) Device Polling: device-centric approach that queries devices typically using SNMP (Simple Network Management Protocol), collecting interface status information, traffic volumes, device load, CPU, etc. (3) Flow Collection solutions that collect traffic information from network devices such as routers/switches. Here the traffic is analysed and flow information is collected for post-analysis using, e.g., Cisco's Netflow monitoring architecture. Flow data is easier to analyse and process than packet data, but provides less granular information. (4) Packet Analysis that usually involves a SPAN port from a switch or a network tap and extracts information from individual packets, including information from payloads using DPI (Deep Packet Inspection) techniques. (5) Log Analysis solutions that collect machine generated data typically in the form of log files (e.g., syslog) and present a query interface to correlate events across different types of systems, such as routers, web servers, load balancers, etc.

Security information and event management (SIEM) technologies aggregate the information from these different monitoring solutions to obtain a more complete security analysis and management solution. SIEM provides, on one hand, Security Information Management (SIM) to correlate and analyse real-time data; and, on the other hand, Security Event Management (SEM) to analyse log-term stored information and log data. SIEM technology aggregates event data produced by security devices, network infrastructures, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as NetFlow and packet capture (DPI). Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data is normalized, so that events, data and contextual information from disparate sources can be correlated and analysed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time security monitoring, historical analysis, as well as support for incident investigation and compliance reporting.

4.1.4 Security Management and Monitoring (SMM) Component

The Security Management and Monitoring (SMM) component involves introducing a dedicated Software Defined Monitoring controller (SDM CTRL) to orchestrate the monitoring activities related to security that are performed by security sensors (i.e., probes) deployed in the network and in the cloud. These sensors can be passive (not disrupting traffic) or active (in the data path to perform online countermeasures); and, can either be installed in existing Network Elements or in dedicated Security Appliances. The probes analyse traffic, correlate information from different sources and produce metadata and verdicts that can then be used by a centralised decision point and by the different network functions. In the figure bellow is depicted the main modules and links that are necessary for this solution: the active sensors, the passive sensors (analysing mirrored traffic), the SDM CTRL interface and the SDM CTRL.

The SDM and SDN CTRLs can be separate modules or integrated in one module. The SDN CTRL will interact with the routers implementing the SDN CTRL interface to manage the traffic (e.g., redirect traffic to the security appliances) and recuperate certain information. The SDM controller will interact with the security appliances or probes implementing the SDM CTRL interface to manage them and recuperate metadata, part of the traffic or verdicts. This information can be used by: the Network Monitoring function in the cloud to perform analysis and trigger mitigation actions; or, the other Network functions/services and Applications.

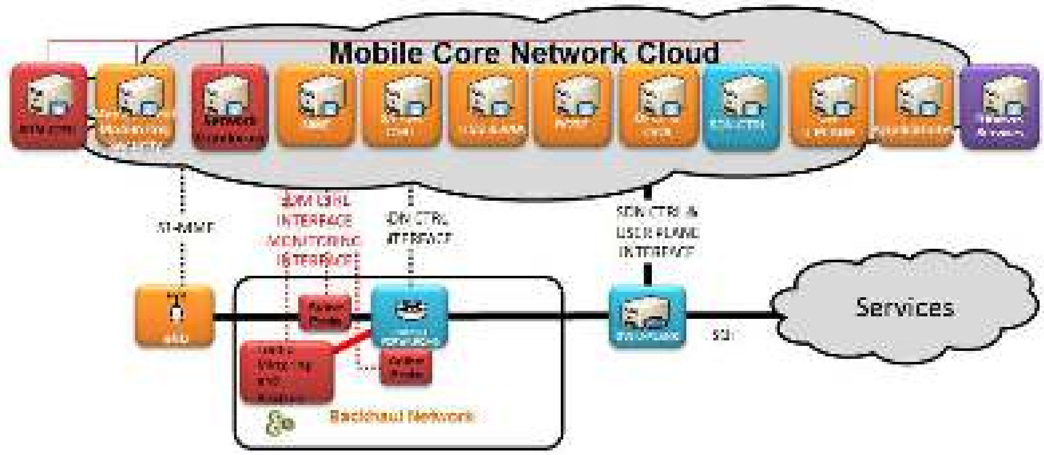

Figure 3: Security Management and Monitoring Component

4.1.5 Deep Packet Inspection Component

SDMN will enhance security by making it easier implement counter-measures and isolate network parts when security problems are detected. But additional software, components and interfaces required in SDMN open new opportunities for attacks by malicious agents. Security needs to be addressed on the network side as well as the mobile device side. Deep Packed Inspection (DPI) as part of Network Intrusion Detection Systems (NIDS) strengthens network security by detecting and tackling harmful traffic flows and packets.

One critical aspect in SDMN security is that the applications and associated control elements need a holistic view of infrastructure conditions. This is a central and something that DPI, in principle, can provide, by gathering information throughout the network and feeding it back to the control layer.

As illustrated in figure below, the proposed DPI component can be part of the active monitoring probe that detects security threats, allowing it to react to security breaches. The DPI component can also work on mirrored traffic as a part of the network monitoring functions. In both cases the DPI component can be virtualized.

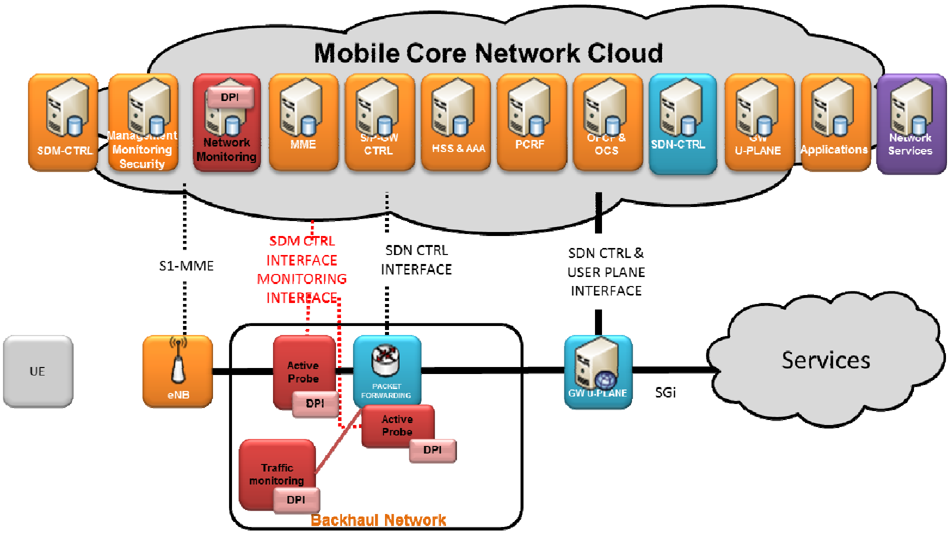

Figure 4: Security Management and Monitoring component DPI

4.1.6 Synchronized Network Security and Traffic (Synch) Component

Network security is an integral part of the network management. SDMN requires a stable and robust security policy deployment. However, this requires a thorough analysis of policy configuration of all the networked elements avoid conflicts and inconsistency in the security procedures, and hence diminish the possibilities of serious security breaches and network vulnerabilities. From security perspective, even a small oversight can lead to a global security problem, such as placing a significant functionality on an unreliable network/system [18]. In SDMNs, since a logically centralized controller is responsible for controlling and managing the whole network, security lapses compromising the controller will affect the traffic in the data paths.

Therefore, we propose the realization of synchronized network security and traffic forwarding policies. This is achieved by leveraging the visibility of the network states in the controller; cooperation between traffic management and forwarding policies, establishing 3GPP entities and security monitoring devices in the operator cloud; and with the help of the synchronizing entity (Synch) as shown in Figure 5. The Synch module mediates between security monitoring and security management device; as well as between traffic monitoring and management devices to deploy forwarding rules in the data plane which are based on security polices defined in higher layers.

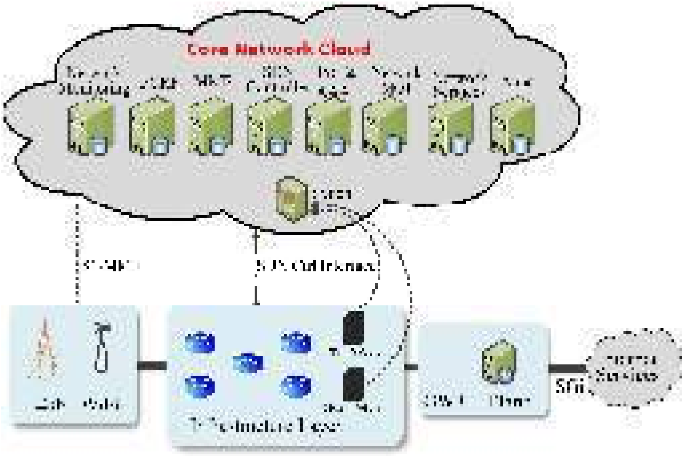

Figure 6: Synchronized Network Security and Traffic Component

As shown in Figure 7, traffic monitoring and security monitoring entities provide real-time information for the Synch module. The traffic monitoring entity maintains a track of changes in flow rules that could occur for example due to mobility. The security monitoring entity checks the previous security techniques used for the particular user. If the traffic from that user was previously directed to a DPI system, the security monitoring entity will inform the Synch module. Henceforth, the Synch module would redirect the traffic from the same user to a DPI system that was used for his previous traffic. In this fashion, the mobility of a node does not hinder in keeping security of the system intact, since activities of the host are monitored from the centralized system that maintains the history of the host and flows originated from the host. Similarly if a user had been behind a firewall, he will still be behind a firewall if he changes the point of attachment in the network.

5. Secure Communication Component

5.1 Introduction

SDMN offers various benefits such as centralized controlling, improved flexibility, efficient segmentation, automatic network management, granular network control, reduction of operation and equipment cost of backhaul devices, on-demand provisioning and resource scaling [1]. For this reason, SDMN is considered as the latest innovation in the telecommunication domain.

However, SDMNs are vulnerable to security threats which can originate at different sections of the network [7]. Security issues in SDMN backhaul network can be divided into four threat vectors: 1) Application Plane Security; 2) Control Plane Security; 3) Data Plane Security; and, 4) Communication Security [7][8]. Furthermore, SDMNs contain two communication channels, control channel and data channel [1][2][3]. Thus, the communication security threat vector can be further divided into: 1) Security issues related to the control channel; and, 2) Security issues related to the data channel [7]. We describe them in the following sections.

5.2 Security Issues related to the SDMN Control Channel

The main security issue of the control channel is the lack of IP level security. Existing SDMN control protocols rely on higher layer security mechanism such as TLS (Transport Layer Security)/ SSL (Secure Sockets Layer) sessions. For instance, the widely used OF (OpenFlow) protocol uses TLS/SSL based control channels [7]. However, higher layer security mechanisms are vulnerable to IP-based attacks such as IP spoofing, TCP SYN DoS and TCP reset attacks [5][7]. Since, the higher layer protection mechanisms do not provide sufficient level of required robustness and security for the control channel [7]. A strong authentication mechanism is required between the controller and the DP (Data Plane) switches. Otherwise, intruders could impersonate legitimate DP switches and launch attacks on the control channel. For instance, the attackers could inject fake flow requests to perform DoS attacks [7]. Furthermore, TLS/SSL sessions do not use a strong authentication procedure between the controllers and the switches. This makes the authentication mechanism of TLS/SSL sessions vulnerable to IP spoofing and Compression Ratio Info-leak Made Easy (CRIME) attacks [5][7].

The network controller is the key component of the SDMN network due to its centralized intelligence and controlling abilities. As a result, attacks on the network controller are the most severe threats to the SDMN architecture. The control channel is merely an interface that enables the communication between DP devices and the controller. The security of this control channel is a key factor to ensure the proper communication with the controller [7]. A DoS attack on the SDN controller is demonstrated in [10] in which an attacker continuously sends IP packets with random headers to the controller via the control channel. This could place the controller in a non-responsive or degraded state, making it unable to timely deploy flow rules in the DP switches. TLSv1 based communication is optional in the latest OpenFlow specifications due to the complexity of its configuration [12]. TLS configuration requires generating network site-specific certificates for the controller and DP switches, and signing device certificates with site-wide private keys. Therefore, many SDN equipment vendors have skipped the support for TLS in their DP switches, leaving the control channel vulnerable to security attacks. Thus, the control channel needs to be secured using other mechanisms.

5.3 Security Issues related to the Data Channel

The SDMN architecture has an all-IP based backhaul network. In contrast to 2G/3G telecommunication networks, the Radio Network Layer (RNL) encryptions are terminated at the eNodeBs in the latest IP-based telecommunication networks including SDMN [7][9][10]. Thus, current SDMN backhaul traffic is unencrypted and attackers can perform “SDN Scanner” mechanisms to collect network information [7][9][10]. Later, this information can be used to perform IP based attacks, such as DoS, reset, replay and spoofing attacks [7][9][10]. Furthermore, current SDMN data channels do not contain any integrity protection mechanisms. Thus, a flow modification attack can alter or destroy the data without being noticed by the network operator. The alternations of data flows may result in the decrease the Quality of Service (QoS) of the communication sessions[7][9][10].

The SDMN architecture requires strong mutual authentication mechanisms for the data channel as well. Without such authentication mechanisms, intruders can impersonate legitimate switches and inject forged traffic flows to the Data Plane [7][9][10][7,9,10]. In this way, attackers can exhaust the flow tables of the DP switches and reduce the available bandwidth for user traffic [7][9][10]. Moreover, it will affect the control plane by inducing unnecessary flow requests to the controller [7][9][10].

5.4 Proposed solution

The secure HIP tunnel establishment under the proposed SC component is illustrated in Figure 8 [7].

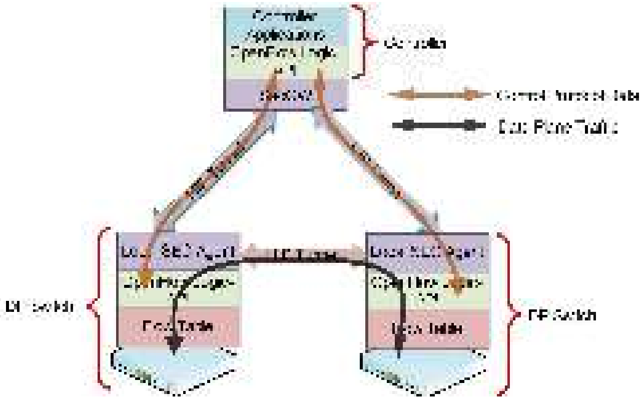

Figure 8: Secure Communication Channel

Here we proposed three main changes to the existing SDMN architecture. First, distributed SecGWs (Security Gateways) are used to secure the controller from outside network, and reduce the risk of becoming the single point of failure. Second, a new Security Entity (SecE) is added to the control SecGWs and to the other security functions in SDMN. Third, a local Security Agent (LSA) application is installed in each DP switch to handle security related functions in the switch. The proposed solution is a bump-in-the-wire mechanism and will not affect the underlying control protocol (e.g., OpenFlow) or the user plane communication channels. Table 2 contains features comparison of proposed SC component with other security solutions.

Table 2: Comparison of proposed architecture with existing security mechanisms

Property	**TLS/SSL**	**IPSec with IKEv2**	**IPSec with HIP**	**Proposed Architecture**
Vulnerability of mutual authentication mechanism	Medium	Medium	Low	Low
DoS attack prevention	No	No	Yes	Yes
Support for seamless mobility of backhaul nodes	No	No	Yes	Yes
Multihomed Support	No	No	Yes	Yes
Centralized Controlling	No	No	No	Yes
Point-to-Multipoint/ Multipoint-to-Multipoint	No	No	No	Yes
Visibility of traffic transportation	No	No	No	Yes
Access Control	No	No	No	Yes
Collaboration with other control entities	No	No	No	Yes

5.5 Evaluation and testbed

The components of the proposed architecture were implemented in a testbed to analyse their performance.

In the first set of experiments, we measured the performance penalty of secure communication component on the throughput, jitter and latency. We also measured the ability of the proposed architecture to protect the communication channels against common IP based attacks such as TCP SYN DoS and TCP reset attacks. The widely utilized OF protocol with TLS/SSL sessions is used as the reference for the control channel. The preliminary testbed components are illustrated in Figure 9.

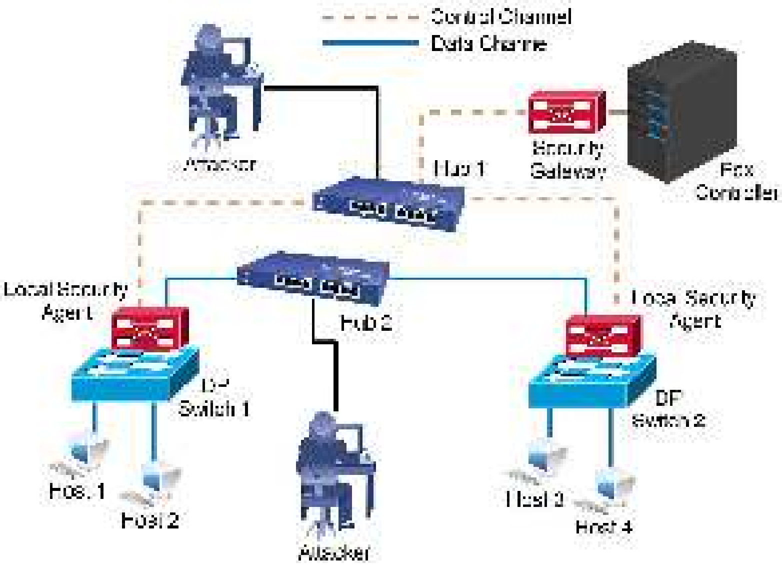

Figure 9: Layout of the experimental testbed

The preliminary testbed has two DP switches, an SDN controller and two hubs. The latest POX controller is used as the SDN controller, and OpenVswitch (OVS) version 1.10.0 virtual switches are used as DP switches. We also connect two virtual hosts to each OVS. The controller and switches are connected using two D-LINK DSR-250N routers. We keep an out-band control channel for these experiments. The OpenHIP implementation is used to model the Security Gateway and the LSAs. The IPERF network measurement tool is used to measure the throughput and latency performance. Finally, we connect an attacker to each hub according to the experiment scenarios. A laptop with an i5-3210M CPU of 2.5GHz processor is used to play the role of an attacker.

Data Plane performance of the existing and proposed architectures are presented in Table 3. Each experiment has been conducted for 500s (500 seconds) and the average values were recorded.

Table 3: Data Channel Performance without Attack (Normal Operation)

Performance Metric	**Existing SDMN Data Channel**	**Proposed Secure Data Channel**
TCP Throughput (Mbps)	93.5514	91.8054
UDP Throughput (Mbps)	95.2845	92.3828
Latency (ms)	36.6514	37.6452
Jitter (ms)	0.34522	0.4651

The experimental results indicate that the proposed secure channel has decreased both TCP and UDP throughput by 2%. Also, it increases the latency by 3% as compared to existing SDMN data channels. The extra layer of encryption is the main reason for the reduced performance. However, the performance loss due to encryption can be minimized by using IPsec accelerators. Recent Intel processors support IPsec acceleration by allowing the use of external accelerators and/or of the new AES (Advanced Encryption Standard) instruction set.

In the next experiment, we attached a TCP SYN DoS attacker to the data channel (Hub2). Each experiment runs for 500s and the attack was performed during the 100s - 200s time interval. The average performances of the existing and proposed architectures are presented in the next table.

Table 4: Data Channel Performance under TCP DoS Attack

Performance Metric	**Existing SDMN Data Channel**	**Proposed Secure Data Channel**
TCP Throughput (Mbps)	72.1945	91.51564
UDP Throughput (Mbps)	74.4656	92.4551

Latency (ms)	548.14854	37.5146
Jitter (ms)	5.1495	0.4301

The experimental results (Table 4) indicate that the existing SDMN data channel is vulnerable to TCP DoS attacks. Both TCP and UDP throughput of existing SDMN data channels dropped by 20%. The drop is equivalent to the portion of the attack duration from the total duration of the experiment. Therefore, one can conclude that existing SDMN data channels are affected for the whole duration of DoS attack. Moreover, the latency and jitter of existing SDMN data channels have increased by 14 times over the normal operation. However, the proposed secure channel has similar performance to that of normal operation. Thus, the proposed secure channel is able to secure the SDMN data channel from DoS attacks.

In the next experiment, we attached a TCP SYN DoS and Reset attacker to the control channel (Hub1). We measure the connection delay and flow table update delay between the “DP switch 1” and the controller. Each experiment is run 25 times and the average performance of each architecture is presented in Table 5.

Table 5: Control Channel Performance under TCP DoS Attack

Performance Metric	**OpenFlow With TLS/SSL**	**Proposed Secure Control Channel**
Connection Establishment Delay (ms)	58.3224	135.4165
Connection Establishment Delay under TCP SYN DoS Attack (ms)	–	135.9145
Flow Table Update Delay (ms)	30.85645	32.1573
Flow Table Update Delay under TCP Reset Attack (ms)	–	32.2472

The experimental results (Table 5) indicate that the proposed secure channel has significantly increased the connection establishment delay. The extra HIP tunnel establishment between LSA and SecGW has added extra latency. On the other hand, the proposed secure channel has increased the flow table update delay only by 4% at steady state of operation (meaning after the connection has been established). Here again the extra layer of encryption is the main reason for the reduced performance of the proposed secure channel.

The experimental results (Table VI) also indicate that existing SDMN control channels are vulnerable to TCP DoS and reset attacks. It is not possible to establish a connection with the controller during TCP SYN DoS attack and it is also not possible to update the flow tables during TCP Reset attack. However, the proposed secure channel has similar performance as compared to the existing architecture and has no effect on these attacks. Thus, the proposed secure channel is able to secure the SDMN control channel from IP based attacks.

6. Policy Based Communication (PBC) Component

6.1 Introduction

Since future mobile networks will be packet switched, they will face challenges to protect the end-user hosts that are weakly equipped compared to their fixed counterparts, i.e. Laptops, Desktop. Following the end-to-end Internet principle, we argue that network or edge nodes shall take the responsibility of hosts they serve and protect them against malicious flows and Internet attacks. We have developed Customer Edge Switching (CES) [14] as a framework to tackle the inherent Internet threats: unwanted traffic, source address spoofing and DoS. CES allows users, hosts or applications to define their reachability policies; and hence control the traffic they deem interesting. The architecture complies with SDN principles to facilitate its deployment in future networks [15], i.e. to proactively mitigate security threats, and can be co-located with P-GW in mobile networks for fine grained security.

6.2 Proposed Solution

CES is an extension of traditional stateful firewall functionality into a cooperative firewall. The solution is a proposed replacement of NATs at network edges, separating the customer network from the public Internet. Fig 1 presents this split architecture, where the CES node acts as a connection broker for the hosts/applications that it serves and exchanges their policy offers and requirements encoded in Customer Edge Traversal Protocol (CETP) [14] with remote node. Compared to traditional stateful firewalls that either accept or drop an inbound packet, the policy-based component allows the destination node to issue additional policy queries to the sender, i.e. to eliminate address spoofing, authenticate sender and ensure policy compliance. Upon successful policy negotiation, connection is created in the CES nodes and the subsequent data packets from hosts are tunnelled using respective CETP session tags, across the networks on negotiated RLOCs.

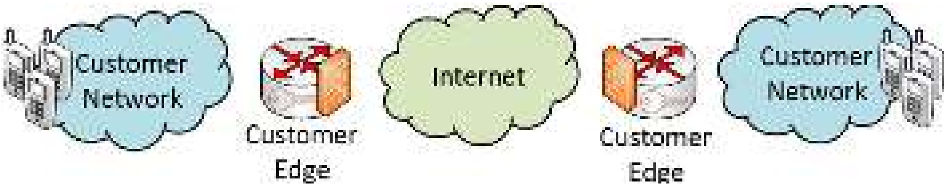

Figure 10: Policy-based communication via CES firewall at network edges

A CES node is reachable in the public Internet using a set of public addresses called Routing Locators (RLOCs) that follow the same semantics as in LISP. CES provides several policy-controlled mechanisms for establishing flow legitimacy, including negotiation of a variety of ID types, return routability checks, proof-of-works and use of secure locators. These methods and mechanisms enable CES to identify the sender and its network on a required level of assurance, prior to admitting flows in the local network. CES can provide different level of assurances based on the configured security mechanisms. These security mechanisms are available as policy-controlled features for network administrators and intend to overcome the classical internet weaknesses of address spoofing, unwanted traffic and DoS. A communication is securely established with CES if the spoofing can be eliminated, identification/authentication can be validated with a reputable source and the CETP negotiation completes using secure/trustworthy identifiers. The elimination of address spoofing in particular enables attributing the misbehaviour against stable identity of the sender and incentivizes deploying mechanisms that build the sender reputation.

6.3 Evaluation and testbed implementation

This section introduces the prototype network developed as CES proof-of-concept and describes the use cases of the technology. The figure presents the implementation of our CES testbed, which is built in the Linux environment and employs control/data plane split architecture. The setup carries two private networks that are respectively served by CES-A and CES-B. The edge of each network bears a data-path element, which implements the rules generated by the control plane and forwards the new flows towards the CES function at control plane, i.e. for security analysis, policy negotiation. The hosts and nodes in the setup are implemented as Linux containers and are connected using basic Linux networking capabilities.

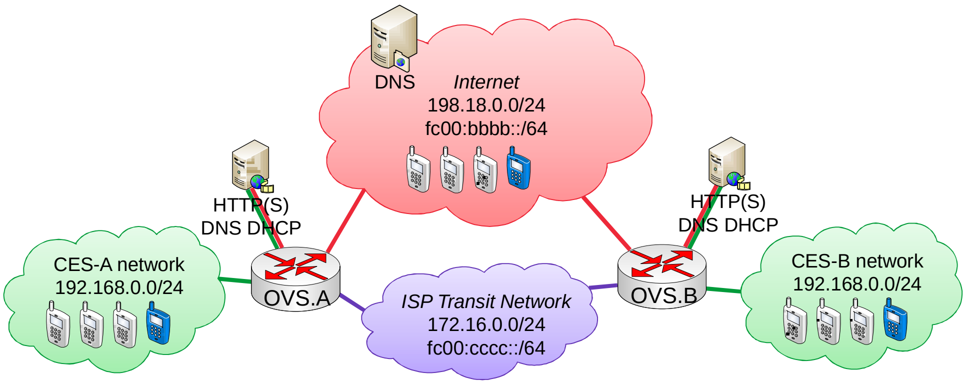

Figure 11: Experimental testbed for PBC component

Use-cases: The edge network has two external interfaces: 1) to receive flows from other CES networks, i.e. on a dedicated ISP transit link; and 2) to receive legacy traffic from the public Internet. The traffic from legacy IP networks is served by Realm Gateway (RGW) [16] functionality in CES. We aim to test both CES use cases: 1) CES-to-CES communication on dedicated links between mobile operators; and 2) inter-operability with legacy IP networks.

6.4 Evaluation results and KPI

The security evaluation measures performance penalty and effectiveness of the proposed mechanisms and their effectiveness against the malicious flows. We define the following Key Performance Indicators (KPIs) for our testing:

Session setup delay: Average connection setup time using CES prototype.

Signalling round trips: CETP negotiation rounds to create new inbound/outbound connections.

Security delay: Performance penalty or Latency of security mechanisms to connection establishment.

False Negatives: Percentage of un-detected attack packets.

False Positives: Percentage of ordinary users (or their flows) classified as attacks.

Penalty to misbehaving hosts: Firewall policies and penalties to misbehaving hosts.

These use-cases and KPIs together aim to elaborate:

• How the CES application can secure the networks against Internet-borne attacks? What is the performance penalty and latency induced by the security mechanisms?

• How effectively does RG protect the served hosts and networks against Internet attacks? What are the delays introduced to end-hosts/protocols? And whether security mechanisms exhibit any false positives/negatives?

• How CES/RG react to policy violations, and security notifications to strengthen the network security? What is the performance penalty when integrated in a control and data-plane split architecture?

Table 6: CES security testing and KPIs

KPIs	Testing Results	
Signalling round trips (RTTs)	1-RTT	2-RTT
Connection Establishment delay (msec)	80	145
Proof-of-Work Sender's delay (msec)	3	
Proof-of-Work Receiver's delay (msec)	0.001	
Certificate/Signature computation (msec) – 1st packet	2	
Certificate/Signature verification (msec) – 1st packet	1.8	

Table 6 presents the results of security testing, which reveals the performance delay and cost of the security mechanisms. Proof-of-work mechanism pushes the burden of communication towards the sender, such that the sender invests more computing cycles than the receiver. Moreover, it effectively eliminates source address spoofing in the admitted flows. As a result, the spoofed addresses failed to claim a connection state or leak traffic into the private network during the testing.

The use of CES certificates (at CETP layer) alongside signed CETP header is used for CES authentication of the remote node. The mechanism leverages an object identifier in X.509 certificates to define CES certificates and identifies the remote node as CES at a minimal processing cost by verifying the CETP header signature. CES triggers this mechanism upon the first flow from a new source address. The subsequent interactions can reutilize the validation result, reducing the verification delay to zero. Our testing did not exhibit any false positives or negatives, allowing only the flows from non-spoofed legitimate CES nodes into the private realm.

For signalling messages, the inbound CES based on the destination node's admission policies decides whether to accept the policy offers; or ask the sender for additional requirements, which may result in another round of policy exchange. Correspondingly, the evaluation of policies results in either: 1) success; or 2) failure, and this is typically achieved in one or two round trips, depending on the policies in use.

Upon receiving the first flow from a new source, CES may negotiate the CES security-policies with the sender. Depending on the complexity of these policies, there can take one or more additional round trips, in addition to the normal host-to-host policy negotiation, for the first CETP flow. As a result, the first CETP flow may establish in ~220 msec for 1-additional RTT of CES-policy negotiation or in ~300 msec for 2-additional RTTs of CES-policy negotiation. Since our testing measures the connection setup delay on zero-latency links, we will have to add the network delay to get the actual connection setup delay. To account for network uncertainties and unpredicted delays, CES state machine can absorb any host retransmissions while the CETP process is still converging.

Outcomes of security testing

The security testing leads us to state that CES security mechanisms can:

- Eliminate spoofing in the admitted traffic, i.e. admit traffic from non-spoofed sources.
- Detect bots, i.e. spoofing elimination enables tracing (and attributing) the attacks to the non-spoofed sender, i.e. bot.
- Attribute the misbehaviour to non-spoofed addresses, and can contribute to threat mitigation (at higher layers), i.e. by tracing the misbehaving host back to its customer network.
- Curb the network attacks and anti-social behaviour through cooperation between networks and enforcing penalties to *malicious* sources.
- Performance penalty (i.e. delay) introduced by security mechanisms is minimal and the testing did not exhibit any false positives/negatives.

RGW security testing

We subjected RGW to different sets of traffic to determine bounds of its security mechanisms. In this case, the testing initiates legacy connection and malicious flows towards RGW (functions hosted in CES), which serves the hosts and domains located in its network. Since RGW serves the traffic from the legacy Internet, it is exposed to all the ills of the Internet, i.e. it is susceptible to the abuse of DNS, address spoofing, botnets and connection hijacks. The goal of RGW security is to neutralize these attacks that can otherwise force network into DoS or hijack the connections reserved by legitimate clients, thus leaving it unable to accept new inbound connections or serve the legitimate users.

The security testing revealed that RGW security can: 1) eliminate source address spoofing in the admitted flows; 2) tackle the DNS floods; 3) detect and mitigate attacks from bot-controlled hosts (or botnets) with some false negatives; and 4) blacklist the aggressive (or misbehaving) hosts to mitigate DDoS. However, the testing revealed that botnet detection mechanism does exhibit some false negatives, which can be further reduced by integrating a commercial firewall solution with RGW, i.e. to harden RGW security against well-known attacks. We report the detailed testing of RGW security in [17].

7. Security information and event management (SIEM) Component

7.1 Introduction

The proposed security management monitoring component is based on SIEM techniques and additionally also on Operational Security Assurance (OSA) monitoring.

It enables the possibility to scale and integrate monitoring functions in SDN and virtual environments, deploying virtual sensors. The deployed sensors will retrieve information required by the different security monitoring tasks throughout the network, depending on the availability of monitoring resources, the information needed to guarantee network performance and resiliency. Virtualized network switches controlled by a centralized software based controller will redirect packets and enable packet forwarding to be analysed by ID & PS (Intrusion Detection and Prevention Systems). Moreover, the information collected from each sensor will be consolidated and presented by a security monitoring Graphical User Interface (GUI) on the management server side.

Mitigation actions and reactions to anomalous traffic or threats that could affect the network will be managed by the security management monitoring component (manager). This component will take as input security events generated by the sensors, and act accordingly to reconfigure the SDN controller. This can be done using REST (Representational State Transfer) API (Application Programmable Interface) based communications that will provoke automated mitigation actions that drop, isolate or redirect network traffic as needed.

7.2 Proposed Solution

Nextel S.A., Eneo and Innovalia focus in the development of a security monitoring and event management system that will analyse security event data in real time to capture pertinent network events. These events are then presented by a consolidated graphical user interface (GUI).

The proposed security solution consists of a distributed and scalable SIEM (Security Information and Event Management) architecture that includes:

- **Security Sensors:** responsible for gathering security information (i.e., having IDS features for security event detection) and reporting to the security server.
- **Security Server:** responsible for collecting security information coming from deployed security sensors. The collected information is correlated and validated against predefined security policies for final decision making. It optionally allows an automatic reaction to detected security events.

This security monitoring and event management system offers the following features:

- Security Management features:
  - Security policies definition
  - Countermeasures definition
- Security Monitoring features:
  - Asset inventory
  - Availability monitoring
  - Network monitoring (usage and latency)
  - Vulnerability discovery
  - Event detection (intrusion, anomalies, etc.)

7.3 Evaluation and testbed implementation

Nextel, Eneo and Innovalia will adapt and validate the security monitoring and event management system on an SDN based architecture, resulting in an SIEM-bases solution for SDN. For this, the following test lab scenario has been deployed.

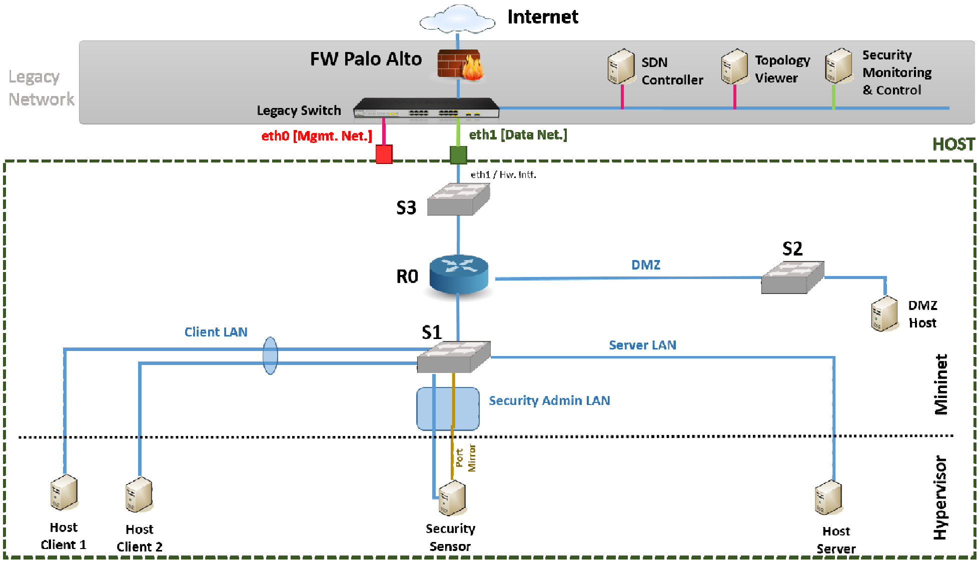

Figure 12: Proposed SDN and NFV scenario for implementing the security framework

As shown in the figure above, the platforms that will support the proposed security framework will be based on a testbed consisting of the following elements:

The different elements showed in previous diagram are referenced to virtualized security functions, which will run in virtualized environment. S1, S2 and S3 deals with virtual switches implemented, as mentioned later with OpenvSwitch. RO deals with a virtualized element for routing purposes.

- SDN related elements:
    - Floodlight v1.1 as the SDN controller
    - Open vSwitch v2.3.1 for the deployment and management of virtual switches
    - OpenFlow v1.3 protocol for control-plane flow management
    - Mininet v2.2.1 for the network emulation
    - Virtualbox 5.0.8 as the hypervisor for the deployment of end point hosts

- Physical resource elements:
    - Switches
    - Routers
    - Firewalls

- Virtual resource virtual elements:
    - L2 link, VLANs, etc.
    - L3 nets, subnets, etc.

- Security monitoring and management elements (SDN adapted SIEM):
    - Security Sensor
    - Security Server

The virtual network has been segmented into several LANs depending on the nature of the services provided; each having different security requirements:

- DMZ LAN: will include services exposed to Internet.
- Security LAN: will include security services, such as the security sensor.
- Server LAN: will include internal services.
- Client LAN: will be the end-user network.

A security use case has been defined and applied on this framework as a proof of concept of how the security solution will help detect and isolate insecure network devices before they can negatively affect the rest of the network. Upon discovering a potential threat, the SIEM identifies the problem and automatically performs the previously defined reactions to mitigate it, by interacting with the Northbound API of the SDN controller. After the threat has been resolved, the SIEM software will allow the affected devices to re-join the network.

The following figure illustrates this previously described security use case.

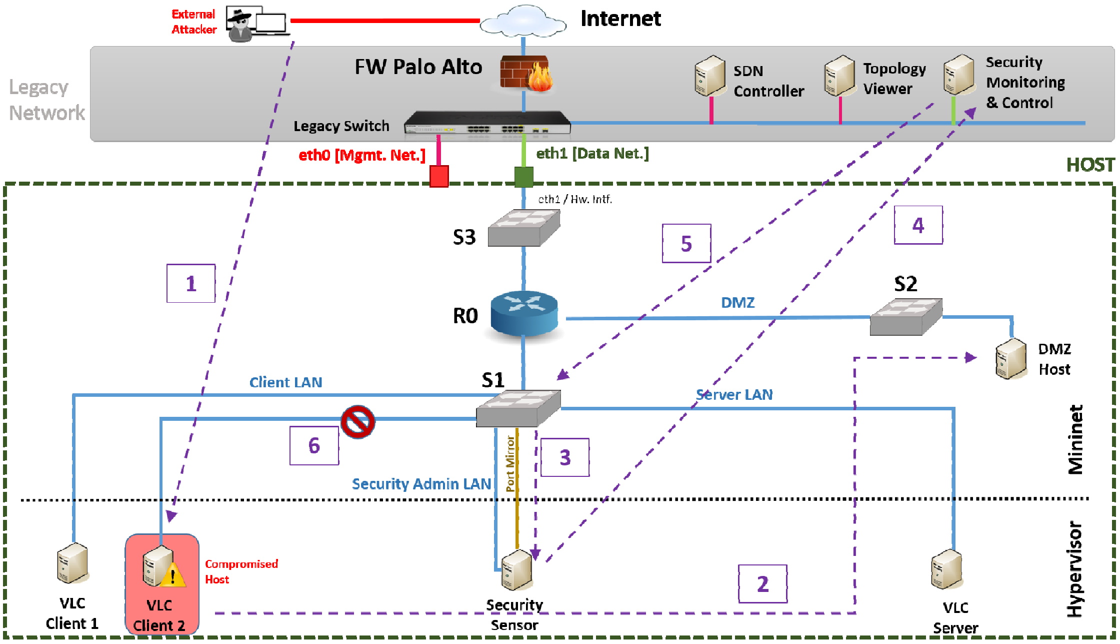

Figure 13: Proposed security use case for SDN adapted SIEM

For the purpose of the use case, a VLC server will be streaming video in the Server LAN and several VLC Clients will be consuming this video from the Client LAN.

1. The “VLC Client 2” has been compromised by an external attacker.
2. The Compromised host tries to extend the attack by launching a network discovery process over the internal networks, the DMZ LAN in this case.
3. The suspicious traffic of the network discovery is detected by the security sensor that is sniffing all the traffic crossing the virtual switch S1.
4. The Security sensor reports this security event to the Security Server, located in the legacy network.
5. The Security Server processes this event matching against a predefined security policy that tells it to immediately block, in S1, the connections to this host.
6. Security Server process the event and it is correlated in Security Server The matching security policy (which is built on the server side) triggers an action that sends an Open Flow request, through the Northbound API of the SDN Controller to the S1, to drop all the traffic related to the compromised host.

Afterwards, once the “VLC Client 2” has recovered from this security breach, a new request will be sent to S1 to re-allow the traffic from the host to the network.

To summarize, the test scenario is focused on:

- The analysis of network security event data captured in real time.

- The isolation of network elements that have been compromised before they can negatively affect the network.
- The automation of the network security remediation tasks.

7.4 Evaluation results and KPI

7.4.1 Key performance indicators

The key performance indicators that are used to evaluate the framework are:

- The number of preventive security measures which were implemented in response to identified security threats.
- The time it takes from the identification of a security threat to the implementation of a suitable counter measure.
- The latency between the attack and the mitigation.
- The latency between the detection and the mitigation.
- The number of identified security incidents, classified by severity.
- The number of security incidents causing service interruption or reduced performance.

7.4.2 Results

The expected results from the validation are focused on resolving the following issues:

- Block malicious traffic to endpoints while still allowing normal traffic.
- Improve network security policy auditing and conflict detection/resolution.
- Centralize network security service policy and configuration management.
- Automate network security remediation tasks.
- Implement more granular network segmentation for network security.

The evaluation environment has been defined under an SDN network deployment, including the security components described as part of the security solution.

The following results will present the case 1 that consists of a cyber-attack detection considering a unique source of information from the security sensor.

The test consists in detecting a port scan followed by sending ten echo requests (pings) that will be detected by the security sensor running SNORT in a virtual machine deployment as described above.

Different measurements will be showed and compiled to an average to have a perception on the results of the different response times and latencies introduced.

The following figure represents the delay time, which will be measured in seconds, between the time the attacker begins to carry out the attack to the time that the attack has been blocked.

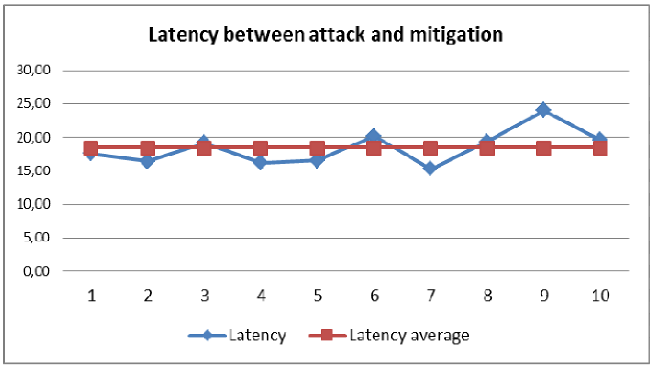

Figure 14: Latency between attack and mitigation. Case 1

The following figure represents the delay time between the detection by the correlation engine generating the alert and the attacking device being blocked.

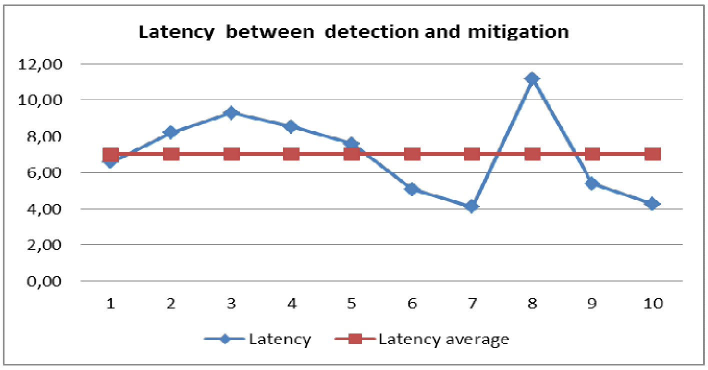

Figure 15: Latency between detection ad mitigation. Case 1

In case 2, the following results consider different sources of information from the security sensor. In this case, the response times have been evaluated using a simulation of a botnet where a host takes control of another host in the network and proceeds to download a malware file.

The compromised host and the attacker host generate a network connexion identified by the security server detecting an outgoing connection from the botnet web server.

The compromised host downloads a malware file that is also detected by the security sensor. In addition, a malware engine analyses the downloaded file and assigns a score, in order to determine if it should be considered as malware.

The following figure represents the delay time between the time the attackers begins to carry out the attack to the time that the attack has been blocked.

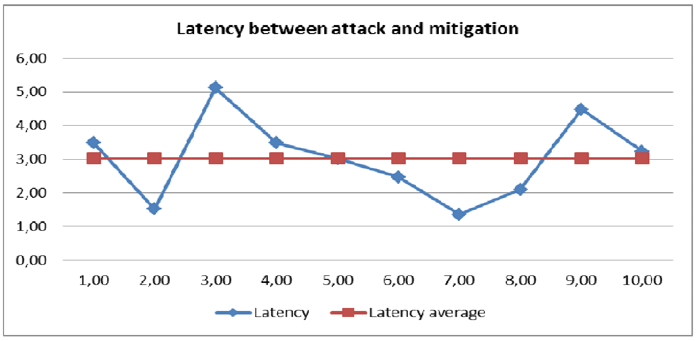

Figure 16: Latency between attack and mitigation. Case 2

The following figure represents the delay time between the detection by the correlation engine generating the alert and the attacking device being blocked.

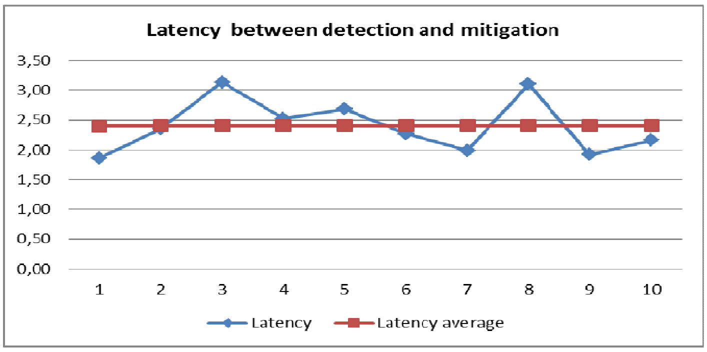

Figure 17: Latency between detection and mitigation. Case 2

7.4.3 Conclusions

The results of the validation show that it is possible automate mitigation and reaction actions in SDN scenarios by providing countermeasures and mitigation actions directly using a RESTful API to the SDN controller. Different latency times between the attack and its mitigation have been presented.

The result of the validation also shows that multiple sources of information can be combined and will help to provide more accurate and rapid detection of the cyber-attack scenarios demonstrated. Improving the performance of combining multiple sources to mitigate attacks will be crucial for future and further work.

8. Security Management and Monitoring (SMM) Component

8.1 Introduction

The architectural possibilities studied and proposed in the SIGMONA project involved extending the Open Flow type interfaces, the SDN CTRL INTERFACE (referred to as SDM CTRL INTERFACE in Figure 3). This would allow obtaining the packet and flow metadata needed by the security applications (e.g., the modules referred to as Management/Monitoring/Security, Applications and Network Services) from either the switches or the probes (i.e., agents). The probes can be passive (e.g., the module Traffic Monitoring and Analysis that analyses mirrored traffic) or active (e.g., the modules Active Probe acting as a firewall that filters traffic). The SDM-CTRL acts as a controller for the software and hardware security devices and could be integrated to the SDN-CTRL or separate. If separate then it will interact with the SDN-CTRL via an Open Flow type interface. The architecture of the devices and controllers can be hierarchically organised or distributed (e.g., with peer-to-peer communications between the controllers).

8.2 Proposed Solution

A security and management monitoring tool developed by Montimage is being adapted to support the SDM CTRL interface and a prototype of the SDM CTRL will be implemented to be able to perform tests and evaluate the scalability and performance of the solution. These modules will be deployed in an existing internal platform consisting of two servers. Montimage will then validate the virtualisation of the DPI function in an SDN environment and validate the deployment of rules to detect abnormal behaviour and security problems. This function will be integrated in the French testbed. Note that this work is ongoing and results will be obtained by the end of March 2016. This is due to the fact that the French consortium started very late and will continue to work past the initial end date of the SIGMONA project (January 2016).

The added modules and interfaces are:

- Modules:
    - Security sensor: an active monitoring probe for the detection of security and behaviour related information (e.g., security properties and attacks) and mitigation (e.g., filtering). It can be installed on the Network Elements or in network taps (passive network observation points).
    - SDM CTRL: a new module or extension of SDN CTRL to allow control of monitoring function (e.g., management of network monitoring appliances, traffic mirroring, traffic load balancing and aggregation); accepts requests from network functions and applications…). SDM CTRLs are distributed following either a peer-to-peer or hierarchical model. They interact with the Management/monitoring/security function and act as distributed analysis or decision points for the defined security policies (security SLAs).
    - Network monitoring: a virtualization of monitoring function (i.e., part of the traffic analysis moved to the cloud).
    - Traffic Mirroring and Analysis: a passive backhaul traffic monitoring device required by different network functions.
- Interfaces:
    - SDM CTRL INTERFACE: an interface that allows controlling the use of monitoring resources, recuperating traffic or metadata for analysis. It allows performing monitoring requests and obtaining status, so that applications and network functions can send requests for monitoring based information, and monitoring functions can send status and recommendations.

By programming flexible switches and other network devices to act as packet interception and redirection platforms, it is possible to detect and mitigate a variety of attacks. By introducing SDN-driven security analysis (or Software Defined Monitoring), SDN-enabled switches, packet processing and security appliances can act as packet brokers. Controllers can act to aggregate and correlate distributed meta-data (e.g., flow and statistical data). This information can be sent to monitoring and analysis appliances and applications. In this way it is possible to obtain adaptive and optimised monitoring, analysis and mitigation.

8.3 Evaluation and testbed implementation

Test scenarios or use cases have been elaborated, in particular to show:

- How the SDM CTRL interacts with the SDN CTRL or uses the SDN CTRL interface to mirror the traffic so that it is analysed to detect certain types of attacks (e.g., scans from known bad hosts or infected machines).
- How the SDM CTRL interacts, via the SDM CTRL interface, with an active probe to deploy a new filtering rule.
- How the SDM CTRL interacts with the SDN CTRL or uses the SDN CTRL interface to send part of the traffic to a probe running in the cloud for analysis.

Furthermore, the validation platform will be used to assess the following:

- The virtualisation of DPI-type monitoring for security purposes.
- The procedure to configure and deploy this function.
- The possibility of analysing both signalling and data links.

and validate (at least partially) the following basic assumptions:

- Assumption on managing the security: How to include security functions of physical and virtual elements and interfaces;
- Verification of the flexibility introduced, and assessment of the possibilities of virtualised security monitoring of physical and virtual network elements.

8.4 Evaluation results and KPI

The following KPI will be used to evaluate the SMM solution:

- Measure scalability, in terms of cost and performance, of monitoring data and control interfaces. Compare monitoring in virtual and physical scenarios.
- Quantitative analysis: Measure resources needed to monitor network behaviour in different bandwidths settings (e.g., 100M, 1G, 10G). Measure any loss of precision due to loss of information.
- Determine scalability graph that depicts:
  - Functionality: different levels of analysis and methods used;
  - Cost: estimated cost of CPU/Memory/HW needed and deployment/operation efforts;
  - Performance: resources needed with respect to functionality and timeliness of detections.
- Compare monitoring in virtual and physical scenarios in the detection and localisation of network security problems.
- Qualitative analysis: Determine the flexibility and effectiveness to detect and locate origin of security breaches.
- Determine the advantages (if any) in correlating metadata captured from the physical and virtual equipment and functions.
- Qualitative analysis: Determine advantages in using metadata from different sources.

9. DPI Based Threat Detection Component

9.1 Introduction

DPI technology allows security applications to inspect the content of each packet of data streams and, thus, help identify harmful traffic. The DPI security solutions integrated to a mobile network can identify the subscribers that are generating malicious traffic and even automatically take actions to eliminate the threat and/or decrease the impact to overall network security and performance.

9.2 Proposed Solution

EXFO is proposing a DPI component that can work with mirrored traffic or integrated to a virtual switch to capture packets for analysis. In both modes, the component can also have the capability to inform other SDMN components about malicious traffic flows. This enables reactions to the security threats by modifying behaviour of traffic flows.

The proposed DPI component provides continuous real time security monitoring of traffic flows. The detections as well as overall flow data is stored to a local database that is utilized by the monitoring user interface and is able to provide overall status of network state as well as analyse detections in detail. Moreover, the user interface enables the analysis of security actions and their effects to network behaviour.

The proposed threat detection functions can be implemented as a virtual network function or using dedicated hardware solution for the DPI analysis. The virtualized solution can provide several benefits such as:

- Scalability: the analysis instances can be dynamically created and deleted based on traffic conditions.
- Reduced investment and maintenance costs: there is no need for dedicated hardware.

The solution implemented with dedicated hardware may provide better overall performance without the security drawbacks that may be introduced by the virtualization.

9.3 Evaluation and testbed implementation

Within DPI technology there can be several means to detect malicious traffic flows and therefore improve the network security level. In the testbed implementation, EXFO focuses on DPI based finger print analysis. The developed prototype for security threat detection is based on the DPI component used in EXFO’s Prower Hawk Pro software. The DPI component was adapted to analyse and prevent security threats related to application data flows matching with mobile malware rule database.

The effectiveness of the threat detection is greatly affected by fingerprint accuracy. For the testbed implementation, the mobile malware information with regular updates was provided by the Finnish F-Secure Company for several protocols such as HTTP, SMTP, IRQ, and FTP. The malware information was then used to generate the protocol specific malware fingerprints.

In general, there are no limitations for the applied protocols as long as they are supported by the underlying DPI component and that the malware information is available. The test bed solution concentrates on the analysis of HTTP application flows. In this way the work effort needed for testbed implementation was reduced, but the results remain pertinent since the HTTP protocol represents the main traffic that needs to be analysed from a security standpoint.

The detections are then written to the local database or optionally provided directly to the other network functions. As addition, packets related to the detected flows are written to local file storage. The local storages are then made available to the monitoring GUI used to analyse traffic flows and detections. The test bed components are illustrated in the following figure.

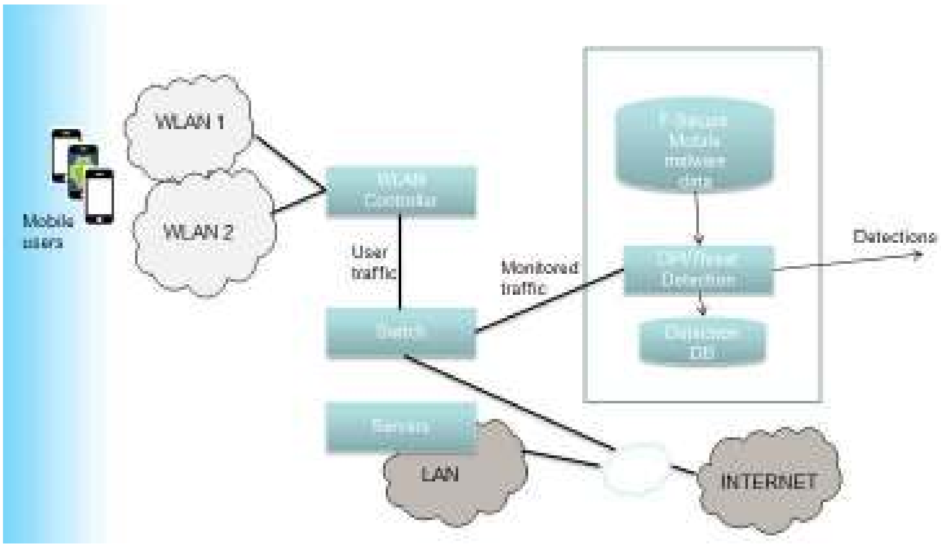

Figure 18: EXFO testbed components

The applied DPI component was installed in hte EXFO PowerHawk Probe HW that captured and analysed all the traffic flows of the EXFO Company's WLANs. Typically, there were from 50 to 100 mobile phones connected using different kinds of internet and internal services via WLAN. According to the original plans, the test bed implementation was also to be evaluated as a virtualized service, but this part was left out from the testbed solution due to the limited resources available for the evaluation phase.

9.4 Evaluation results and KPI

As part of the network monitoring solution, the testbed implementation stored detections to the local raw file storage and detection database.

The defined KPIs are:

- Average processing delay. The KPI indicates additional latency for application flows due to the analysis.
- Average detection delay. The KPI indicates the time used to generate detection events after receiving the packet.
- CPU usage ratio. The KPI indicates increase of CPU usage compared to typical DPI based application profile analysis.

In the evaluation we concentrate on performance aspects of the proposed threat detection component. Average packet processing delay and average detection delay KPIs indicate an overhead caused by the proposed component when implemented with the dedicated hardware.

Due to the extended functionality over the existing DPI component, CPU usage was increased by several percentage points.

10. Dissemination, discussions and future directions

SIGMONA WP4 work has produced the following considerable results:

- Books
  - Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture , Wiley, 2015.

- Book chapters
  - Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, A case study on security issues in LTE backhaul and core networks , Book Chapter, to appear in B. Issac (ed.) "Case Studies in Secure Computing – Achievements and Trends"- Taylor & Francis, 2013.
  - Title: “Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture”. Editors: Madhusanka Liyanage, Andrei Gurtov, Mika Ylianttilla. Publisher: WILEY Publishers.
    - Chapter 18: “Security Aspects of SDMN”, Edgardo Montes de Oca, Wissam Mallouli
  - Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, IP based Virtual Private Network implementations in Future Cellular Networks , Book Chapter, to appear in M.A. Matin (ed), "Handbook of Research on Progressive Trends in Wireless Communications and Networking"- IGI Global Publications, 2013.

- Journal paper
  - R. Kantola, J. Llorente and N. Beijar, “Policy Based Communications for 5G Mobile with Customer Edge Switching,” in Special Issue on Software Defined Networking Security of Security and Communication Networks (SCN), Wiley.
  - Madhusanka Liyanage, Pradeep Kumar, Mika Ylianttila, Andrei Gurtov, Novel Secure VPN Architectures for LTE Backhaul Networks , to appear in Security and Communication Networks- Wiley Online Library, 2015.
  - Madhusanka Liyanage, Ahmed Bux Abro, Mika Ylianttila, Andrei Gurtov, Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective , to appear in IEEE Security and Privacy, 2015.
  - Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Secure Hierarchical VPLS Architecture for Provider Provisioned Networks , to appear in IEEE Access, 2015.

- Conference papers
  - Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Securing the Control Channel of Software-Defined Mobile Networks , to be appeared in Proc. of 1st IEEE WoWMoM Workshop on Software Defined Networking Architecture and Applications, Sydney, Australia. June 2014.
  - Jose Costa-Requena, Jesús Llorente Santos, Vicent Ferrer Guasch, Kimmo Ahokas, Gopika Premsankar, Sakari Luukkainen, Ijaz Ahmed, Madhusanka Liyanage, Mika Ylianttila, Oscar López Pérez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, SDN and NFV Integration in Generalized Mobile Network Architecture , to be appeared in Proc. of European Conference on Networks and Communications (EUCNC), Paris, France. June 2015.
  - Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila, Jesús Llorente Santos, Raimo Kantola, Oscar López Pérez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, Asier Valtierra, Carlos Jimenez, Security for Future Software Defined Mobile Networks , to be appeared in Proc. of 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST,2015), Cambridge, UK. September 2015
  - R. Kantola, "Implementing Trust-to-trust with Customer Edge Switching.," in AINA, WS on Advances in Mobile Computing and Applications: Security, Privacy and Trust, Perth, Australia, 2010.
  - P. Leppäaho, J. Llorente Santos, R. Kantola, and N. Beijar, "Traversal of the Customer Edge with NAT-unfriendly Protocols," in ICC, 2013.

- J. Llorente Santos, R. Kantola, N. Beijar, and P. Leppahalo, "Implementing NAT Traversal with Private Realm Gateway," in ICC, 2013.
- H. Kabir, R. Kantola, and J. Llorente Santos, "Security Mechanisms for a Cooperative Firewall," in CSS, Paris, 2014.
- J. Llorente and R. Kantola, "Transition to IPv6 with Realm Gateway 64," in IEEE Int. Conf. on Communications, ICC 2015, London, UK, 8-12 June 2015.
- Jose Costa-Requena, Jesús Llorente Santos, Vicent Ferrer Guasch, Kimmo Ahokas, Gopika Premsankar, Sakari Luukkainen, Ijaz Ahmed, Madhusanka Liyanage, Mika Ylianttila, Oscar López Pérez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, SDN and NFV Integration in Generalized Mobile Network Architecture , to be appeared in Proc. of European Conference on Networks and Communications (EUCNC), Paris, France. June 2015.

- Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila, Jesús Llorente Santos, Raimo Kantola, Oscar López Pérez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, Asier Valtierra, Carlos Jimenez, Security for Future Software Defined Mobile Networks , to be appeared in Proc. of 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST,2015), Cambridge, UK. September 2015.
- Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN , to be appeared in Proc. of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA. January 2016.
- C11) Madhusanka Liyanage, Ijaz Ahmad, Mika Ylianttila, Andrei Gurtov, Ahmed Bux Abro, Edgardo Montes de Oca Leveraging LTE Security with SDN and NFV , to be appeared in Proc. of 10th IEEE International Conference on Industrial & Information Systems (ICIIS), Peradeniya, Sri Lanka, December 2015.
- Jude Okwuibe, Madhusanka Liyanage, Mika Ylianttila Performance Analysis of Open-Source Linux-Based HIP Implementations , to be appeared in Proc. of 10th IEEE International Conference on Industrial & Information Systems (ICIIS), Peradeniya, Sri Lanka, December 2015.
- Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov, Secure Virtual Private LAN Services: An Overview with Performance Evaluation , to be appeared in Proc. of IEEE ICC 2015 - Workshop on Advanced PHY and MAC Techniques for Super Dense Wireless Networks, London, UK. June 2015.
- Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, A Novel Distributed Spanning Tree Protocol for Provider Provisioned VPLS Networks , to be appeared in Proc. of IEEE Conference on Communications: ICC 2014, Sydney, Australia. June 2014.
- Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Secure Hierarchical Virtual Private LAN Services for Provider Provisioned Networks , to appear in Proc. of IEEE 1st Conference on Communications and Network Security: CNS 2013, Washington DC, USA. October 2013.
- Madhusanka Liyanage, Andrei Gurtov, A Scalable and Secure VPLS Architecture for Provider Provisioned Networks , to appear in Proc. of IEEE Wireless Communication and Networking Conference: WCNC 2013, Shanghai, China. April 2013.

Utilization of IPsec tunnels introduced extra performance penalty. In future, it will be interesting to solve this issue by utilizing cloud resources to enhance the performance of the proposed IPsec tunnelling architecture and using external accelerators and/or using new AES (Advanced Encryption Standard) instruction sets for processors.

Integration of threat detection and other DPI functions to EXFO virtual analyser component (vAnalyzer) looks to be the most promising topic for the future activities. Architecture of vAnalyzer and refences to ETSI NFV architecture has been defined in SIGMONA WP2. Exchanging performance of the virtualized threat detection component means of improved scalability, load balancing and other potential means should be the main concern.

The future research focus at Aalto will be to improve the CES prototype, in particular: 1) study the dynamic policy management architectures with CES; 2) integrating a commercial firewall solution with CES to further harden its security; and 3) perform wide-scale testing of the protection mechanisms.

11. ANNEX. Mapping SDMN security to NFV architecture

The following picture describes the different security modules implemented and the effort to mapping to the NFV [19] reference architecture, as a result of the work also done in SIGMONA WP1[20].

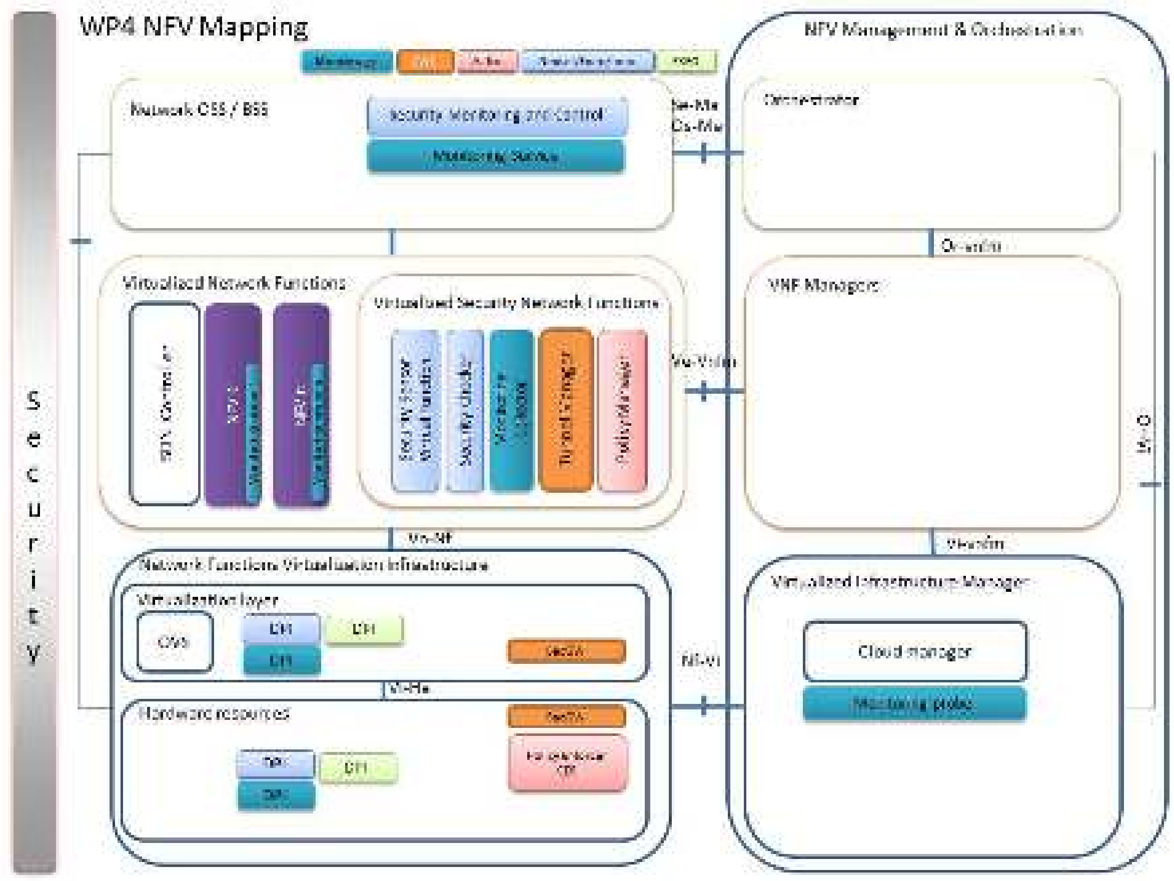

Figure 19: NFV architecture mapping

The components described in this architecture are mapped to the different components described in this deliverable.

A virtualised security network function developed by Nextel, Eneo and Innovalia includes a Security sensor virtual function and a Security checker. These components recollect information from virtualisation layer using DPI techniques and others and will consolidate this information together with network and security conditions. The information compiled in the Virtualised Security Network Functions will be consolidated in Security Monitoring and Control component, which will represent a more that useful information for security monitoring and awareness management.

Interfaces description of these components, Security Monitoring and Control interacts with northbound API of the SDN controller, to deploy security countermeasures in accordance with security events and threats detected by the Virtual Security Network Functions deployed sensor and consolidated in the Security Monitoring and Control. Interface between virtualised security functions and network functions Vn-Nf, should provide virtual network monitoring mirrored port to the sensor. Interface between Network function virtualised and virtualised infrastructure manager should provide configuration about the forwarding ports in the virtual switches implemented with Open vSwitch, required to be managed to provide required visibility.

A security and management monitoring tool developed by Montimage includes a security and QoS performance probe (i.e., sensor or monitoring agent) that captures the metadata needed by the different network functions to assure network reliability. This probe is deployed in the virtual machines hosting the different network functions. It serves to monitor the ongoing activity to detect security and performance events and incidents that can either trigger an automated local reaction or report to the centralised monitoring service part of the OSS/BSS management system. In turn, the centralised monitoring service allows analyzing the events and incidents, correlating the information received, present this information to the human operators, and act as a decision point to remediate any deficiencies in an automated or semi-automated way.

The management of the probes will be carried out by the centralised service. This system brings the possibility of deploying and enforcing policies and rules related to the network functions and services (and not just of the virtual machines as provided by the VIM), and gives operators improved visibility and control of their networks.

12. Conclusions

According to the topics covered attending security concerns in WP4 different partners involved have proposed each specific validation environments.

- Security between control plane and data plane.

  CWC related work in WP4 has described a platform selection and concrete validations, attending the main focus which is synchronizing the network security and network traffic. The main purpose of the validation testbeds proposed is to analyse the penalty of security due to proposed architectures on throughput, jitter and latency parameters and study the expected protection from proposed architecture under different IP based attacks such as TCP SYN DoS, TCP reset and IP spoofing attacks. Similarly, policy consistency techniques will be developed that will check that forwarding rules follow the security policies and check that security policies are in place with node mobility.

- Security implementations in the data paths.

  Aalto University related work in WP4 has described a platform and concrete validations alternatives to implementing security in the data path. As detailed in this deliverable tests are focused in trying to enable policy-based communications in a deployed SDN network especially enforcing policies when participate remote hosts accessing from the Internet where the security is supposed to be weaker. By enabling a policy negotiation, the edge nodes can assure certain level of *trust* relative to the current hazard evaluation. This means that policies can be dynamically modified, either loosens or made more strict, according to the trustworthiness of the remote actor and previous behavior. In addition, this validation environment will include new mechanisms to detect most common security threats inherent to the Internet model, such as DDoS, source address spoofing and also DNS based attacks.

- Security management and monitoring.

  Different partners inside WP4 will face the security management and monitoring under the scope of SIGMONA as demonstrating applying security in SDN, NFV, and cloud environments. Montimage related work in WP4 is described in this deliverable, where a high level description of the validation platform that will be used is presented. This will serve to validate some aspects deemed important of security monitoring of SDMN, virtual networks and virtualised functions. In particular through this setup, it will be investigated how the SDM CTRL should interact with the SDN CTRL to manage and control active probes deployed for security analysis, threat prevention and mitigations. Likewise, Montimage research work will investigate on how at least part of the security monitoring tasks can be virtualised, how the traffic or extracted meta-data can be analysed by a probe running in the cloud, and how the monitoring can analyse virtual connections and signalling to detect any abnormal behaviour.

  Nextel S.A., Eneo and Innovalia related work in WP4, is described with a detailed architecture of components applied to the test bed, implementing an SDN and SDMN based network where applicable use case related enhanced security information and event management in this environment will be tested. Detection of network events and threats in the testbed scenario integrating the required components in a virtual network will be validated, deploying a security solution. Finally this work will research also in enhanced reaction communicating different components.

  Exfo related work is focused in the testbed to build the prototype of the DPI based threat detection component and validate its capabilities in the SDMN context.

13. References

[1] K. Pentikousis, Y. Wang, and W. Hu, “Mobileflow: Toward software defined mobile networks,” Communications Magazine, IEEE, vol. 51, no. 7, 2013.

[2] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, “NFV: State of the Art, Challenges and Implementation in Next Generation Mobile Networks (vEPC),” arXiv preprint arXiv:1409.4149, 2014.

[3] M. Liyanage, M. Ylianttila, and A. Gurtov, Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. Wiley, 2015.

[4] J. Costa-Requena, V. F. Guasch, and et. al., “SDN and NFV Integration in Generalized Mobile Network Architecture,” in European Conference on Networks and Communications (EUCNC), Paris, France. IEEE, 2015.

[5] C. Meyer and J. Schwenk, “Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses.” IACR Cryptology ePrint Archive, vol. 2013, p. 49, 2013

[6] D. Kreutz, F. Ramos, and P. Verissimo, “Towards secure and dependable software-defined networks,” in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 55–60.

[7] M. Liyanage, M. Ylianttila, and A. Gurtov, “Securing the control channel of software-defined mobile networks,” in A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on. IEEE, 2014, pp. 1–6.

[8] R. Axelrod, “The evolution of cooperation: revised edition,” Basic books,vol. 185, p. 186, 2006.

[9] Liyanage, Madhusanka, Andrei Gurtov, and Mika Ylianttila, eds. Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. John Wiley & Sons, 2015.

[10] Liyanage, Madhusanka, et al. "Security for future software defined mobile networks." Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on. IEEE, 2015.

[11] Liyanage, Madhusanka, et al. "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective." IEEE Security and Privacy Magazine (2015).

[12] R. Beckett, X. K. Zou, S. Zhang, S. Malik, J. Rexford, and D. Walker, “An assertion language for debugging SDN applications,” in Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, ser. HotSDN, vol. 14, 2014, pp. 91–96.

[13] McKeown, Nick, et al. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38.2 (2008): 69-74.

[14] H. Kabir, R. Kantola and J. Llorente Santos, “Security Mechanisms for a Cooperative Firewall,” in CSS, Paris, 2014.

[15] R. Kantola, J. Llorente Santos and N. Beijar, “Policy based Communications for 5G Mobile with Customer Edge Switching,” Security and Communication Networks, 2015.

[16] J. Llorente Santos, R. Kantola, N. Beijar and P. Leppahalo, “Implementing NAT Traversal with Private Realm Gateway,” in ICC, 2013.

[17] H. Kabir, J. Llorente Santos, R. Kantola, O. López, M. Liyanage and E. Montesdeoc, "Security Framework based on Customer Edge Switching," 2015

[18] ***Ahmad, I***.; Namal, S.; Ylianttila, M.; Gurtov, A., "Security in Software Defined Networks: A Survey," in *Communications Surveys & Tutorials, IEEE* , vol.17, no.4, pp.2317-2346, Fourthquarter 2015. doi: 10.1109/COMST.2015.2474118

[19] ETSI ISG NFV Architectural Framework, ETSI GS NFV 002 (V1.2.1, 2014-12): http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[20] SIGMONA D1.2 Software Defined Mobile Network Architecture