# Assessing Lightweight Virtualization for Security-as-a-Service at the Network Edge

Abderrahmane Boudi[1,2], Ivan Farris[1], Miloud Bagaa[1], Tarik Taleb[1] and Yacine Khettab[1]
[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
Emails:{firstname.lastname}@aalto.fi

***Abstract*—Accounting for the exponential increase of security threats, the development of new defense strategies for pervasive environments is acquiring an even growing importance. The expected avalanche of heterogeneous IoT devices which will populate our industrial factories and houses will increase the complexity of managing security requirements in a comprehensive way. To this aim, cloud-based security services are gaining notable impetus to provide security mechanisms according to Security-as-a-Service (SECaaS) model. However, the deployment of security applications in remote cloud data-centers can introduce several drawbacks in terms of traffic overhead and latency increase. To cope with this, edge computing can provide remarkable advantages avoiding long routing detours. On the other hand, the reduced capabilities of edge node introduce potential constraints in the overall management. This paper focuses on the provisioning of virtualized security services in resource-constrained edge nodes by leveraging lightweight virtualization technologies. Our analysis aims at shedding light on the feasibility of container-based security solutions, thus providing useful guidelines towards the orchestration of security at the edge.**

## I. Introduction

The interest towards cybersecurity is fast growing over the last years accounting for the tremendous effects and damages which can be carried out in our hyper-connected world. The potential attack surfaces are increasing at fast pace leveraging the widespread adoption of Internet of Things (IoT) devices. Furthermore, the heterogeneity of IoT devices, ranging from smart industrial appliances to simple domestic sensors, can even increase the complexity to provide the desired protection [1]. Novel security strategies are required to meet security policies in both industrial and domestic environments.

Accounting for the success of cloud solutions, the provisioning of on-demand security services according to the Security-as-a-Service model [2] is gaining notable attention from both industrial and research communities. In this way, organizations and users can be assisted by cloud-hosted components providing security and privacy protection [3]. On the other hand, the deployment of security instances in remote data centers present several drawbacks, such as long routing detours and delay increase. To face these issues, Edge Computing [4] offers the opportunity to efficiently host services at the network edge, thus introducing remarkable benefits in terms of latency and traffic reduction.



In this paper, we aim at investigating the provisioning of security services in resource-constrained edge nodes, such as network access points and IoT gateways. In this vein, we will evaluate Docker containers as promising lightweight virtualization technology [5]. We strongly believe that performance analysis of security defense systems is of utmost importance, since security mechanisms can notably influence the overall Quality of Service [6]. Our analysis aims at shedding light on the feasibility of container-based security services in resource-constrained devices, assessing relevant resource consumption in a realistic testbed environment for a broad range of possible workloads.

The 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

Accounting for the remarkable benefits introduced by cloud service provisioning, an increasing number of security vendors are exploiting cloud ecosystems to provide their security solutions. This approach, referred to as SECurity-as-a-Service (SECaaS) [2], is based on the provisioning of security applications via the cloud, thus leveraging greater flexibility and economies of scale. In this vein, the Cloud Security Alliance (CSA) has defined guidelines for cloud-delivered defense solutions, to assist enterprises and end-user to widely adopt this security paradigm shift [7].

In this landscape, specific research efforts aim at developing schemes to appropriate model virtualized security services and to provide guidelines for efficiently integrating security services within standard cloud delivery solutions [8]. In [9], 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.

Accounting for the significant advantages introduced by replacing dedicated network hardware with software instances, Network Function Virtualization (NFV) is gaining high momentum to enhance the scalability and flexibility of softwarized networks [10]. In [11], a framework for characterizing performance of virtual network functions has been developed, to determine optimal resource 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. Indeed, the performance of virtualized components can have a great impact on the overall service chaining, accounting for the hardware settings and virtualization technologies overhead [12]. The objective of this paper is to consider the evaluation of container-based technologies for providing security mechanisms in resource-constrained edge nodes.

### 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 a pillar of next-generation 5G network able to support demanding verticals such as massive IoT, virtual reality, and Tactile Internet [13], [14]. Also, standardization bodies and industrial consortia are promoting its widespread adoption by creating specific study groups, thus leading to ETSI Multiple-access Edge Computing (MEC) [15] and Open Fog Consortium [16].

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] [5].

As discussed in [17], Docker containers represent a promising platform for Edge Computing. In this work, Docker has been evaluated in terms of deployment and termination, resource and service management. Different application fields for container-based virtualization have been demonstrated. Container technologies are used in a Capillary Network scenario [18], where Docker containers allow to package, deploy, and execute different functionality at the capillary gateway. In [19], lightweight virtualization technologies is used to deploy on-demand gateway features for the Cloud of Things. However, an analysis of container technologies for security services is still missing.

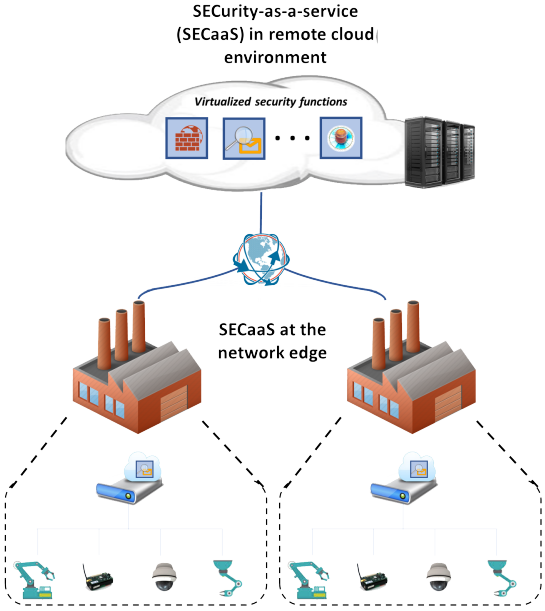



Fig. 1. Security-as-a-Service in industrial edge scenarios.

## III. Case studies

In this section, we present two promising use cases in both industrial and domestic environments which strongly push the need for provisioning security functions at the edge with advanced flexibility compared to classic dedicated hardware solutions.

### A. Factory 4.0

The fourth industrial revolution is next-to-come and will be boosted by a progressive digitalization of industrial production processes. 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 [20]. The increased connectivity of industrial systems will thus be the key factor for next-generation Factory 4.0.

The dark side of the medal of this increased openness will be represented by the new potential security vulnerabilities which can be exploited by malicious attackers [21], [22]. Indeed, security threats can cause catastrophic effects in industrial environment leading to process interruption, product adulteration and event to health risk for worker operating in strict synergy with robots. These accidents can provoke huge loss in revenues and brand reputation, thus undermining the overall digitalization of industrial revolution.

Further challenges of industrial environments deal with the confidentiality of information gathered during production processes. Data leakages can also advantage potential

competitors, and consequently companies are reluctant to have their data processed outside their boundaries. In this complex scenario, the increased abstraction capabilities of edge node can provide the appropriate environment to execute virtualized secure functions, as sketched in Fig. 1. For instance, enhanced gateway can forward data to/from industrial sensors and analyze relevant traffic flows to identify potential security vectors. Only the verified data can be admitted and security alerts are logged. Key aspects deal with the analysis of performance ensured by virtualized security functions in resource-constrained edge nodes. 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 internetworking to exchange and cooperate with neighboring devices, as well as cloud-hosted application 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, cybercriminals launched a Distributed Denial of Service (DDoS) attack[1] against an Internet service provider Dyn, thus disrupting access to several popular websites. To carry out this attack, a large number of internet-connected devices (mostly DVRs and cameras) were used as their helpers by exploiting some firmware security flaws. The heterogeneity of devices make extremely complex to guarantee the desired requirements for end-users.

To enhance defense mechanisms, security-as-a-service paradigm can be promoted by Telco operators, which can provide router/gateway with enhanced virtualization capabilities to their subscribers. A broad range of services can be deployed on-demand within the home environment, while enabling the creation of local edge cloud able to secure and verify the communications from/into domestic environment. In this way, potential sensitive information included in the traffic flows can be processed locally, thus preserving relevant confidentiality. For instance, Intrusion Detection System (IDS) can be deployed to verify malicious traffic between personal IoT devices and remote cybercriminals. When potential threats are detected, security alerts are launched to inform the end-user and to trigger the adoption of appropriate countermeasures.

## IV. Performance evaluation

In this section, we aim at comprehensively assessing the performance of virtualized security functions in resource-constrained edge nodes in a real testbed setup. Our objectives are also to demonstrate the feasibility of efficiently adopting container-based virtualization, by comparing the native execution of security functions and 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 comprises the IDS Suricata running on a Raspberry Pi3 edge node. The experimental results show the difference between Suricata running on bare metal (SoBM) and Suricata running inside a Docker container (SoDC). The rule set that was used to detect the attacks is the emerging threat rules set[2]. As was done in [23], the traffic was generated from pcap files containing attacks[3]. The rate of the traffic varies from $10Mbps$ up to $90Mbps$, it should be noted that the Raspberry Pi3 has only a Fast-Ethernet interface. Due to the lack of space, we shall only discuss the results for the simulations where the number of small and large packets were roughly the same. Finally, each simulation setup was run 10 times and the average and standard deviation are plotted for each experiment.

### 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 process slightly more packets than SoDC. But as will be shown later with the number of drops, this difference is not significant.

### B. Network utilization

Fig.2(b) depicts the performance of network utilization. From the obtained results, we can conclude that SoBM slightly outperforms SoDC. As before, running Suricata on bare metal or on a Docker container does not show a clear difference in the performance of each.

### 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%.

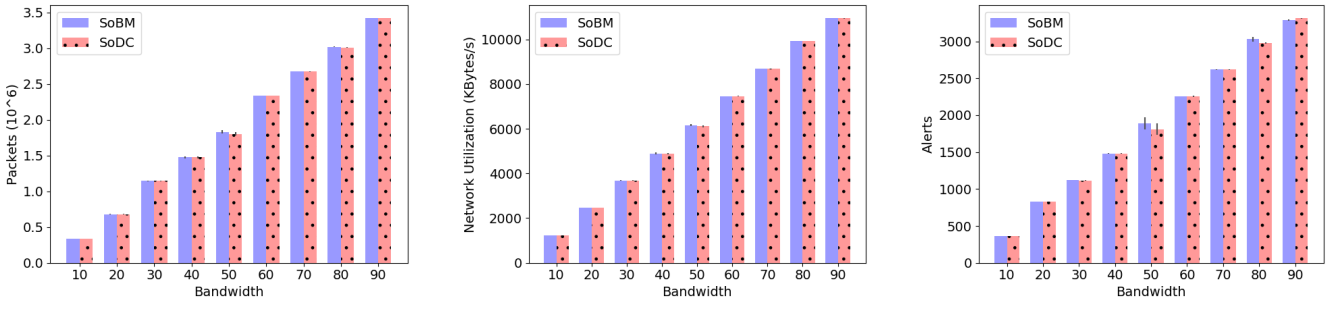
### E. CPU utilization

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.

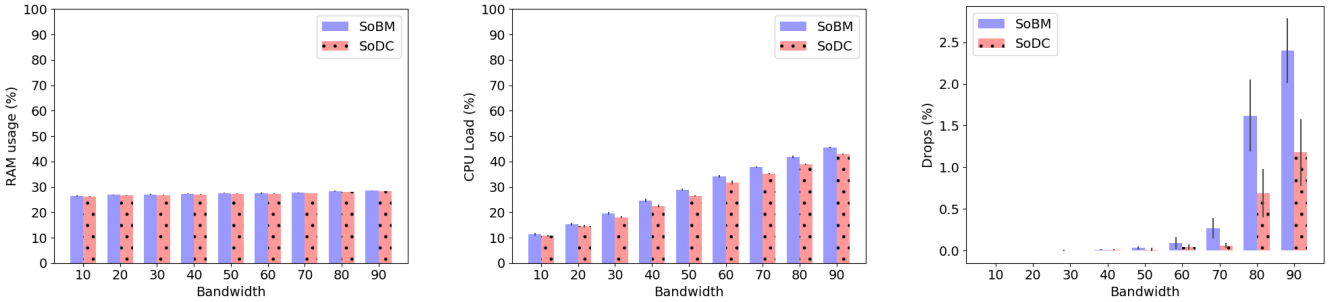
[1] http://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/

[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 results.

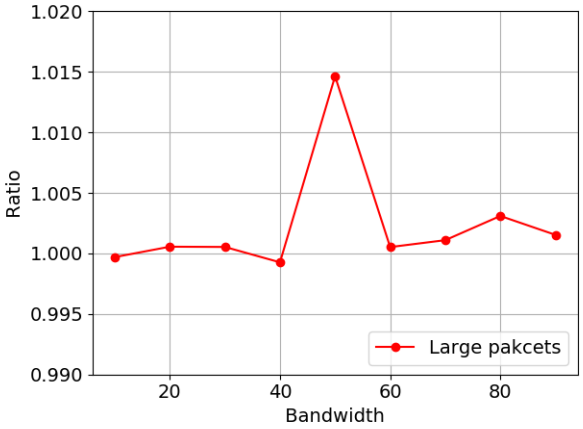



Fig. 3. Ratio of successfully treated packet by SoBM over SoDC.

### 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. The number of drops is less than 2%, even when the rate is 90%. The reason beneath SoDC showing less drops is due to two main reasons. As shown in Fig.2(e), SoDC has less impact on the CPU on average, therefore, it is less prone than SoBM to drop packets due, in turn, to bursts. The second reason is that SoBM generally receives more packets than SoDC, thus SoBM will have to drop more packets. Fig.3 shows the ratio between the number of successfully processed packets by SoBM and SoDC (Eq.1). As it can be seen in Fig.3, SoBM processes slightly more packets than SoDC.

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

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 the simulations, when the rate is $50Mbps$, the CPU load reaches more than 80%. Going beyond that would causes crashes, therefore the results were not reliable. There is also a high variability in the number of detected attacks, this is due to the big 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*: A key feature of edge computing concerns the opportunity to spread and coordinate service provisioning among distributed edge nodes to efficiently balance workload. However, current orchestration solutions have been mainly designed for data center environments and further efforts are required

to cope with challenges of resource-constrained edges. Also, multiple devices can collaboratively perform security functions, providing added-value benefits. For instance, in the case of intrusion detection scenarios, each containerized IDS instance can share contextual information with neighboring nodes, so to dynamically refine the detection process.

- *Security of container virtualization*: Container virtualization heavily relies on underlying kernel features to provide the necessary isolation for virtualized services [24], [25]. Therefore, specific efforts should address the relevant security concerns, accounting also for misleading configuration of relevant container options. 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.

## VI. Concluding remarks

The community of academic and industrial researchers has paid remarkable attention towards the adoption of cloud-based security functions to provide on-demand defense mechanisms against the increasing malicious ICT attacks. To benefit from reduction in latency and network traffic overhead, edge environments are promising candidates to host virtualized security functions. However, the resource constraints of edge nodes can impact the overall performance of SECaaS solutions. In this paper, we shed light on the provisioning of security functions via lightweight virtualization technologies, by assessing the performance of Docker container-based IDS Suricata in a real testbed. Future works will be addressed to explore the open challenges envisioned in Section V to boost SECaaS at the network edge. Furthermore, we will extend the characterization of containerized security functions to efficiently orchestrate security 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.

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

[6] 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.

[7] "Defined Categories of Service 2011," https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_V1_0.pdf, Cloud Security Alliance - SecaaS WG, Tech. Rep., 2011.

[8] 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.

[9] 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.

[10] T. Taleb, A. Ksentini, and R. Jantti, ""Anything as a Service" for 5G mobile systems," *IEEE Network*, vol. 30, no. 6, pp. 84–91, November 2016.

[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] "ETSI GS MEC 003 Mobile Edge Computing (MEC); Framework and Reference Architecture V1.1.1," ETSI MEC ISG, Tech. Rep., 2016.

[16] "Open Fog Reference Architecture," Open Fog Consortium, Tech. Rep., 2017.

[17] 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.

[18] O. Novo, N. Beijar, M. Ocak, J. Kjällman, M. Komu, and T. Kauppinen, "Capillary networks-bridging the cellular and IoT worlds," in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 571–578.

[19] 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.

[20] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, December 2016.

[21] 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.

[22] 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.

[23] A. Sforzin, F. G. Mrmol, M. Conti, and J. M. Bohli, "RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT," in *2016 13th IEEE International Conference on Advanced and Trusted Computing (ATC 2016)*, July 2016, pp. 440–448.

[24] 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.

[25] 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.