Towards Provisioning of SDN/NFV-based Security Enablers for Integrated Protection of IoT Systems

I. Farris[1], J. B. Bernabe[2], N. Toumi[1], D. Garcia-Carrillo[2], T. Taleb[1], A. Skarmeta[2], and B. Sahlin[3]

[1] Aalto University, Finland, e-mails: {ivan.farris, nassima.toumi, tarik.taleb}@aalto.fi
[2] University of Murcia, Spain, e-mails: {jorgebernal, dan.garcia, skarmeta}@um.es
[3] Ericsson Research, Finland, e-mail: bengt.sahlin@ericsson.com

***Abstract*—Nowadays the adoption of IoT solutions is gaining high momentum in several fields, including energy, home and environment monitoring, transportation, and manufacturing. However, cybersecurity attacks to low-cost end-user devices can severely undermine the expected deployment of IoT solutions in a broad range of scenarios. To face these challenges, emerging software-based networking features can introduce new security enablers, providing further scalability and flexibility required to cope with massive IoT. In this paper, we present a novel framework aiming to exploit SDN/NFV-based security features and devise new efficient integration with existing IoT security approaches. The potential benefits of the proposed framework is validated in two case studies. Finally, a feasibility study is presented, accounting for potential interactions with open-source SDN/NFV projects and relevant standardization activities.**

I. Introduction

The Internet of Things (IoT) paradigm has the potential to make our environments smarter by leveraging the increased computing and networking capabilities of surrounding objects [1]. Connected IoT devices can, indeed, provide a fertile ground to develop advanced applications able to fully exploit the sensing and actuation operations in both industrial and domestic scenarios. However, many of these IoT-based solutions have not been designed accounting for security and privacy issues. The avalanche of expected devices can therefore bring new potential attack surfaces [2]. Not by chance, cybersecurity is considered one of main research areas towards the effective adoption of IoT solutions. Furthermore, the heterogeneity of IoT devices, ranging from smart industrial machinery to simple wearable sensors, can even increase the complexity to provide the desired protection. All these security vectors claim for new advanced mechanisms able to meet the desired defense levels.

In this vein, Telco networks are progressively facing a drastic transformation by embracing Software Defined Networking (SDN) and Network Function Virtualization (NFV) [3]. SDN introduces a new level of network programmability, by decoupling control and data planes. This network model enables novel security defense mechanisms, such as promptly managing malicious traffic and enabling secure network zones. NFV leverages virtualization technologies to deploy network elements as software instances, thus allowing an increased level of flexibility and elasticity in service provisioning [4] [5]. Furthermore, NFV can enable remarkable reduction in both expenditure and operational (CAPEX/OPEX) costs, by replacing dedicated hardware with commodity servers able to host software-based network appliances, including virtual security functions.

In this paper we will explore the opportunities that NFV and SDN jointly offer in coping with security threats against IoT services. The envisioned framework has been designed to provide security protection mechanisms through new software-based enablers and to create added-value services accounting for potential integration with existing IoT security mechanisms. Different levels of security policies are defined, so to decouple the desired defense intent from the low-level configuration of the underlying components and to enable a technology-agnostic refinement process. Specific focus concerns the orchestration features, which need to enforce the desired security controls over heterogeneous domains, such as SDN/NFV and IoT networks.

The paper is organized as follows. Section II provides an overview of state-of-the-art security solutions in software-based Telco networks. In Section III we present the envisioned framework, highlighting the main potential components to provide the desired security mechanisms. In Section IV two promising use cases are presented to assess the introduced security features, whereas Section V includes a feasibility study of the framework, analyzing the current SDN/NFV open-source projects. Section VI presents potential contributions to relevant standardization bodies. Conclusions are drawn in Section VII.

II. Related Work

The concept of SECurity-as-a-Service (SECaaS) [6] has been initially introduced to dynamically provide security mechanisms in cloud environments. The Cloud Security Alliance (CSA) has defined guidelines for cloud-delivered defense solutions, to assist enterprises and end-users to widely adopt this security paradigm shift [7]. In this vein, specific research efforts have developed schemes to appropriate model virtualized security services [8].

Accounting for the main advantages to move security countermeasures within networks, SDN and NFV can play key roles to face the increasing IoT threats [9]. In [10] several examples of security applications using SDN are described,

978-1-5386-3070-9/17/$31.00 ©2017 IEEE

whereas the feasibility of deploying various SDN-based security functions has been investigated in [11]. A secure SDN IoT network architecture, BlackSDN [12], is proposed to increase protection of IoT communications by encrypting both the meta-data and packet payload, and using the SDN controller as a trusted third party. Furthermore, NFV allows for on-demand deployment of virtual security functions within network, thus avoiding traffic rerouting compared to classic cloud-based approaches. To this aim, in [13] an approach towards the adoption of security policies management with dynamic network virtualization is proposed.

However, the joint use of SDN and NFV security features is currently at a preliminary stage and significant efforts are still required to fully exploit their benefits. Furthermore, the integration with existing security solutions, especially for IoT, is still missing. In this paper, we propose a novel framework to efficiently integrate SDN/NFV-based security countermeasures to cope with the increasing threats of IoT systems.

III. An SDN/NFV-based Security Framework

The envisioned security framework aims at providing self-protection, self-healing, and self-repair capabilities through novel enablers and components. It is designed to manage security policies and define relevant security controls to be orchestrated over heterogeneous networks. The required security actions can be enforced in different kinds of physical/virtual appliances, including both IoT networks and software-based networks. To this aim, the proposed architecture defines three main planes as shown in Figure 1. The user plane provides interfaces and tools allowing end-users to specify the desired policy definition, service monitoring and management. The orchestration plane plays a key role in translating the user policies in security mechanisms and provides dynamic reconfiguration and adaptation in case of deviation from the expected behaviour. The security enforcement plane manages the resource usage and real-time operation of the services and provides network connectivity components for the security enablers. In addition a seal management plane combines security and privacy standards with run time monitoring that allows to verify if the platform is running in a trusted manner. The main features and components of each plane are described in the remainder of this section.

A. User Plane

The User Plane includes interfaces, services, and tools to end-users for policy definition, system monitoring and service management. Its policy editor provides an intuitive and user-friendly tool to configure security policies governing the configuration of the system and network, such as authentication, authorization, filtering, channel protection, and forwarding. The high level policies serve as input to the policy interpreter component of the security orchestration plane to facilitate the orchestration of security enablers required to satisfy the user policies.

B. Security Orchestration plane

The Security Orchestration plane enforces policy-based security mechanisms and provides run-time reconfiguration and adaptation of security enablers, thereby providing the framework with intelligent and dynamic behavior. It includes: Monitoring component, Reaction component, Security Orchestrator, Policy Interpreter, and Security Enablers Provider. It is an innovative layer of our architecture and provides self-protection and self-healing capabilities for softwarized networks through novel modules.

The *Policy Interpreter* module receives as input the policies specified in a high-level language and identifies the capabilities needed to enforce such policies (capability matching). Then, the Interpreter interacts with the *Security Enablers Provider* to identify the SDN/NFV-based enablers that are able to enforce the desired capabilities. The Policy Interpreter performs a first refinement process translating the high-level security policies into a set of policies defined in a medium-level security language. Besides, it generates a graph that describes how the user packets will be processed by enablers. This medium-level security policy language allows to abstract the orchestration process, thereby empowering interoperability among different security enablers, which might use vendor-specific mechanisms to generate low-level security configurations to be enforceable in NFV and SDN networks. After receiving these medium-level security policies, the *Security Orchestrator* selects the enablers to be effectively deployed, accounting for the security requirements, the available resources in the underlying infrastructure, and optimization criteria. Then, it requests a second policy refinement process, which is carried out by the Policy Interpreter to translate the medium-level security policies into specific low-level configurations according to the selected enablers.

The *Monitoring* component collects security-focused real-time information related to the system behavior from physical/virtual appliances. Its main objective is to provide alerts for the reaction module in case something is misbehaving. Security probes are deployed in the infrastructure domain to support the monitoring services. Then, the *Reaction* component is in charge of providing appropriate countermeasures, by dynamically defining reconfiguration of the security enablers according to the circumstances. The reaction outcomes are then analyzed by the Security Orchestrator, which enforces the corresponding enablers' countermeasures. In this way, the overall framework can guarantee self-healing and resilience abilities, by constantly ensuring the satisfaction of the security requirements defined in the end-user policies.

Although it is not shown in Fig. 1, the envisaged architecture is also endowed by a transversal plane called *Seal Management Plane* that combines security and privacy standards. This plane provides users with a run-time indication of the overall level of trust in the system, combining normative approaches and run-time monitoring. Its normative approaches include analysis and integration with international standards, such as the regulation of the European General

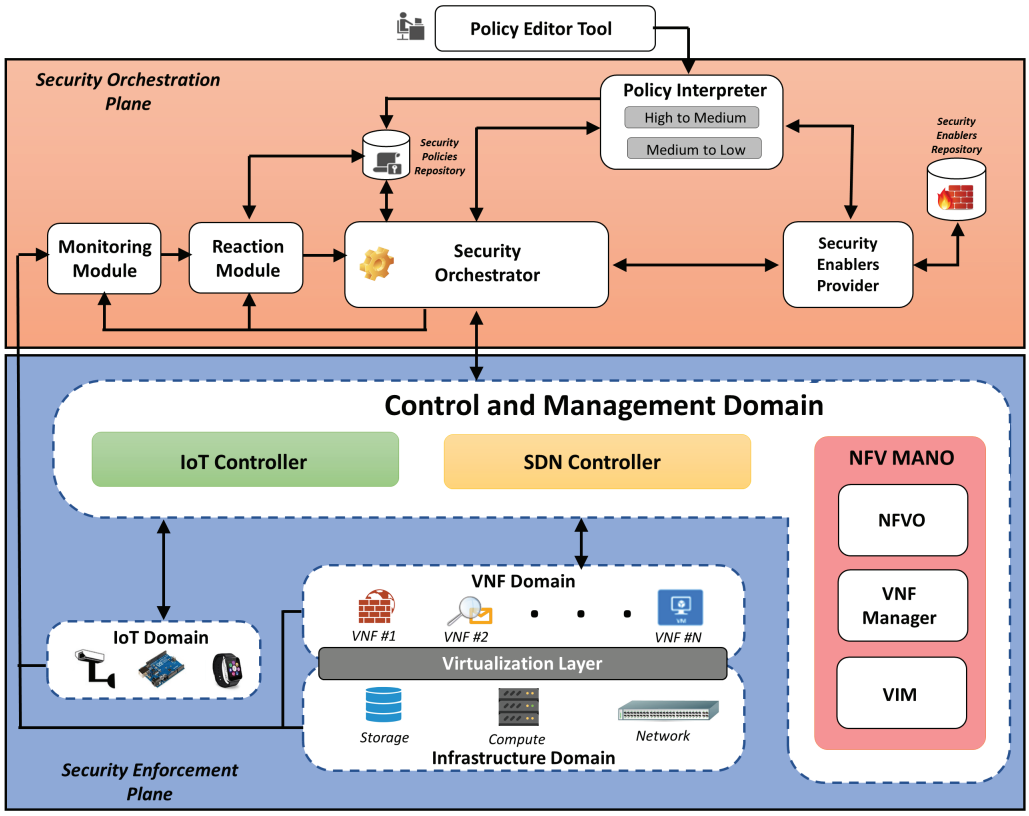

Fig. 1. Architecture high level overview.

Data Protection, security related ISO standards, and methodologies for security and privacy labeling.

C. Security Enforcement Plane

The Security Enforcement Plane includes both the envisioned security enablers and the components required for their management.

1) Control and management domain: The Control and Management domain modules supervise the usage of resources and run-time operations of security enablers deployed over software-based and IoT networks. A set of distributed SDN controllers takes charge of communicating with the SDN-based network elements to manage connectivity in the underneath virtual and physical infrastructure. NFV ETSI MANO-compliant modules support secure placement and management of virtual security functions over the virtualized infrastructure. As the envisioned framework aims to cover legacy IoT scenarios, different IoT controllers can be used to manage IoT devices and low power and lossy networks (LoWPANs). These IoT controllers are usually deployed at the network edge (e.g., gateways) to enforce security functions in heterogeneous IoT domains.

2) Infrastructure and Virtualization domain: This domain comprises all the physical machines capable of providing computing, storage, and networking capabilities to build an Infrastructures as a Service (IaaS) layer by leveraging appropriate virtualization technologies. This plane also includes the network elements responsible for traffic forwarding, following the rules of SDN controllers, and a distributed set of security probes for data collection to support the monitoring services.

3) VNF domain: The VNF domain accounts for the VNFs deployed over the virtualization infrastructure to enforce security within network services. Specific mechanisms will be developed to verify the trustworthiness of VNFs and to continuously monitor their key parameters. Specific attentions will be addressed to the provisioning of advanced security VNFs (such as virtual firewall, Intrusion Detection/Prevention System (IDS/IPS), channel protection, etc.), capable to provide the defense mechanisms and threat countermeasures requested by security policies.

4) IoT domain: This domain comprises the IoT devices to be controlled. This includes the security enablers, actuators or software agents needed to enforce the security directives coming from the orchestration plane and managed, at the enforcement plane, by the IoT controller. For instance, a special kind of local security agent can be deployed in IoT devices to protect the communications between two devices. To this aim, the CoAP-EAP [14] protocol can be used as lightweight authentication service that uses EAP (Extensible Authentication Protocol) transported by means of CoAP (Constrained Application Protocol) messages, with two purposes: authenticate two CoAP endpoints and derive

cryptographic material to protect the exchanges between them to bootstrap security associations at different levels of the protocol stack. In this way, if a Datagram Transport Layer Security (DTLS) channel has to be established, a Premaster secrect can be derived from the Master Secret Key (MSK) that results from the EAP authentication.

IV. Use cases

To validate the potential benefits of the proposed security framework, we present two promising use cases for cyber-physical systems, involving Multi-access Edge Computing applications and Building Management system, respectively. These use-cases provide a challenging opportunity to prove the maturity of the solution offered by the security and trust assessment architecture in realistic scenarios.

A. MEC use case

Emerging IoT-based applications, such as autonomous cars, industrial automation systems, and Tactile Internet, present demanding requirements in terms of tolerable latency and traffic generation. To face these challenges, the Multi-access Edge Computing (MEC) paradigm is gaining high momentum, boosting increased processing and storage capabilities towards the network edge [15] [16]. By leveraging virtualization technologies, enhanced edge nodes can host VNFs and third-party applications near the end-users, thus meeting the desired Quality of Service (QoS) requirements.

Accounting for the increased threats introduced by IoT devices, edge environments can also represent a strategic position in the network infrastructure to enforce security features. Indeed, accounting for the end-user protection requirements, virtualized security functions, such as IDS, can be deployed on-demand over edge nodes. These virtual network probes can monitor the traffic generated by the IoT devices with increased scalability and send valuable information to the Monitoring module, which triggers security alerts in case of potential threats. Then, the Reaction module is in charge of elaborating appropriate security countermeasures, such as the isolation of the compromised IoT devices. To this aim, the Security Orchestrator can exploit SDN capabilities to dynamically reconfigure the devices' connectivity. By interacting with the SDN controllers, secure network zones are created enforcing proper rules in the SDN switches deployed at the network edge.

This exemplary use case aims at highlighting how the joint management of NFV and SDN approaches can bring remarkable benefits to provide on-demand security features in software-based networks. The increased capabilities of Edge infrastructure can even augment the efficiency of the envisioned security solutions, by enabling prompt reactions near the IoT devices.

B. Building Management system use case

In smart buildings, all the electrical and mechanical devices are controlled and monitored by a centralized Building Automation System (BAS). As part of the supported services, the building usually is equipped with a Heating, Ventilation and Air Conditioning (HVAC) system exposed to the Internet whereby sensors, controllers, actuators, and equipment are accessible remotely. Internet connectivity of networked cyber-physical system enables services such as remote monitoring, reporting, billing, predictive maintenance, and remote control.

The BAS system can be subject to many incidents of hackers, breaching commercial buildings such as data-centers and supermarkets. The proposed security framework is developing new methodologies and enabling tools to increase the resilience of Building Management System (BMS) upon cyber-attacks. Various scenarios of cyber-attacks on the network of embedded systems, software systems and Internet connected devices that are part of the diverse building operations can be envisaged.

For instance, in the scope of the HVAC, our framework will effectively deal with man-in-the-middle attacks, in which the attacker manipulates some sensors introducing wrong temperature values. This kind of attack in BMS targets might produce long term financial impact, due to the imagery loss in reaching the set-point. Our proposed framework can detect uncommon temperatures and the system can react and enforce security policy to isolate the compromised sensor from the rest of the BMS system, for a time period until further investigation takes place. In addition, as a result of that attack detection, the framework can react improving the security between certain IoT devices or within devices in some networks, enforcing a security policy for channel protection.

V. Potential alignment with open-source initiatives

To accelerate the deployment of NFV and SDN paradigms, several open source and proprietary projects have been recently developed. In this section, we provide an analysis of the main open source initiatives from a security perspective, so to identify current gaps and discuss a feasibility study on the development of our proposed framework. By leveraging open-source initiatives, we aim at boosting the adoption of the envisioned security mechanisms in both academic and industrial communities.

A. Open-source NFV projects

In the following we briefly present three main NFV open-source projects:

OpenBaton[1] is an open source NFV platform whose architecture is ETSI MANO compliant. It integrates an NFV Orchestrator to coordinate network services deployment, and a generic VNF Manager that can be replaced by either Juju or customized VNFMs using a vnfm-sdk. The life-cycle of deployed VNFs can be managed through an Element Management System (currently only available for Debian-based x86 operating systems). OpenBaton also enables multi-tenancy between different operators.

[1]Open Baton project, http://openbaton.github.io

Open Source Mano (OSM)[2] is an ETSI project that aims to provide End-to-End service provisioning and orchestration by means of a Network Service Orchestrator, as well as Resource Orchestrator responsible for processing the resource-allocation requirements of each VNF, based on the corresponding descriptor. OSM can also integrate multiple VIMs for resource provisioning, and SDN controllers for network management.

Open Network Automation Platform (ONAP)[3] is a recent project derived from the merging of two different open-source NFV platform, i.e., ECOMP (Enhanced Control, Orchestration, Management and Policy) and Open-O. It is also ETSI MANO compliant and includes further software subsystems, as well as integration for SDN controllers. An interesting addition compared to other open source orchestrators is the introduction of a security framework, to increase both the security of the platform itself and the capability to deploy on-demand security services.

All of the aforementioned projects provide basic security mechanisms as authentication and authorization. Furthermore, OpenBaton uses different roles and projects in order to provide isolation between multiple tenants, and implements encryption of the communications over the Northbound APIs. ONAP's security framework supports a set of additional security applications and services such as security event analysis and response, as well as security service chaining.

B. Open-source SDN projects

Two main open-source projects are leading the adoption of SDN in a broad range of environments. *Open Network Operating System* (ONOS)[4] is a distributed and modular SDN controller specifically designed for service providers. The main goals behind its development are high availability, scalability, an performance. The network configuration can be communicated to the controller through its northbound API as *intents*, which are enforced in the underlying network through the southbound API using the OpenFlow protocol. Furthermore, some recent efforts have extended the ONOS architecture to support networking in IoT scenarios [17]. *Open DayLight* (ODL)[5] is an open source SDN controller supported by the Linux foundation. Similar to ONOS, it is distributed and supports the OpenFlow protocol for southbound communication as well as other standard protocols from the IETF. It also provides a large set of application modules, like the IoT data broker, to cover IoT domain challenges [18].

To sum up relevant security features, ONOS provides a security mode that includes a mechanism to grant fine grained access privileges to northbound applications and users, while ODL provides more elaborate mechanisms like Authentication, Authorization and Accounting (AAA), and attack detection and mitigation through the Defense4All module. In [19] a security analysis, using the STRIDE threat modeling framework[6], has also demonstrated that both controllers still present security vulnerabilities. Within our envisioned security framework we aim at exploiting SDN solutions as new countermeasures to security threats, while enhancing their inherent defense to malicious attacks.

[2]Open Source Mano project, https://osm.etsi.org/

[3]Open Source Mano project, https://www.onap.org/

[4]ONOS project, http://onosproject.org/

[5]Open DayLight, https://www.opendaylight.org/

VI. Relevant standardization activities

In this Section we illustrate current standardization activities in relevant research areas. Our objective is to identify how the outcomes of the envisioned security framework can provide novel contributions to international standards.

Regarding software-based networks, the European Telecommunications Standards Institute (ETSI) has remarkably boosted the adoption of NFV paradigm from pre-standardization studies to implementation specifications. The Industry Specification Group (ISG) for NFV has published over 50 documents, defining a common NFV architecture, main components and interfaces, and data models. Recently, significant efforts have addressed the security analysis of NFV architecture, aiming at identifying potential vulnerabilities and countermeasures actions [20]. Our envisioned framework can provide inputs on three different fronts: (i) enhanced provisioning of security VNFs; (ii) definition of security policy models to specify desired protection levels over integrated software-based networks; (iii) advanced mechanisms to increase the inherent security of the NFV infrastructure [21] [22].

To enhance security of IoT systems, significant standardization contributions have been conducted within the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). The IEEE has recently released the IEEE 802.15.9 [23] standard to transport Key Management Protocol (KMP) frames on top of IEEE 805.14.5. The IETF considers security at different levels through different Working Groups (WGs). Our envisioned framework aims at enabling control security within the IoT devices and providing contributions in several research domains. The CORE WG has defined the Constrained Application Protocol (CoAP) for managing resources in constrained networks via RESTful APIs. Beyond securing CoAP communications at transport layer with Datagram Transport Layer Security (DTLS), different works are considering how to secure the communications at application layer, such as defining Object Security (OSCOAP) [24] and Application level security for CoAP [25]. The ACE WG deals with secure authentication and authorization for accessing resources and services within the IoT domain. As part of our proposed framework, EAP over CoAP [26] will be used to provide network access authentication and bootstrap other security association protocols, such as DTLS. The 6tisch WG takes a more holistic approach considering different aspects needed for an operative low power IoT networks, including routing, network maintenance, and security challenges [27]. A minimal security framework

[6]The STRIDE Threat Model, https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[28] defines the process of network access and joining of new nodes to the network and how the link-layer keys are obtained. Accounting also for the increased interest in long-range communications for IoT devices, a new IETF WG works has been created on Low Power Wide Area Networks. Since our framework aims at covering different IoT connectivity, we will pay attention towards security aspects related to LPWAN networks. In particular, promising extensions for RADIUS [29] and Diameter [30] are considered to support AAA in LoRaWAN.

VII. Conclusions

Security threats related to IoT domains are acquiring great attention from both academic and industrial communities due to potential disruptive effects. New approaches are required especially accounting for the scalability and heterogeneity issues introduced by IoT devices. In this paper we have presented a novel framework able to efficiently integrate new security features enabled by SDN and NFV approaches in IoT scenarios. A novel orchestration layer has been designed to enable interaction with different security technologies for enforcing the desired policies, and provide prompt reactions in case of deviations from the expected behaviour. Two realistic case studies have been investigated for evaluating and fostering the adoption of the proposed framework. Finally, we have discussed potential interactions with open-source SDN/NFV projects and relevant standardization activities.

Acknowledgment

This work was partially supported by the ANASTACIA project, that has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

References

[1] L. Atzori, A. Iera, and G. Morabito, "Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122–140, 2017.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[3] 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.

[4] T. Taleb, B. Mada, M. I. 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.

[5] T. Taleb, M. Corici, C. Parada, A. Jamakovic, S. Ruffino, G. Karagiannis, and T. Magedanz, "EASE: EPC as a service to ease mobile core network deployment over cloud," *IEEE Network*, vol. 29, no. 2, pp. 78–88, March 2015.

[6] 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.

[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] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. ACM, 2015, p. 5.

[10] S. Shin, L. Xu, S. Hong, and G. Gu, "Enhancing network security through software defined networking (sdn)," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Aug 2016, pp. 1–9.

[11] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with sdn: A feasibility study," *Computer Networks*, vol. 85, pp. 19 – 35, 2015.

[12] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*. IEEE, 2015, pp. 190–198.

[13] 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.

[14] D. Garcia-Carrillo and R. Marin-Lopez, "Lightweight coap-based bootstrapping service for the internet of things," *Sensors*, vol. 16, no. 3, 2016.

[15] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5g network edge architecture orchestration," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2017.

[16] 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 Telecommunications Technologies*, 2017.

[17] A. C. G. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Towards a software-defined network operating system for the iot," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Dec 2015, pp. 579–584.

[18] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, "Sdn controllers: A comparative study," in *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, April 2016, pp. 1–6.

[19] R. K. Arbettu, R. Khondoker, K. Bayarou, and F. Weber, "Security analysis of opendaylight, onos, rosemary and ryu sdn controllers," in *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, Sept 2016, pp. 37–44.

[20] ETSI ISG NFV, "Etsi gs nfv-sec 003 nfv security; security and trust guidance v1.1.1," 2014.

[21] S. Lal, T. Taleb, and A. Dutta, "Nfv: Security threats and best practices," *IEEE Communications Magazine*, vol. PP, no. 99, pp. 2–8, 2017.

[22] S. Lal, S. Ravidas, I. Oliver, and T. Taleb, "Assuring virtual network function image integrity and host sealing in telco cloud," in *Communications (ICC), 2017 IEEE International Conference on*, 2017.

[23] "Ieee recommended practice for transport of key management protocol (kmp) datagrams," *IEEE Std 802.15.9-2016*, pp. 1–74, Aug 2016.

[24] G. Selander, J. Mattsson, F. Palombini, and L. Seitz, "Object Security of CoAP (OSCOAP)," IETF, Internet-Draft draft-ietf-core-object-security-03, May 2017, work in Progress.

[25] D. Garcia, S. N. M. Garcia, and R. Lopez, "Application Layer Security for CoAP using the (D)TLS Record Layer," IETF, Internet-Draft draft-garcia-core-app-layer-sec-with-dtls-record-00, Dec. 2016, work in Progress.

[26] D. Garcia and R. Lopez, "EAP-based Authentication Service for CoAP," IETF, Internet-Draft draft-marin-ace-wg-coap-eap-05, Apr. 2017, work in Progress.

[27] T. Watteyne, M. R. Palattella, and L. A. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement," RFC 7554, May 2015.

[28] M. Vuini, J. Simon, K. Pister, and M. Richardson, "Minimal Security Framework for 6TiSCH," IETF, Internet-Draft draft-ietf-6tisch-minimal-security-02, Mar. 2017, work in Progress.

[29] D. Garcia, R. Lopez, A. Kandasamy, and A. Pelov, "LoRaWAN Authentication in RADIUS," IETF, Internet-Draft draft-garcia-radext-radius-lorawan-03, May 2017, work in Progress.

[30] A. Kandasamy, R. Lopez, D. Garcia, and A. Pelov, "LoRaWAN Authentication in Diameter," IETF, Internet-Draft draft-garcia-dime-diameter-lorawan-00, May 2016, work in Progress.