# Lightweight Virtualization based security framework for Network Edge

Abderrahmane Boudi[1,2], Ivan Farris[1], Miloud Bagaa[1] and Tarik Taleb[1,3]
[1] Dep. of Communications and Networking, School of Electrical Engineering, Aalto University, Espoo, Finland
[2]Laboratoire de la Communication dans les Systèmes Informatiques, École nationale Supérieure d'Informatique, Algiers, Algeria
[3] Oulu University, Oulu, Finland
Emails:{firstname.lastname}@aalto.fi

***Abstract*—The interest towards cybersecurity is fast growing over the last years. Accounting for the tremendous increase of security threats, the need for new defense strategies is acquiring an even growing importance. The widespread adoption of Internet of Things (IoT) devices, ranging from smart industrial appliances to simple domestic sensors, will increase the complexity of managing security requirements in a comprehensive way. The provisioning of on-demand security services according to the SECurity-as-a-Service model is gaining notable attention. Nevertheless, the hosting of security functions in remote data-centers will inevitably introduce long routing detours, thus high latency and traffic overhead. To cope with this, edge computing will prove to be useful to process data locally. But the reduced capabilities of edge nodes can negatively impact the overall performance of SECaaS solutions. This paper focuses on the provisioning of virtualized security functions via lightweight virtualization (i.e., container) technologies running in a resource-constrained environment. Our analysis focuses primarily on the feasibility and the performance evaluation of such scenario.**

## I. Introduction

Accounting for the exponential increase of security threats and the tremendous effects and damages which can be carried out in our hyper-connected world, cybersecurity is acquiring an ever-growing importance. The expected avalanche of heterogeneous Internet of Things (IoT) devices which will populate our industrial factories and houses will increase the potential attack surfaces. Furthermore, the heterogeneity of IoT devices can drastically increase the complexity to provide the desired protection [1]. Novel security strategies are gaining notable impetus to meet security requirements in both industrial and domestic environments.

Over the last years, the provisioning of on-demand security services according to the Security-as-a-Service (SECaaS) model [2] gathered a great amount of attention from both industrial and research communities. SECaaS consists in providing cloud-hosted security and privacy solutions to organizations and users [3]. Deploying security instances in the cloud introduces several drawbacks, such as delay increase and privacy concerns. To face these issues, Edge Computing [4] is a promising solution. Indeed, hosing security services at the network edge, will relieve the data from doing long routing detours to the cloud which will greatly reduce latency.

In this paper, we propose an analysis study on the performance of the provisioning of security functions using lightweight virtualization platforms running in resource-constrained edge nodes, such as IoT gateways. Given the fact that the security mechanisms can have a big influence on the overall Quality of Service [5], maximizing the performance of security mechanisms is a fundamental for enabling the functionality of variant services. Therefore, a performance analysis of container-based security services in resource-constrained devices is of utmost importance. In our analysis, we will be assessing resource consumption of virtualized security functions running in resource-constrained edge nodes. This study can also provide useful guidelines for the orchestration of security functions at the edge.

The remaining of this paper is organized as follows. In Section II, we present a background on cloud-based security functions and edge computing features. Two promising case studies are discussed in Section III. Section IV reports the performance evaluation of container-based security functions. While we list some promising open research challenges in Section V, concluding remarks are drawn in Section VI.

## II. Background

### A. Cloud-based Security Functions

Cloud service provisioning has become a great target for many applications since it provides storage and computation capabilities with relatively low-cost. Nowadays, there are more and more of security vendors that are providing their security solutions as cloud services using different virtual network functions (VNFs). This approach, called SECurity-as-a-Service (SECaaS) [6], consists in the provisioning of security solutions hosted in remote data-centers. SECaaS offers a great flexibility for enabling different security solutions while reducing the cost.

In this landscape, specific research efforts aim at developing schemes to appropriately model virtualized security services and to provide guidelines for efficiently integrating security services within standard cloud delivery solutions [7]. In [8], an approach towards the adoption of security policies management with dynamic network virtualization is presented. In particular, three different policy abstraction layers are defined and an iterative refinement process is proposed to determine

the resources necessary to enforce specific security features through the provisioning of selected virtualized security functions. To meet the desired objectives and avoid deviation from the expected policies' goals, an accurate estimation of the requirements for virtualized functions becomes crucial, as well as the management of the overall lifecycle.

Lately, network function virtualization (NFV) has gathered a significant attention from both industry and academic communities. By replacing dedicated network hardware with software instances, NFV will facilitate the deployment of new services with increased agility and faster time-to-value. As a matter of fact, NFV will be fundamental in securing IoT devices [9], [10]. Authors in [11] have suggested a framework for characterizing performance of virtual network functions. The proposed framework determines optimal resources configuration for a given workload and useful insights to scale up or down relevant instances. Among the analyzed functions, the analysis of IDS systems executed in virtual machines have been tested for cloud environments. In fact, this study has a great impact on defining different resource characteristics of virtualized security function for enabling security services that fulfill the policy requirements with low cost [12].

In contrast to the aforementioned solutions, in this paper, we evaluate the feasibility for container-based technologies running security functions to provide decent performance when run in resource-constrained edge nodes. Indeed, to efficiently extend the hosting of security features towards the network edge, the characterization of virtualized security services is of utmost importance.

### B. Lightweight Virtualization for Edge Computing

Over the last years, Edge computing has received an increased attention, accounting for the opportunity to extend the successful cloud model towards the edge of the network. In this way, great advantages can be introduced in terms of reduced latency, traffic reduction, and context-awareness. Not by chance, edge computing is considered as a pillar of next-generation 5G networks able to support demanding verticals such as massive IoT, virtual reality, and Tactile Internet [13], [14]. However, new challenges are introduced in the deployment of service instances at the network edge. Especially when considering resource-constrained edge nodes, lightweight virtualization technologies are strictly required. In this vein, container-based virtualization is able to offer several benefits with respect to classic hypervisor-based virtual machine environments: *i*) Fast creation and initialization of virtualized instances; *ii*) High density of applications, thanks to the small container images; *iii*) Reduced overhead, while enabling isolation between different instances running in the same host [13], [15].

In [16], the authors have evaluated Docker containers in terms of deployment and termination, resource and services management, fault tolerance, and caching. Docker containers show high agility with small and lightweight images, fast service deployment and tear down, low storage footprint and many more advantages which make it a promising platform to be used in Edge Computing. With the ability to run different applications, container technologies can extensively be used in capillary networks, where Docker containers are deployed to execute various functionalities at the capillary gateway. In [17], Docker is used to package and deploy different features for the Cloud of Things that will be executed at the gateway. However, an analysis of container technologies of security services in resource-constrained edge nodes is still missing.

## III. Case studies

This section introduces two promising use cases whereby the provisioning of security functions at the network edge is needed. These use cases show that in both industrial and domestic environments, the lightweight virtualization is fundamental.

### A. Factory 4.0

The fourth industrial revolution is next-to-come and will be boosted by a progressive digitalization of industrial production processes [18]. In this fervent ecosystem, sensor and actuator devices will play a fundamental role to bridge the physical and virtual domains by providing the necessary capabilities to monitor the industrial environment and to promptly react. Furthermore, automated robots are expected to provide real-time information about operational behavior, for enabling both remote quality of product and maintenance analysis. The increased connectivity of industrial systems will thus be the key factor for next-generation Factory 4.0.

The increasing openness, in the next-generation Factory 4.0, will inevitably lead to huge security concerns. Indeed, given the number and the disparity of industrial equipments, the attack surfaces will drastically increase, which will lead to a myriad of security vulnerabilities exploitable by malicious attackers [19], [20]. In industrial environments, the damage suffered from security breaches is amplified. It can lead to process disruption, product adulteration and even compromising the physical integrity of the workers operating in strict synergy with robots. Which will result in bad brand reputation and huge revenue losses. All these security concerns will greatly undermine the overall digitalization of industries.

Another core aspect of industrial environments is the confidentiality of information that are within the companies boundaries. Such information can be of utmost importance for the competitiveness of the company. For instance, information gathered during production processes can be targeted by potential competitors. For this reason, companies can be reluctant to process their data in remote cloud datacenters. In such complex scenarios, the ability to execute virtualized security functions at edge nodes is very important. For instance, enhanced gateways can forward data to/from industrial sensors while analyzing the relevant traffic flows to identify potential security vectors. When serious attacks are detected, it can anonymize the data and send it to remote cloud to be scrutinized. For this idea to become viable, a thorough performance analysis of virtualized security function

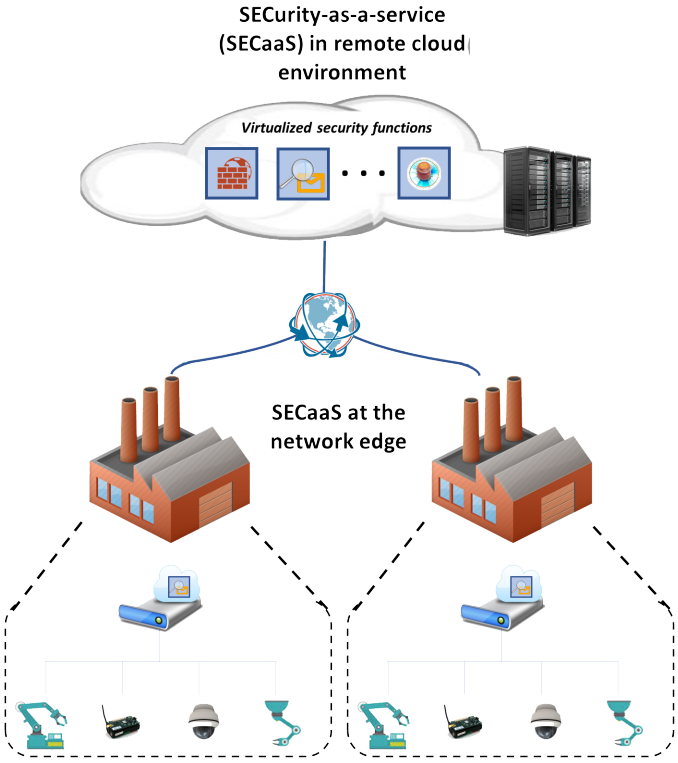



Fig. 1. Security-as-a-Service in industrial edge scenarios.

running in resource constrained edge nodes should be carried. In this way, the interplay of virtualized security functions between cloud and edge can be further improved and novel offloading strategies can be developed, specifically tailored to the constraints of virtualized edge nodes.

### B. Smart Home

A myriads of IoT devices will transform our houses in smart pervasive environments, ranging from smart kitchen appliances to tiny light sensors. A key factor is their enhanced interworking to exchange and cooperate with neighboring devices, as well as cloud-hosted applications back-end. The dark side of this connectivity relates to the new potential security vectors which attackers can leverage to lead their malicious activities. Indeed, in October 2016, exploiting some firmware security flaws, cybercriminals launched a Distributed Denial of Service (DDoS) attack[1], using a large number of IoT devices, against an Internet service provider Dyn, thus disrupting access to several popular websites.

In order to protect end users, telecommunications service providers (TSP) can promote SECaaS by providing gateways with enhanced virtualization capabilities. The gateway, or the local edge cloud, can then be used to host a wide range of services as securing and verifying inbound and outbound traffic of domestic environment. The local edge cloud can also be used to process sensitive information, thus preserving confidentiality and subscribers' right of privacy. It can also be used to deploy Intrusion Detection Systems (IDS) to verify malicious traffic between local IoT devices and potential remote cybercriminals. If security breaches are detected, the end-users will be informed and appropriate countermeasures can be carried out. For instance, in the event that the IoT devices are participating in a DDoS attack, the TSP can filter the malicious traffic as close to the source as possible.

[1]http://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/

## IV. Performance evaluation

In this section, we study the performance of virtualized security functions in resource-constrained edge nodes in a real testbed setup. In fact, in this section, we aim at demonstrating the feasibility of container-based virtualization of security functions, by comparing the execution of security functions natively against their respective containerized counterparts. In our analysis, we focus on: *i*) number of processed packets; *ii*) network utilization; *iii*) number of alerts; *iv*) RAM utilization; *v*) CPU load; and *vi*) number of dropped packets.

The testbed setup consists of a Raspberry Pi3 Model-B. It is a card-sized minicomputer with 1.2 GHZ quad-core CPU, 1GB of RAM, and a Fast-Ethernet network interface. These relatively light specifications are a good example of the capacity that should be expected in edge nodes. In our evaluation, we use the IDS Suricata as virtualized security function. Similar to Snort, Suricata uses a configuration file containing rules to detect the attacks. In this study, we use the

emerging threat rules set[2]. Malicious traffic is generated from a pcap file[3]. Docker containers are used as the virtualization technology. The pcap files are played using different speeds. This allows to vary the traffic rate from $10Mbps$ up to $90Mbps$. In order to reduce noise, each setup is run 10 times with enough time between simulations to let the Raspberry Pi cool off. In what follows, we refer to Suricata running on bare metal as SoBM while SoDC refers to Suricata that runs inside Docker container.

### A. Processed packets

Fig.2(a) shows the relationship between the number of processed packets and the traffic rate. Obviously, the rate and the type of traffic have a huge impact on the number of processed packets. As the rate increases, SoBM processes slightly more packets than SoDC. But as will be shown later with the number of drops, this difference is not significant.

### B. Network utilization

In Fig.2(b), the utilization of the network interface is shown. It is clear that SoBM slightly receives more packets that SoDC. But the difference between the two is well within the error margin.

### C. Alerts

In Fig.2(c), the number of alerts is similar between SoBM and SoDC. As it can be expected, when the sending rate increases, Suricata will analyze more packets and thus the number of detected alerts also increases. Also, by increasing the rate, the number of alerts varies due to the fact that the number of drops and the number of processed packets change from one simulation to another.

### D. RAM utilization

Fig.2(d) shows that SoBM and SoDC have the same memory usage. Only the traffic type affects the memory. When the packets are small, the RAM utilization reaches 50%. Meanwhile, for large packets runs, the RAM usage is between 26% and 28%.

### E. CPU utilization

In Fig.2(e), the evaluation of CPU load is performed. The difference between SoBM and SoDC is between 2% and 6%. Investigating this situation shows that SoDC is taking more time running on kernel space, while SoBM is taking more time on user space.

### F. Number of drops

Fig.2(f) shows the percentage of drops occurred during the performance evaluation. The dropping began at $50Mbps$, and the percentage of dropped packets increases with the bandwidth. Even with a rate over 90%, the dropping rate does not exceed 2%. The reason beneath SoDC being less prone to drop packets is two folds. As depicted in Fig.2(e), SoDC shows less CPU usage on average, therefore, it is less prone than SoBM to drop packets due, in turn, to bursts. Also, given the fact that SoBM receives slightly more packets than SoDC (Fig.2(b), it becomes clear then that SoBM may have to drop more packets. Fig.3 shows the ratio between the number of successfully processed packets by SoBM and SoDC (Eq.1). Fig.3 shows that SoBM slightly outperforms SoDC in regards to the absolute number of processed packets.

$$ratio = \frac{ptks_{bm} - drop_{bm}}{ptks_{dc} - drop_{dc}} \quad (1)$$

where $ptks_{bm}$ and $ptks_{oc}$ denote the number of packets received by SoBM and SoDC, respectively. $drop_{bm}$ and $drop_{dc}$ are the number of drops performed by SoBM and SoDC, respectively.

### G. Small packets simulations

When the traffic is mainly composed by small packets, the impact on the CPU is huge. During our experiment setup, when the rate is $50Mbps$, the CPU load reaches more than 80%. Going beyond that would cause crashes, therefore the results were not reliable. There is also a high variability in the number of detected attacks. This is due to the high number of drops.

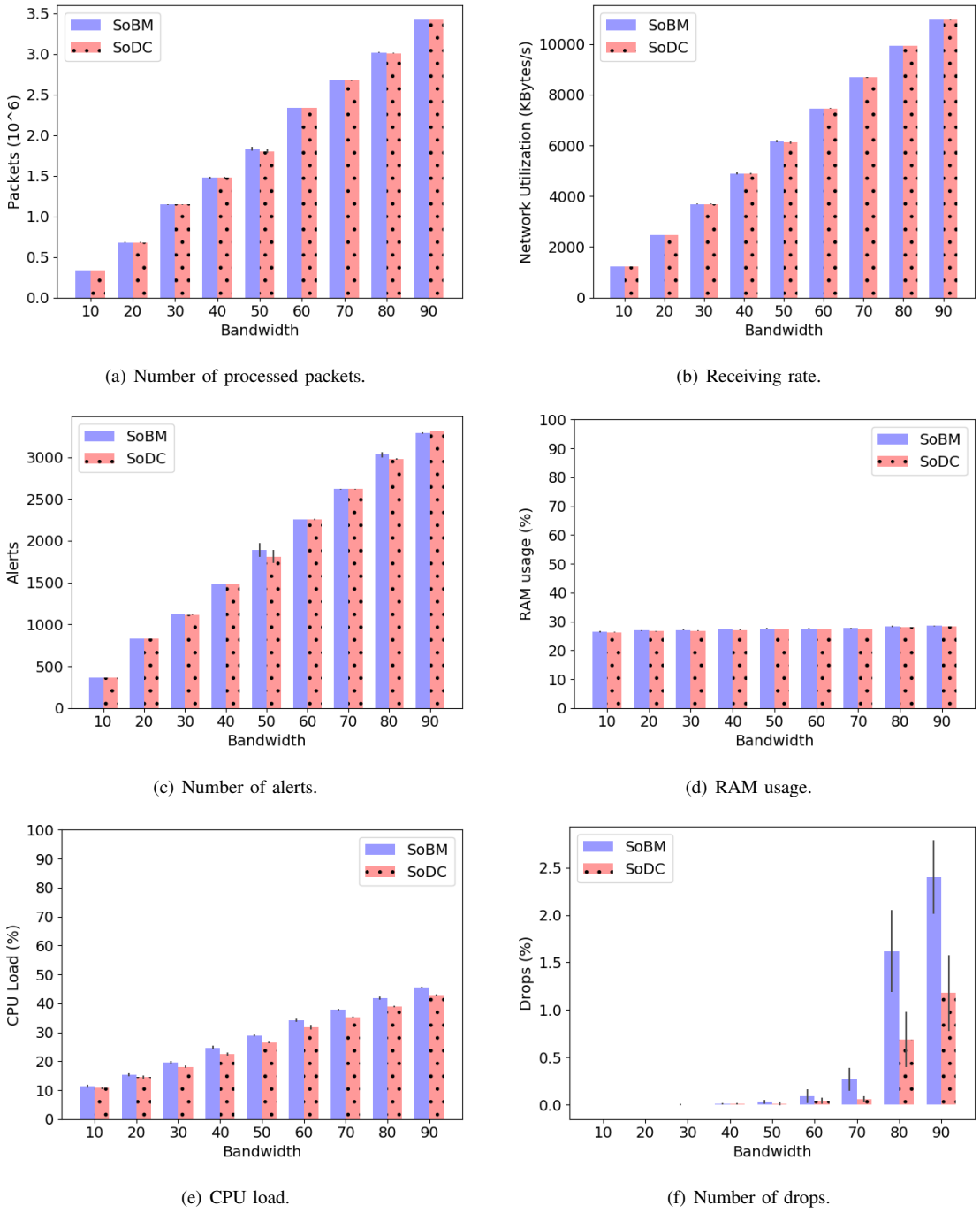
## V. Open research challenges

The joint use of lightweight virtualization and edge computing represents a promising environment to provide SECaaS, considering the multiple envisioned benefits reported in the previous sections. Furthermore, this study opens up several research challenges to be further investigated for an efficient provisioning of security features at the network edge.

- *Security services orchestration*: Edge computing offers the possibility to spread and coordinate multiple services among distributed edge nodes for an efficient workload balancing. Also, multiple edge nodes can collaborate to provide enhanced security mechanisms. For instance, in an intrusion detection scenario, the neighboring nodes can share contextual information to dynamically refine the detection process. Unfortunately, existing orchestrations mechanisms have been designed mainly for data centers and further research efforts are needed to cope with the resource constraints and the geographic distribution of edge nodes.
- *Security of container virtualization*: Container virtualization heavily relies on underlying kernel features to provide the necessary isolation between containers [21], [22]. Therefore, specific efforts should address the relevant security concerns. Furthermore, a complex ecosystem has been developed around the Docker virtualization technologies, including container image repositories and orchestration platforms. These complementary tools introduce new security challenges which go beyond the classic host domain, involving for instance the integrity of container images during transfer over insecure Internet connections, as well as the interactions with potentially untrusted management modules.

[2]http://rules.emergingthreats.net/open/suricata/

[3]http://www.netresec.com/?page=PcapFiles




(a) Number of processed packets.

(b) Receiving rate.

(c) Number of alerts.

(d) RAM usage.

(e) CPU load.

(f) Number of drops.

Fig. 2. SoBM vs SoDC comparaison with respect to (a) Processed packets, (b) Rate, (c) Alerts, (d) RAM, (e) CPU and (f) Drops.

## VI. Conclusion

With the increase of malicious Information and Communications Technology ICT attacks, providing on-demand defense mechanisms using the cloud is gaining high momentum. Indeed, both research and industrial communities are highly interested in the SECaaS paradigm. Processing data in remote cloud-servers will introduce long routing detours, while deploying virtualized security solutions in the edge environment will considerably reduce latency and traffic overhead. However, the resource scarcity and constraints of edge nodes can negatively impact the overall Quality of Service (QoS). In this paper, we provided a performance analysis of a virtualized security function running in constrained edge nodes. Using a real testbed environment, the IDS Suricata was running inside a Docker container detecting attacks for a broad range of possible workloads. Future works will explore

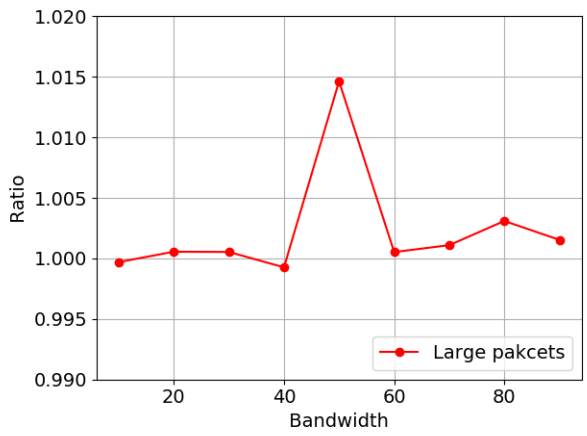



Fig. 3. Ratio of successfully handled packets by SoBM over SoDC.

the challenges presented in Section V which will boost the adoption of SECaaS at the network edge. Furthermore, we will extend the characterization of containerized security functions to efficiently orchestrate them over distributed edge nodes.

## Acknowledgment

This work was partially supported by the ANASTACIA project, that has received funding from the European Unions Horizon 2020 Research and Innovation Programme under Grant Agreement N 731558 and from the Swiss State Secretariat for Education, Research and Innovation. This work was supported in part by the Academy of Finland 6Genesis Flagship (grant no. 318927).

## References

[1] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015, pp. 21–28.

[2] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, pp. 60–75, 2014.

[3] I. Farris, J. Bernabe, N. Toumi, D. Garcia, T. Taleb, A. Skarmet, and B. Sahlin, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, Sept 2017, pp. 187–192.

[4] I. Farris, T. Taleb, H. Flinck, and A. Iera, "Providing ultra-short latency to user-centric 5G applications at the mobile network edge," *Transactions on Emerging Telecomm. Technologies (ETT)*, Mar. 2017, DOI 10.1002/ett.3169.

[5] T. Taleb and Y. Hadjadj-Aoul, "QoS2: a framework for integrating quality of security with quality of service," *Security and communication networks*, vol. 5, no. 12, pp. 1462–1470, 2012.

[6] M. Hussain and H. Abdulsalam, "Secaas: Security as a service for cloud-based applications," in *Proceedings of the Second Kuwait Conference on e-Services and e-Systems*, ser. KCESS '11. New York, NY, USA: ACM, 2011, pp. 8:1–8:4. [Online]. Available: http://doi.acm.org/10.1145/2107556.2107564

[7] A. Furfaro, A. Garro, and A. Tundis, "Towards security as a service (secaas): On the modeling of security services for cloud computing," in *Security Technology (ICCST), 2014 International Carnahan Conference on*. IEEE, 2014, pp. 1–6.

[8] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization," in *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*. IEEE, 2015, pp. 1–5.

[9] I. Farris, T. Taleb, Y. Khettab, and Y. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE COMST*, (to appear).

[10] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for internet of things realization," *IEEE COMST*, (to appear).

[11] L. Cao, P. Sharma, S. Fahmy, and V. Saxena, "NFV-vital: A framework for characterizing the performance of virtual network functions," in *Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on*. IEEE, 2015, pp. 93–99.

[12] R. Bonafiglia, I. Cerrato, F. Ciaccia, M. Nemirovsky, and F. Risso, "Assessing the performance of virtualization technologies for NFV: A preliminary benchmarking," in *2015 Fourth European Workshop on Software Defined Networks*, Sept 2015, pp. 67–72.

[13] T. Taleb, S. Dutta, A. Ksentini, M. Iqbal, and H. Flinck, "Mobile edge computing potential in making cities smarter," *IEEE Communications Magazine*, 2017.

[14] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing & softwarization: A survey on principles, enabling technologies & solutions," *IEEE Communications Surveys Tutorials*, 2018.

[15] R. Morabito, J. Kjällman, and M. Komu, "Hypervisors vs. lightweight virtualization: a performance comparison," in *IEEE International Conference on Cloud Engineering (IC2E)*. IEEE, 2015.

[16] B. I. Ismail, E. M. Goortani, M. B. Ab Karim, W. M. Tat, S. Setapa, J. Y. Luke, and O. H. Hoe, "Evaluation of docker as edge computing platform," in *Open Systems (ICOS), 2015 IEEE Confernece on*. IEEE, 2015, pp. 130–135.

[17] R. Petrolo, R. Morabito, V. Loscrì, and N. Mitton, "The design of the gateway for the cloud of things," *Annals of Telecommunications*, pp. 1–10, 2016.

[18] T. Taleb, I. Afolabi, and Bagaa, "Orchestrating 5G network slices to support industrial internet and to shape next-generation smart factories," *IEEE Network Magazine*, (to appear).

[19] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1091–1104, 2013.

[20] T. Taleb, B. Mada, M. Corici, A. Nakao, and H. Flinck, "PERMIT: Network slicing for personalized 5G mobile telecommunications," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 88–93, May 2017.

[21] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, May 2017.

[22] S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, "Securing VNF communication in NFVI," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, Sept 2017, pp. 187–192.