Leveraging LTE Security with SDN and NFV

Madhusanka Liyanage*, Ijaz Ahmad, Mika Ylianttila
University of Oulu, Oulu, Finland

Andrei Gurtov
Aalto University, Espoo, Finland

Ahmed Bux Abro
VMware, California, USA

Edgardo Montes de Oca
Montimage, Paris, France

***Abstract*—In this paper, we study the current and emerging security mechanisms to protect the LTE (Long Term Evolution) architecture. We also highlight the limitations of legacy LTE security mechanisms. SDN (Software Defined Networking) and NFV (Network Function Virtualization) are positioned as innovative concepts to improve overall LTE security posture. This paper proposes enhancements to the legacy security mechanisms and introduces new security applications based on SDN and NFV technologies. The performance of proposed SDN based LTE security architecture is analyzed with simulations.**

***Index Terms*—SDN, NFV, LTE, Security, Mobile Networks**

I. Introduction

The introduction of IP based LTE architecture has significantly changed the behavior of telecommunication networks. IP based LTE networks not only provide high bandwidth, simplified network control but also support a wide range of heterogeneous network services. However, the latest all-IP LTE network architecture is now exposed to complex IP origin threat vectors on the top of legacy mobile security challenges [1] [2]. On the other hand, the introduction of various mobile broadband and network services are also originating new security challenges and threat vectors [2].

However, legacy LTE security mechanisms are isolated, uncoordinated, complex and rigid to meet the security requirement of future mobile network services. Future LTE networks need an inclusive and intrinsic security model across the entire mobile network. Enhanced visibility, real time threat detections, centralized intelligence and network wide control are required features to design a scalable, dynamic and optimized security mechanism for future LTE networks.

In these grounds, SDN and NFV concepts are the promising technologies which offer capabilities to solve the limitations in legacy LTE security mechanisms. SDN and NFV offer the required improvements in visibility, flexibility, scalability and coordination to design high performing security mechanisms for LTE networks [3].

This paper proposes a new security architecture for LTE networks based on SDN and NFV concepts. It also highlights how SDN and NFV features can be used to overcome the limitations in present-day LTE security mechanisms. Moreover, we analyze the performance of SDN based security architecture with the existing LTE security mechanisms in a simulation environment.

The rest of the paper is structured as follows. Section II provides the background of LTE network architecture, SDN and NFV concepts. Section III describes LTE security architecture and its limitations. Section IV describes enhanced SDN based security architecture for LTE networks. It also presents the expected benefits and current limitations of SDN based LTE security architecture. Section V and VI contain the numerical results and the conclusion of the article.

II. Background

A. Long Term Evolution (LTE) Architecture

The LTE architecture was standardized as a part of 4G (4th Generation) networks. LTE proposes an all-IP network architecture called EPS (Evolved Packet System). It can be divided in to two systems: E-UTRA (Evolved Universal Terrestrial Radio Access) and EPC (Evolved Packet Core) [2]. Figure 1 illustrates the LTE architecture.

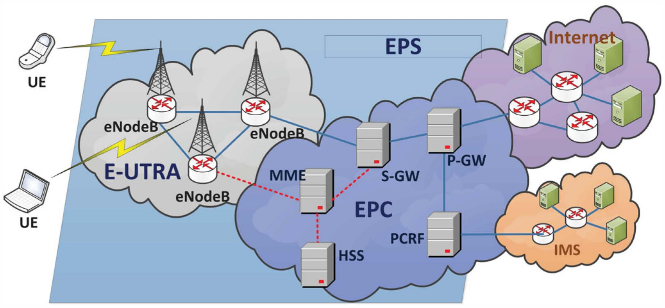

Fig. 1: The LTE Architecture

E-UTRA is the radio access network of the LTE transport network. It contains eNodeBs (evolved NodeBs) and interconnections (X2 interface) between them. EPC is the core network segment of the LTE transport network. It contains network control elements such as Mobility Management Entity (MME), Home Subscriber Server (HSS), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), and Policy and Charging Rules Function (PCRF). Finally, LTE EPC is connected to the external networks, such as the Internet, IP Multimedia Core Network Subsystem (IMS) and roaming networks [2], [4].

Recent research work is highly focused on 5G (5th Generation) networks by developing new network architectures. However, it is expected that 4G LTE will still be utilized during

*Corresponding author. Email: madhusanka@ee.oulu.fi

978-1-4799-1876-8/15/$31.00 ©2015 IEEE

the next few decades [5]. Therefore, it is equally important to improve the performance and security of existing LTE networks in order to address the demands of future traffic needs.

B. Software-Defined Networks (SDN)

Software-Defined Networking (SDN) is considered as the new norm for future networks [6], [7]. SDN proposes to decouple the control and data planes of the network. It places the control functions outside of the switches and enables external control through a logical software entity called the network controller. SDN based networks support simple abstractions to describe the underlining devices, the functions and features they support, and a network protocol to manage the forwarding plane from a remote controller via a secure control channel [7].

The value of SDN in mobile networks lies specifically in its ability to provide new capabilities like centralized control, abstraction, network virtualization, common device standards and automation [6]–[9]. These features are useful for designing scalable, dynamic and optimized security mechanisms [9].

C. Network Function Virtualization (NFV)

Traditionally, network operators have always used dedicated and specially designed black box type network equipment to construct their networks. However, this approach inevitably leads to high time-to-market and costs (CapEx). It also requires a dedicated staff (OpEx) to deploy and run the networks. NFV technology aims to build an end-to-end infrastructure that enables the consolidation of many heterogeneous network devices by moving network functions from dedicated hardware onto general purpose computing/storage platforms such as servers [10], [11].

The main idea behind NFV is to virtualize a set of network functions by deploying them as software packages in a cloud environment [10]. This is also known as network softwarization. In such systems, network functions are implemented independent of the physical resources and are deployed in virtualized environments, such as mobile clouds, so that a given service is available to many devices on a demand basis. SDN is the key enabler of NFV.

III. LTE Security Architecture

A. LTE Security Principles and Architecture

With the evolution to LTE technology, mobile networks have been transformed to a new all-IP based transport network architecture. It provides IP based end-to-end communication from eNodeBs in Radio Access Network (RAN) to core network elements in EPC. While this flat architecture has simplified the operation of mobile network, it has increased the overall risk of vulnerabilities and threats. Therefore, the challenge is to design a complete and effective security defense framework which can provide fault isolation as well as protect the interworking of legacy and non-3GPP networks.

The 3rd Generation Partnership Project (3GPP) has defined an LTE security architecture that covers security features, mechanisms and procedures for each section of EPS [12]. Figure 2 illustrates the 3GPP security architecture.

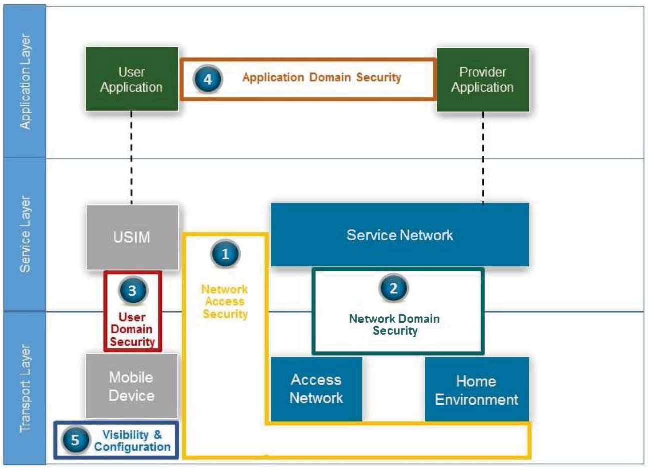

Fig. 2: 3GPP Security Architecture [12]

3GPP security architecture has been divided into five domains as follow:

1) Network access security: ensures that mobile users have secure access to network services and mobile network is secured against attacks via the (radio) access link.

2) Network domain security: ensures that mobile backhaul nodes to securely exchange signaling data and user data at the mobile backhaul networks and protects against attacks on wireline link.

3) User domain security: secures access to mobile stations.

4) Application domain security: allows applications on user and network side to securely exchange data.

5) Visibility and configurability of security: allows user to get information about enabled security features and provision of services.

B. LTE Security Architecture

Present-day LTE network operators use a wide range of security mechanisms in each domain. Figure 3 illustrates the deployment of security mechanism in today's LTE networks [9].

LTE security architecture contains different security mechanisms at different levels. First of all, E-UTRA reuses the security mechanisms which were used in 2G/3G network. For instance, LTE uses USIM cards in User Equipment (UE) and RNL (Radio Network Layer) encryption for radio links [1], [2], [13]. In addition, LTE introduces new security mechanisms, such as: key derivation mechanism during mobility (KASME), protection of radio interfaces (PDCP frames, user session ciphering, RRC radio signaling integrity control and ciphering) [2]. LTE introduces a new interface called X2 to exchange the user and signalling data at EUTRA. GTP (GPRS Tunnelling Protocol) and IPsec tunnels are used to protect X2 interface.

EPS also adapts 2G/3G security mechanisms to obtain an optimised security architecture by embedding confidentiality

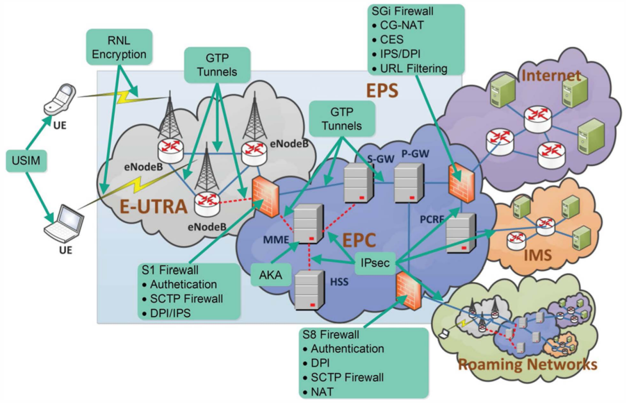

Fig. 3: LTE Security Architecture

and integrity mechanisms in the EPS protocol stack [4]. For instance, AS (Access Stratum) signalling integrity and encryption protects RRC (Radio Resource Control) protocol [1]. In LTE, MME identifies UEs by using the authentication data from the home network and triggering the AKA (Authentication and Key Agreement) protocol in the UE. This process will share a KASME key (Access Security Management Entity Key) [2]. Further keys can be derived for confidentiality and integrity protection at the NAS (Non-Access Stratum) level. IPsec tunnels are used to protect the integrity of backhaul traffic. They are used to protect signalling and user data in many EPC interfaces such as X2, S1-MME, S1-U, S8 and S11.

C. Limitations on LTE Security Architecture

LTE Security is built on prior 2G/3G security mechanisms with some improvements that include better security algorithms, longer keys, extended key hierarchy and the introduction of new features to address backhaul and relay node security. Nevertheless, it inherits many of the flaws mainly due to the complexity and fragmentation of the security model, the dependence on distributed and uncoordinated security mechanisms, and its decentralized control. Other limitations are the following:

1) Open Mobile Networks: Pre-LTE era mobile networks were basically a closed system with specialized security controls built-in to the communication protocols. An extensive knowledge and expertise were required to break into these systems. On the other hand, LTE and new mobile architecture were designed to be more flexible and supportive to outside networks such as partner roaming networks, IMS and the Internet. All voice and data services are now served over the IP protocol.

This openness has offered agility. However, it has exposed the network to new threat vectors such as IP spoofing, network worms and DDoS attacks [2] [4].

2) PIN (Place In Network) Based Security Model: Most of the security controls in today's LTE security architecture are point based implementations. For instance, NAT (Network Address Translation), DPI (Deep Packet Inspection), IDS (Intruder Detection Systems), CES (Customer Edge Switching), firewalls are applied only at the Internet, mobile access and roaming borders [1] [2]. They offer dedicated security functions for network points. Thus, security is heavily focused on externally originated attacks [8], while little focus is applied to address the internally originated attacks.

3) Isolated Security Model: A diverse set of non-coordinating security mechanisms are deployed in different sections of the mobile network [1] [4]. Furthermore, most of the security functions are applied in an isolated fashion with a dedicated job is assigned to that security component. For instance, the S1 firewall is dedicated to protect the E-UTRAN to EPC border. Security is deployed in a fragmented manner which eventually presents a complex and uncoordinated picture of the overall security and health of the LTE network. These security mechanisms take autonomous decisions and may apply redundant or contracting security features.

4) Lack of interoperability: Most of the LTE security systems are vendor proprietary and designed to service a specific function. As a result, such systems are closed in nature and it is difficult to obtain a "mixed and matched" use of different security solutions [8].

5) Over-provisioned security resources: Toady's LTE security mechanisms are always designed to handle busy hour traffic. They prevent the service disruptions by overpopulating the resources for security mechanisms. Therefore, most of the security resources are underutilized for long periods of time.

6) No protection against backhaul devices compromised and impersonated attacks: LTE networks uses small cell based stations such as mobile femto cells which are deployed in customer premises. These small base stations are not physically secured in the same way as a conventional base station. Most of these microcell base stations are not controlled by the operator and they are highly vulnerable to unauthorized tampering [14].

These limitations not only hinder the scalability, flexibility and adaptability, but also increase the implementation and operational cost of the legacy LTE security mechanisms. Therefore, future mobile networks demand advanced, intelligent and collaborative security systems to address the above limitations.

IV. SDN BASED SECURITY ARCHITECTURE FOR LTE

A new security model needs to be designed and deployed for the current and future mobile networks that is collaborative, integrated and agile enough to protect the network from emerging threats. Real-time security analysis and network intelligence is needed to mitigate the on-going threats and to ensure the quality of the services in security point of view.

By leveraging latest SDN and NFV technologies, new security functionalities and capabilites can be introduced to the current all-IP based network. We can build an effective security architecture on the top of these technologies. SDN and NFV concepts allow the separation of the control and data planes, enabling the programmability and centralized control of the network. Figure 4 illustrates the new security architecture which uses SDN and NFV concepts to enhance the security in LTE networks.

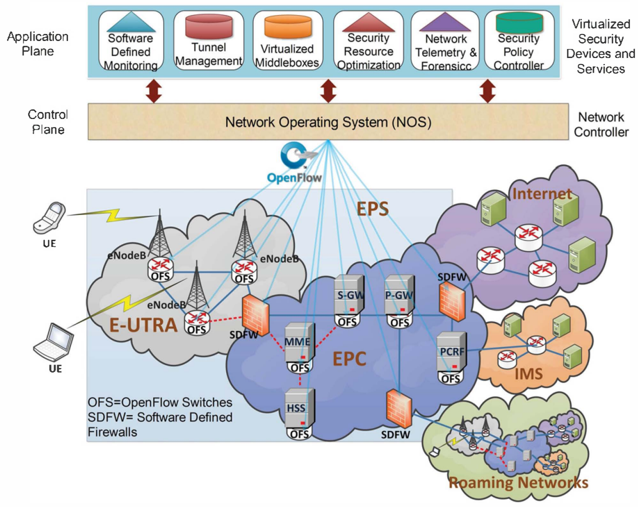

Fig. 4: The SDN based Security Architecture for LTE

SDN/NFV based security architecture is proposed following key modifications to existing LTE architecture. 1) The backhaul and access network switches and routers are replaced with SDN switches; 2) Security controlling functions are implemented at the application plane as software applications; 3) Security middleboxes are softwarificated and virtualized; 4) Logically centralized controller is used to control security mechanisms in the network;

With the help of SDN and NFV features, traditional security mechanisms can be virtualized so that they can run as software applications. Here, we propose several virtualized security apps (applications); namely, SDM (Software Defined Monitoring) app, GTP TM (Tunnel Management) app, SRO (Security Resource Optimization) app , NTF (Network Telemetry and Forensic) app, and SPC (Security Policy Control) app. However, it is possible to implement as many apps as required.

A. Expected Benefits of SDN based Security Architecture

The SDN based security architecture has a rich set of security benefits which can be used to solve the limitations in legacy LTE networks. These expected benefits are as follows;

1) Simplified and Automated Security Management: One of the main advantages of SDN is that it simplifies security management. Moreover, programmability allows fast and easy implementation and deployment of the new security mechanisms at both hardware and software levels [15]. Automated security management reduces Operational Expenditure (OPEX) by minimizing the human interactions and misconfiguration events [16].

2) Dynamic Attack Mitigation: Reaction to vulnerabilities and attacks is also improved by giving the ability to quickly assess the network from a centralized viewpoint. Furthermore, it is possible to apply dynamic changes and automate mitigation actions rapidly [15]. SDN based systems also allow improving the resiliency and fault tolerance of the network by using well known techniques such as automated fail-overs [16].

3) Efficient Segmentation: SDN supports efficient segmentation which ensures that critical assets (e.g. Home Subscriber Server HSS DB) are accessible during a security breach or network attack [17]. For instance, access to core elements should be secured during security breaches performed by malware, DoS and DDoS attacks. Moreover, holistic view and centralized controlling help to build isolated tiers, zones or network segments in real-time by dynamically evaluating the network status and service requirement such as application criticality, classification, network trust and risk levels [15].

4) Network Telemetry: SDN improves the network intelligence by enabling network-wide visibility of one's network. With the help of OpenFlow network information reports and the centralized controlling, it is possible to implement a centralized network telemetry system which provides information about the origin, destination, nature and other attributes of the traffic from various network components [15] [18]. Such an intelligent telemetry system will enable making informed security decisions to mitigate ongoing and future security threats.

5) Resource optimization: SDN and NFV makes possible the sharing, aggregation and management of available security resources to implement security mechanisms across mutli-access and multi-operator networks. Moreover, the security resources are available to scale-up in on-demand basis via mobile clouds [10] [16]. Furthermore, centralized policy controlling eliminates overlapping security polices and redundant security mechanisms. It will optimize the resources utilization for the security.

6) Abstraction: SDN and NFV offer the virtualized abstraction by hiding the complexity of hardware devices from the control plane and SDN applications [10]. In this way, it is possible to implement common security mechanisms that can be deployed repeatedly without concern for underlying physical infrastructure or different access technologies of the mobile network [8].

7) Centralized intelligence and control orchestration: With a centralized control plane and telemetry information system, SDN application can correlate required information to intelligently push network and security updates. Network governing policies can be developed and pushed in real time to meet certain capacity or performance requirements such as bandwidth and establish new tunnels or insert new flows. A controller can also manage the inventory of network nodes and with the programmable northbound interfaces, orchestration code can be executed to perform various regular functions in a centralized manner [15].

8) DDoS Mitigation: DDoS is the top security threat to mobile networks that consumes network bandwidth and resources and significantly downgrades the quality of mobile services. However, it is always challenging to protect from such attack. In LTE networks, EPC is the ideal target for DDoS attacks while the attack itself can be sourced in a distributed fashion from various points in the network [1] [4].

Traditional tools such as ACLs, provisioning additional capacity, QoS or dedicated DDoS point appliances can be used as mitigation techniques but none of these tools offers network wide protection in a collaborative and integrated manner with uniformed impact across the network. New attack techniques such as the use of Botnets, make it complicated to identify the malcicious traffic out of the legitimate [1].

By using the OpenFlow protocol [19], the SDN controller can monitor, detect and protect the network from DDoS attacks. The controller can efficiently identify DDoS attacks with real-time traffic monitoring, filtering and correlation with the network telemety data [15] [18].

B. Current Limitation of SDN based Security Architecture

Despite all these expected advantages, SDN based security architecture is also suffering form several limitations. Centralizing the network control and separating the control and data planes are very important for future networks. However, these characteristics also increase the network attack surface [20]. Starting from the application plane, applications can pose serious security threats to SDN-based architecture since applications comprise most of the network functionality through the software-based control plane [16], [20]. In SDN, authentication and authorization of applications is very important, but there are no compelling authentication and authorization mechanisms for user and third-party applications. Moreover, there are no mechanisms to establish trust relationship between the controller and remote SDN applications [16], [21].

Since the control plane is centralized, its visible nature makes it prone to security threats. The centralized nature also makes it a favorite choice for DoS attacks. In SDN, most of the flow forwarding decisions are taken in the control plane; hence, the scalability of the control plane can be targeted by sending a huge number of flow-setup requests [8]. The control plane can be saturated by unnecessary flow request to exhaust its resources making it a bottleneck for the whole network. Similarly, the control and data plane separation can be exploited by attackers due to the weak nature of the security of the control channel between the data and the control planes.

Enabling programmability requires strict isolation between different applications' traffic and scrutiny of applications before deployment to avoid conflicting modules that create security vulnerabilities. Conflicting software modules can create security problems, such as deploying contradictory flow rules and exposing sensitive network information or APIs for malicious activities [22].

Therefore, it is important to address these limitations when implementing SDN/NFV based security systems for LTE networks.

V. Numerical Results

The performance of SDN based security architecture (SDMN) is compared with the existing LTE architectures by using MATLab simulation environment. Our simulation model contains a backhaul network which has 100 backhaul devices. The model network is generated by using stochastic Kronecker graphs [23]. We assume that every backhaul device has equivalent amount of resources and the bandwidth of the network is set to 100 Mbps.

Here, we compare the performance of tunnel management mechanism of SDMN architecture. SDMN architecture uses the real-time and historical flow information to dynamically the estimate tunnel duration. We use the algorithm presented in [24] to estimate the next tunnel duration. On the other hand, LTE architecture defines static tunnel durations while deploying the security systems [1] [25].

The simulation model establishes IPsec tunnels between backhaul devices according to the tunnel management mechanism of each architecture. We simulate the session arrival process as a Poisson process ($\lambda_a = 1$ per minute) and session duration as an exponential distribution. We change the mean session duration (λ_d) and measure the performance.

Figure 5 illustrates the number of tunnel establishment instances per session against the average session duration (λ_d). We run each experiment for 1000 times and average values are presented. Here, we consider five LTE cases where tunnel duration is predefined as 20, 40, 60, 80 and 100 minutes.

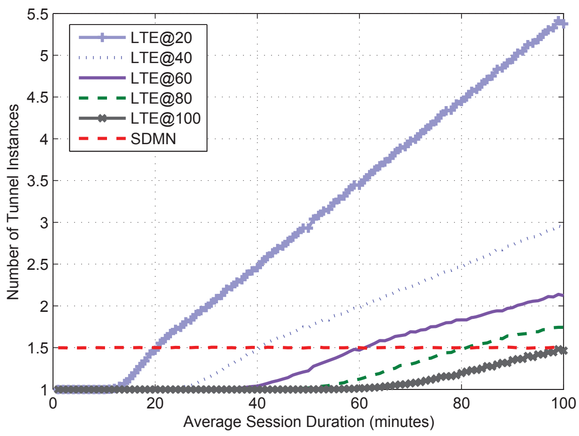

Fig. 5: Tunnel Establishment Instances per Session

The experiment results indicate that the performance of SDMN is independent of session duration. It dynamically increases the tunnel duration to match with session duration. Thus, it reduces the number of tunnel establishment instances. However, the performance of LTE architecture gets worst when λ_d is higher than the predefined tunnel duration.

Figure 6 illustrates the percentage tunnel idle time against the average session duration (λ_d). We run each experiment for 1000 times and average values are presented.

The experiment results indicate that the performance of SDMN is independent of session duration. It has the tunnel idle time of 30% under the utilized algorithm. However, performance can be further improved with better tunnel estimation algorithms. On the other hand, the performance of LTE architecture is highly depending on the session duration. In steady state, it is converging to the 50% mark. Still, SDMN has better performance than LTE.

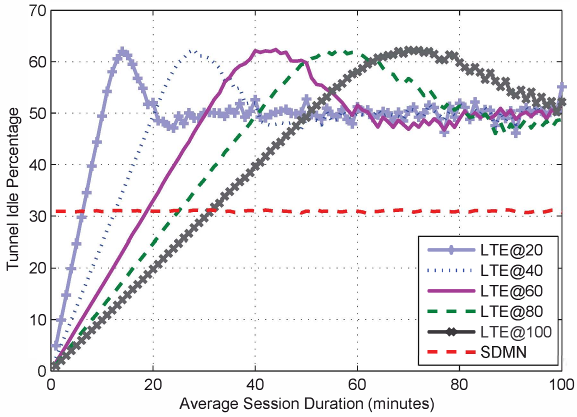

Fig. 6: Percentage Tunnel Idle Time

VI. Conclusion

We studied security mechanisms used in today's LTE networks and their limitations. Legacy LTE security mechanisms are inflexible, uncoordinated, distributed, complex and too static to address the security requirement of future mobile network services. Thus, we studied the usability of SDN and NFV concepts to solve the limitations in LTE security mechanisms.

Furthermore, we presented new security architecture for LTE networks based on SDN and NFV concepts. We also discussed the expected advantages and limitations of SDN based security architecture. Moreover, we analyzed the performance of SDN based security architecture with the existing LTE architecture in a simulation environment. SDN based security architecture uses the real-time and historical flow information to dynamically estimate the tunnel duration. SDMN architecture reduces the percentage of time the tunnel is idle and the number of tunnel establishments per session.

In the future, we will focus on the development of new security services based on SDN based security architecture and show how we solve the existing limitations in operating settings.

Acknowledgment

This work has been performed in the framework of the CELTIC CP2012 project SIGMONA.

References

[1] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 283–302, 2014.

[2] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *Security & Privacy, IEEE*, vol. 11, no. 2, pp. 55–62, 2013.

[3] C. Kolias, S. Ahlawat, C. Ashton *et al.*, "OpenFlow-Enabled Mobile and Wireless Networks," *White Paper*, Open Network Foundation, September 2013.

[4] M. Liyanage, M. Ylianttila, and A. Gurtov, "A Case Study on Security Issues in LTE Backhaul and Core Networks," *Case Studies in Secure Computing: Achievements and Trends*, p. 167, 2014.

[5] (2015) LTE World. [Online]. Available: http://lteworld.org/

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

[7] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, T. Turletti *et al.*, "A survey of software-defined networking: Past, present, and future of programmable networks," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1617–1634, 2014.

[8] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security enhancement in wireless mobile networks," *Computer Networks*, vol. 66, pp. 94–101, 2014.

[9] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective," *IEEE Security and Privacy Magazine*, 2015.

[10] 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.

[11] J. Costa-Requena, J. L. Santos, V. F. Guasch, K. Ahokas, G. Premsankar, S. Luukkainen, I. Ahmed, M. Liyanage, M. Ylianttila, O. L. Prez, M. U. Itzazelaia, and E. M. de Oca, "SDN and NFV Integration in Generalized Mobile Network Architecture," in *European Conference on Networks and Communications (EUCNC)*. IEEE, 2015, pp. 1–5.

[12] (2014) 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401. [Online]. Available: http://www.3gpp.org/DynaReport/33401.htm

[13] M. Liyanage, M. Ylianttila, and A. Gurtov, "IP-Based Virtual Private Network Implementations in Future Cellular Networks," *Handbook of Research on Progressive Trends in Wireless Communications and Networking*, p. 44, 2014.

[14] S. Namal, M. Liyanage, and A. Gurtov, "Realization of Mobile Femtocells: Operational and Protocol Requirements," *Wireless personal communications*, vol. 71, no. 1, pp. 339–364, 2013.

[15] M. McBride, M. Cohn, S. Deshpande, *et al.*, "SDN Security Considerations in the Data Center," *White Paper*, Open Network Foundation, October 2013.

[16] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A Survey," in *IEEE SDN for Future Networks and Services (SDN4FNS)*. IEEE, 2013, pp. 1–7.

[17] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, "Flowvisor: A network virtualization layer," *OpenFlow Switch Consortium, Tech. Rep*, 2009.

[18] K. Pentikousis, Y. Wang, and W. Hu, "Mobileflow: Toward software-defined mobile networks," *Communications Magazine, IEEE*, vol. 51, no. 7, 2013.

[19] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[20] M. Liyanage, I. Ahmad, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. de Oca, A. Valtierra, and C. Jimenez, "Security for Future Software Defined Mobile Networks," in *9th International Conference on Next Generation Mobile Applications Services and Technologies (NGMAST),*. IEEE, 2015, pp. 1–9.

[21] 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.

[22] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1–1, 2015.

[23] J. Leskovec, D. Chakrabarti, J. Kleinberg, C. Faloutsos, and Z. Ghahramani, "Kronecker graphs: An approach to modeling networks," *The Journal of Machine Learning Research*, vol. 11, pp. 985–1042, 2010.

[24] V. Jacobson, "Congestion avoidance and control," in *ACM SIGCOMM Computer Communication Review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[25] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*. IEEE, 2012, pp. 1–5.