Liability-Aware Security Management for 5G

Chrystel Gaber*, José Sánchez Vilchez*, Gürkan Gür†, Morgan Chopin*, Nancy Perrot*, Jean-Luc Grimault *, Jean-Philippe Wary*
*Orange Labs, Châtillon, France
†Zurich University of Applied Sciences, Winterthur, Switzerland
Email: *{firstname.lastname}@orange.com,†gueu@zhaw.ch

***Abstract*—Multi-party and multi-layer nature of 5G networks implies the inherent distribution of management and orchestration decisions across multiple entities. Therefore, responsibility for management decisions concerning end-to-end services become blurred if no efficient liability and accountability mechanism is used. In this paper, we present the design, building blocks and challenges of a Liability-Aware Security Management (LASM) system for 5G. We describe how existing security concepts such as manifests and Security-by-Contract, root cause analysis, remote attestation, proof of transit, and trust and reputation models can be composed and enhanced to take risk and responsibilities into account for security and liability management.**

***Index Terms*—Liability, network slicing, 5G, trust and reputation models, Security SLAs (SSLAs).**

I. Introduction

5G is claimed to satisfy the dramatically growing need of users and things for diverse services and massive connectivity in future networks. Indeed, 5G networks are expected to be multi-access to serve around 7 trillion heterogeneous connected things, amongst which 20 billions are human-oriented devices, with 1000x higher mobile data volume per area and 10x-to-100x higher user data rate, as stated by the 5G-PPP partnership [1]. In addition, 5G is envisaged to be an extremely flexible and dynamic network to fulfill the myriad of use cases and verticals with very different requirements such as ultra-low latency or ultra-reliability. As an enabler to meet the service levels expected by verticals, 5G slicing is proposed to deploy several logical networks on top of the same infrastructure. In that setting, each slice is optimized to fulfill certain objectives imposed by specific use cases [2]. Network softwarization via Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies is a key paradigm for implementing 5G slicing.

This technological revolution in communications and networking implies the shift to more enriched business cases or advanced consumer services where multi-party 5G networks with slicing are crucial. However, this situation requires opening up a 5G infrastructure (e.g. towers, gateways, networks) to third parties (e.g. mobile devices, IoT devices, VNF providers), which raises many questions regarding the responsibilities among partners. In absence of any prior trust relationship, the slice provider (SP) always bears the financial or legal impact of fraud or mischief. The SP is legally bound by contracts to provide the agreed QoS. Additionally, if there are accidents or frauds in a critical service using a slice (e.g. due to an insecure product or operation), the SP or any Slice Component Provider can be liable.

In this multi-party and multi-layer 5G architecture, the definition of liability and responsibilities when security breaches occur is essential to support confidence between parties and compliance with regulation, since zero-risk security cannot be achieved. As in the "Y2K Act" [3], one can assume that, legal and financial responsibility in 5G contexts will have to be distributed proportionately among any liable parties involved in a service. However, the appreciation of the stakeholder's liabilities is defied by 5G's worldwide deployment, multiple stakeholders and complex interconnections of hardware and software at different levels. In addition to this, many different orchestration entities appear at different layers in 5G networks, such as the VIM, VNFM and NFV, which make multiple decisions concerning the end-to-end service management with partial views of the network. This implies that responsibility regarding mismanagement and outages is blurred even within the same administrative domain.

To address these challenges, this paper proposes to adapt Security-by-Contract principles [4]–[6] to create a Liability-Aware Security Management (LASM) system for 5G. To the best of our knowledge, there is no prior work related to such systems since existing systems only take into consideration security, trust or performance as detailed in Section II. The rest of this paper is organized as follows. Section II introduces several key notions and related works, while Section III defines the goals and requirements. The proposed LASM architecture and its building blocks are detailed in Section IV. Finally, Section V concludes the paper and provides insights on future steps.

II. Background

Several multi-party business models are possible in 5G, where traditional services can be enriched by adding external third-party functionalities. One example is the "operator offer enriched by partner" [11] shown in Figure 1. This concrete example consists of enriching a connectivity offer from a operator with a set of third-party applications. This third-party application could be a VNF embedded in the same operator premises.

The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

TABLE I
LIABILITY CONCEPTS AND TERMINOLOGY.

Name	Definition
Trust	The most important behavioural factor in managing relationships and in overcoming risks/uncertainty. It relies either on the formalization of agreements (contracts), mutual confidence established by fruitful exchanges and acquaintance [7]. Trust is a non-reciprocal ($T_{i,j} \neq T_{j,i}$) peer-based property where the trustor forms an opinion on how good the trustee is on providing a specific service. It is the subjective degree of belief a trustor has on a trustee to perform a concrete task in this specific system [8]. It depends on context and corresponds to a real number of positive collaborations between trust and trustee [9].
Reputation	The collective opinion by members of a community and hence is a community-based property. It is a function of trust. In most reputation models in the state of the art [8], reputation should be very difficult to earn and very easy to lose, especially when the reputation concerns a management entity carrying out critical tasks.
Risk exposure	A combination of 1) a Loss, the financial consequences of the risk and a peril, 2) the uncertain event provoking a loss and 3) an object of risk, the exposed resource [10].
Responsibility	A party's capability to organize itself and potential delegates in order to achieve a task as agreed and to provide evidence on its achievement.
Accountability	Gathering evidences of the execution of a task in order to "give accounts" or inform, explain why specific decisions have been taken without any consideration related to a fault.
Liability	Accountability towards legislation. Financial consequence of an outage, that can increase by actions or pre-conditions which increase the probability or the impact of a potential danger [10].

In this example, the operator acts as intermediary between its customers (residential users and enterprises) and the different third-parties necessary to provide those high-value services. It becomes both provider and client (tenant), thus with different responsibilities and rights in this high-value chain. This example manifests that responsibility in multi-party services is distributed among all partners. Indeed, in this context, in addition to cooperation among partners, a minimal level of transparency on how each partner manages its domain is crucial. Trust and reputation mechanisms or security-by-contract approaches can help to increase confidence between partners. We consider for the rest of the article that partners follow an strategic type of alliance, defined in the Etics project [12]. In this alliance, each partner is an independent entity, i.e. it has the sufficient autonomy to manage its domain. However, the combination of autonomous domains may lead to unpredictable and uncertain consequences regarding the end-to-end service quality level offered to customers, mainly due to the interaction of heterogeneous orchestration mechanisms of each domain. With a liability perspective, we are particularly interested in identifying the domain(s) or partners responsible for fault(s) and outages in order to hold those domains responsible for the damage inflicted upon customers.

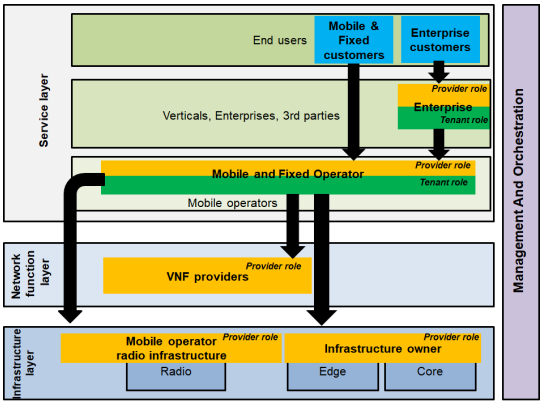

Fig. 1. Multi-party and multi-layer 5G architecture for service delivery.

Liability is a multifaceted conceptualization with a large set of associated concepts and terminology. In that regard, Table I synthesizes definitions of liability-related concepts and terminology from the perspectives of different domains such as Artificial Intelligence [13], construction contracts [7], Access Control [14], software development [15], trust modeling [9] or insurance [10]. For instance, trust and reputation are key concepts to build a Trust and Reputation Model (TRM), whose goal is to distribute trust and reputation to assess the associated risk in engaging in an interaction between two entities (trustor and trustee). This risk is generally based on the experience perceived by the trustor from past interactions with the trustee.

III. LIABILITY-AWARE SECURITY MANAGEMENT (LASM)

To the best of our knowledge, there is no prior work on a LASM system for 5G slice management as existing management systems only consider security, trust or performance. In that regard, one example is [16], where an Information System Security Risk Management meta-model including responsibility, accountability and commitment was used to create a multi-agent system-based architecture for broadcasting forecasts and alerts in a power distribution infrastructure. In [17], an adaptation of this model was proposed for a decision mechanism for incident reaction in telecommunications network but it is not adapted for the 5G Slicing context. A Security Panel was proposed in [18] as a platform regrouping risk managers and experts throughout the eSIM ecosystem and allowing them to collect the information required for their risks analysis.

Giaretta *et.al* propose to use Security-by-Contract paradigm for fog-based IoT management [6]. The decision to add an IoT device in the local network, update or monitor it is taken by matching the IoT device's manifest with a security policy. Costa *et. al.* [19] show that Security-by-Contract paradigm can be extended to include models and KPIs for quantitative trust management. However, responsibilities are implicit.

A. Ecosystem

As shown in Figure 2, we define the sliced 5G ecosystem and how entities (blue boxes) and roles (persons) interact with

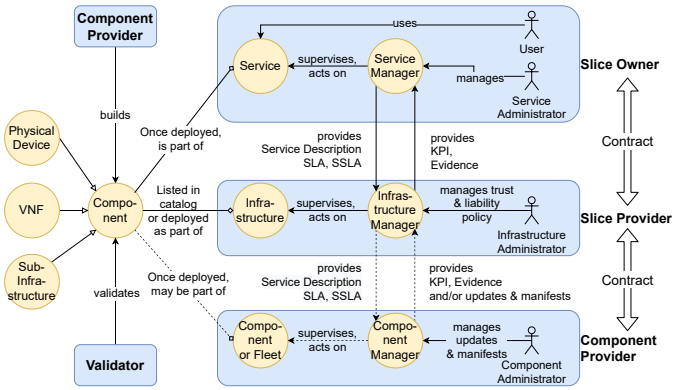

Fig. 2. Ecosystem actors model.

technical components (yellow circles) of the infrastructure based on [20]. We consider that a Slice contains hosting equipment, VNFs, IoT and mobile devices.

The *Slice Owner* (SO) owns a Slice provided by a *Slice Provider* with the intent of deploying a *Service* over it. A *Service Administrator* manages the Service at application level through a *Service Manager*. The SP's *Infrastructure Administrator* (IAdm) ensures that the SLA (Service Level Agreement) or SSLA (Security Service Level Agreement) of the Slice and its underlying *Infrastructure* are fulfilled by defining and enforcing security policies through the *Infrastructure Manager*. The *Infrastructure* is made of several *Components* provided by a *Component Provider* (CP) and tested or certified by a *Validator* (V). Either being physical devices, virtual functions or sub-infrastructures operated by a delegated third-party, Components may be part of a multi-infrastructure (or multi-domain) fleet and managed through a *Fleet Manager*. This is particularly interesting in those cases where the Component is a part of the infrastructure and its operation is delegated to a sub-contractor.

As a result of the Component definition, the Infrastructure can have multiple layers of subsystems potentially operated by third parties. In the rest of this article, we assume that the Infrastructure Manager only manages a layer i of C_i Components and does not manage the internals of any Component in this layer. Each Component is considered as a black box whose responsibility is to respect the SLA/SSLA and provide the agreed KPIs.

B. Objectives

A LASM Infrastructure Manager (LASM-IM) assists the Infrastructure Administrator (IAdm) by automating management decisions to fulfill its commitments and obligations optimally and by providing him insight on the taken decisions and the overall status. As depicted in Figure 2, the Infrastructure Manager interacts with the Service Manager to provide measures and evidence that the requested SLAs/SSLAs are fulfilled. It either acts directly on a Component or through a Fleet Manager to enforce security measures. It gathers evidence of the taken actions that can be aggregated for reporting purpose or produced in a legal claim.

To achieve its mission, the LASM-IM should analyse each new or updated Component to verify that its characteristics comply with its obligations (SLA, regulation, Components' requirements) and capacities in order to keep the threat and liability levels at an acceptable level. After this risk analysis, the LASM-IM proposes to the IAdm some recommendations on the deployment or configuration of security services and Low Level Security Policies, organization of the network topology so that obligations are fulfilled while optimizing costs, performance, risk exposure and liability level. Any potential conflicting obligations should be notified to the IAdm for information and resolution. The LASM-IM aims at preventing incidents by using trust and reputation metrics and acting on the Infrastructure. If a Component is not able to perform a task because of loss of reputation or trust, its task should be reassigned. In the case where issues occur nevertheless, the LASM-IM collects evidence, reacts and notifies impacted stakeholders so that they are able to analyse and mitigate it.

Since the SP and CPs are not necessarily acquainted or bound by contractual relationships, it is necessary to formalize the Components' properties and conditions of use as a user manual would do, i.e. the notion of Manifest. This Manifest draws the boundaries of the liability of both the CP and the SP.

IV. Proposed LASM Architecture

A. High Level Architecture

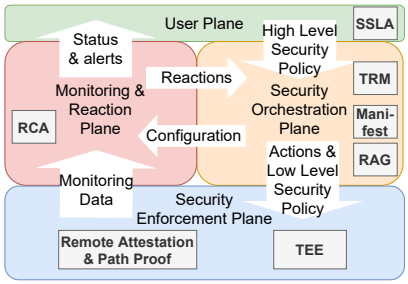

Fig. 3. LASM high level architecture.

LASM can be achieved by enhancing security orchestrators with building blocks which allow to appreciate and establish stakeholder's liabilities. Manifests are the cornerstone of the high level architecture illustrated in Figure 3 because their authors commit on the correct description of the Components features, security needs and provided security services. These descriptions are then used as baseline for defining expected behavior, setting security policies, configuring the Root Cause Analysis (RCA) or Risk Assessment Graphs (RAG) modules and calculating liability-related trust and reputation metrics which measure how well Manifests' authors respected their commitment. Liability is further enforced by Remote Attestation and Trusted Execution Environment (TEE) modules to ensure non-repudiation of actions and compliance proofs. The security orchestrator decides how the Infrastructure should be

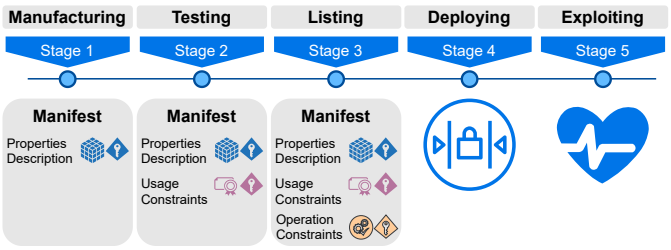

Fig. 4. Life-cycle of a Component and its manifest.

organized and managed using the optimal countermeasures selected by RAG based on network topology and the liability-related trust and reputation metrics. In presence of changes, network failures and faults, the RCA can detect those changes and inform RAG and TRM to improve countermeasure placement and risk assessment in establishing new routes through trusted and liable network elements or deploying VNF in trusted and liable hosts.

B. Manifests

In the 5G ecosystem, several profiles and manifests coexist implicitly referencing different responsibility levels. Their authors can commit on properties as in the deployment template of Virtual Network Function Descriptors (VNFD) [21], Network Service Descriptors (NSD) [22] and the SUIT manifest for IoT firmware updates [23]. Recommendations for control on a Component's usage can also be expressed as done by the Manufacturer Usage Definition (MUD) profiles for IoT devices [24]. Opposed to properties, recommendations imply that the Manufacturer advises some controls on the Components but it is up to the IM to enforce them.

We propose to combine characteristics of various existing manifests in order to define and assign different levels of responsibilities, as described in Figure 4. The desired manifest is modular and follows the 5G infrastructure component throughout its life-cycle. During the manufacturing phase, the CP builds the component by using building blocks provided by software editors, hardware manufacturers or Service Providers. CP provides a first version of the manifest based on the description of features and preliminary usage recommendations. Then, the Validator tests the component, evaluates risks and compliance to applicable requirements. Based on its observations, it can add properties or describe controls or requirements, called usage constraints, that need to be enforced by the SP to guarantee normal functioning or avoid exploitation of a known vulnerability. The SP lists the Component in its Catalog and may perform additional tests. It identifies operation constraints, similar to usage constraints, except that they express conditions to comply with specific infrastructure requirements, company policy or local regulation and are not available to other stakeholders. The SP uses the manifest to decide how, where and under which conditions a Component should be deployed. After putting the Component in service, the SP uses the Manifest to decide whether and how to observe and manage the Component. It can also be used as a baseline to define expected behavior for monitoring.

Thus, each stakeholder is able to express its commitments and expectations to/from other parties. In turn, this will help SPs to formalize their risks and take decisions in order to manage the level of risk of their infrastructures. In the future, we will propose organisational and technical solutions to allow the SP to publish and share manifests that it enhanced as part of LASM system.

C. Root Cause Analysis (RCA)

An RCA algorithm is a fault management technique to pinpoint the responsible entity causing a disruption. In our context, it indicates to which extent how faults propagate through the network and eventually lead to service failures. This entity may be a network component, a management entity performing an incorrect action, or even a networking service not working on the expected conditions. In general, RCA algorithms reason over a network model (model-based RCA) comprising all analysed networked elements and services as well as the detected alarms or symptoms. We can classify RCA techniques mainly in two classes. On one hand, topology-aware approaches exploit a network model comprising the network topology. Therefore it only considers how faults in network resources impact other network resources, whereas impact of faults in network resources on services or clients is not then considered. On the other hand, service-aware approaches are an extension of topology-aware approaches to take into account the impact of faulty network resources on services as well as the clients using them. We propose a topology-aware RCA and its extension as service-aware RCA in [25] for SDN-NFV infrastructures. This framework discovers the network topology from a given SDN controller and instantiates a set of predefined templates describing inner dependencies for each discovered networked resource and generates on-the-fly a probabilistic dependency graph that includes the physical, logical, and the virtual dependencies of networking services. The RCA algorithm can then identify the root cause of failures in real-time and update the network model if the physical or virtual network topology changes.

D. Trust and Reputation Management Systems (TRM)

As noted in Section II, TRMs are generally used to assess the risk of a given interaction between two elements (a trustor and a trustee) within a system. Reputation models for web services and telecommunications can be classified on how reputation is assessed (i.e. subjective, objective, hybrid) but also on how those are mathematically built (i.e. probabilistic approaches, deterministic, fuzzy approaches) [26]. Trust and reputation models have been applied to many different technologies with very different purposes, mainly security. A first example is wireless sensor networks, where the equipment is hardware-constrained and very easily compromised. A trust and reputation model can be used to evaluate the trustworthiness of the captured information on an equipment [8]. A second example is cognitive radio networks, where the spectrum information provided by the sensing units must be verified by means of a trust and reputation model to make

sure interference between the secondary users and primary users (legitimate users have the right to transmit in those frequencies) does not occur.

Nevertheless, there are plenty of other different purposes, such as mobile ad hoc networks, where network nodes have freedom to choose which nodes they use as relay to exchange information. Trust and reputation models can be applied to this context to assess how trustworthy the nodes are based on their performance when transmitting packets. The nodes can collect evidence on their past interactions with their neighbours and rank them based on their trustworthiness and reputation and choose those most trustworthy and renowned neighbors to optimize the throughput [8]. Trust and reputation models can be also used for automating the decisions regarding the choice made by a user of a virtual network over multiple virtual networks claiming to cater for a given level of service to that user [27]. A hybrid reputation model was proposed by [26] to assess the Quality of Experience in the context of web services, where QoE and user context are subjective metrics and QoS and QoE aggregation are objective ones. In addition, there are some TRMs for softwarized networks, such as the trust model based on reputation scores to evaluate SDN controllers proposed by Mughal et al. in [28]. Betge-Brezetz et al. in [29] propose a trust-oriented controller proxy that intermediates between the controllers and the data plane by making sure the flows sent by different controllers are correct. Isong et al. in [30] propose to include trust between SDN applications and the SDN controller to control how efficient is the use of the networking resources by the SDN applications and prevent attacks.

E. Remote Attestation, Proof Of Transit, and TEE

TEE [31], Remote Attestation [32] and Proof of Transit [33] are complementary technologies which can be coupled to deliver evidences that the Components comply with specific constraints that are required to establish trust. Indeed, the TEE ensures that the host OS cannot access to the VM or container memory space. Remote attestation verifies the integrity of software components while Proof of Transit ensures that all packets follow a pre-defined path across a set of pre-determined nodes.

F. Risk Analysis Graphs

Among existing risk evaluation models, attack graphs [34] rely on graph theory to describe how existing exploits may be chained to get root access to a system (also called an attack path). This kind of mathematical model offers several advantages such as providing a compact way to express different possible attack scenarios on a system. Furthermore, the use of a graph offers a rather intuitive support for justifying the provided countermeasures or assessment measures to non-experts. Dependency graphs [35] are also based on graph theory and aim at modeling the inter-dependencies of the different components of a system. These types of graphs are mostly used to decide what would be the best answer against ongoing attacks, while attack graphs are used to give a risk assessment measure of the system.

The concept of Risk Assessment Graphs (RAGs) [36] has been developed to extend these models to a new framework that captures simultaneously the topology of a system, the vulnerabilities, the accessibility between the components, their external exposure, and the way all these elements may evolve over the time. Thus, RAGs provide a framework for fine qualitative and quantitative risk assessment approaches: to assess the impact of the vulnerabilities exploitation and their exposition surface throughout the nodes of the graph, to compute risk indicator metrics and to observe their evolution over several time periods. More precisely, the system is represented as a directed graph in which a node can be either an asset-vulnerability pair or an access point (Figure 5). An arc in the RAG means that the exploitation of a vulnerability of the source node exposes the target node to the exploitation of its vulnerability. A path corresponds to a potential violation of a node. A potentiality function and an accessibility function are also introduced in the model. The former evaluates the likelihood of each attack at each time slot. On the other hand, the accessibility function gives the ratio of time the system assets are accessible from each other at each time slot. The accessibility and potentiality functions are used to evaluate, respectively, the nodes and the arcs at each time slot. Last, RAGs could be used as an input to determine the best strategies to secure a system. Given a set of available countermeasures associated to the vulnerabilities (ranging from firmware updates or patches to VNF deployments), several optimization models have been developed to solve security-issue optimization problems [37], e.g., where to place counter measures *a priori* to mitigate the risk of a chain of exploits. An interesting research question is the *online* variant of this problem where the optimal placement of counter measures is decided over time.

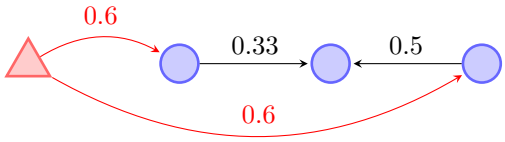

Fig. 5. RAG with one access point (red triangle) and three asset-vulnerability nodes (blue circles). Accessibility values are given on the arcs.

G. Security Service Level Agreements (SLAs)

SLAs have been extensively investigated for cloud and telecom infrastructure. Among them, Security SLAs for Cloud Infrastructure [38] need to be adapted for network infrastructure and slicing. For this, research should identify Key Performance Indicators (KPIs) to measure security and investigate how to aggregate them so that administrators are able to optimize their orchestration choices to maximize SSLA compliance. These KPIs should illustrate the security level of the end-to-end Slice, the interface between Slice Owner and a Slice Provider or between Slice Providers and subcontracted Component

Providers. Other challenges such as defining publicly verifiable proofs of compliance, automated incentives and penalties [39] should also be investigated.

V. Conclusion and future works

This paper defines the concept of a LASM System and proposes an architecture to achieve this vision inspired by Security-by-Contracts. It leverages existing technical modules such as SSLAs, RCA, RAG, TRM, Remote Attestation, TEE and manifests. The INSPIRE-5Gplus project will pursue this work by building a LASM Proof of Concept, investigating the challenges highlighted for each technology, evaluating their relevance and added value to manage the liabilities of each component and tenant.

References

[1] 5GPPP, "5G Infrastructure Public Private Partnership (5GPPP) the next generation of communication networks and services," http://superfluidity.eu/wp-content/uploads/5GPPP-brochure-draft02.pdf.

[2] GSMA, "Network Slicing Use Cases Requirements," https://www.gsma.com/futurenetworks/wp-content/uploads/2020/01/2.1_Network-Slicing-Use-Case-Requirements-Booklet-1.pdf, 2020.

[3] D. Mulvin, "The legal and political battles of Y2K," *IEEE Annals of the History of Computing*, 2020.

[4] N. Dragoni, F. Massacci, C. Schaefer, and E. Vetillard, "A Security-by-Contract Architecture for Pervasive Services," in *Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)*, 2007.

[5] N. Dragoni and F. Massacci, "Security-by-Contract for web services," *SWS*, 2007.

[6] A. Giaretta, N. Dragoni, and F. Massacci, "IoT Security Configurability with Security-by-Contract," *Sensors*, vol. 19, no. 19, p. 4121, 2019.

[7] W. K. Wong, S. O. Cheung, T. W. Yiu, and H. Y. Pang, "A framework for trust in construction contracting," *International Journal of Project Management*, vol. 26, no. 8, pp. 821 – 829, 2008.

[8] D. D. S. Braga, M. Niemann, B. Hellingrath, and F. B. D. L. Neto, "Survey on Computational Trust and Reputation Models," *ACM Comput. Surv.*, vol. 51, no. 5, Nov. 2018.

[9] R. A. C. Bianchi and R. L. D. Mántaras, "Should I trust my teammates? An experiment in Heuristic Multiagent Reinforcement Learning," in *IJCAI'09, W12: Grand Challenges for Reasoning from Experiences*, 2009.

[10] L. Condamin, J.-P. Louisot, and P. Naïm, *Risk quantification - Management Diagnosis and Hedging*. John Wiley and Sons, 2007.

[11] NGMN Alliance, "5G White Paper," *Next generation mobile networks, white paper*, vol. 1, 2015.

[12] ETICS, "Final publishable summary report," May 2013. [Online]. Available: https://www.laquadrature.net/files/ETICS_final_publishable_summary.pdf

[13] M. Baldoni, C. Baroglio, O. Boissier, K. M. May, R. Micalizio, and S. Tedeschi, "Accountability and Responsibility in Agent Organizations," in *PRIMA 2018: Principles and Practice of Multi-Agent Systems*, T. Miller, N. Oren, Y. Sakurai, I. Noda, B. T. R. Savarimuthu, and T. Cao Son, Eds. Cham: Springer International Publishing, 2018, pp. 261–278.

[14] R. Wies, *Using a Classification of Management Policies for Policy Specification and Policy Transformation*. Boston, MA: Springer US, 1995, pp. 44–56.

[15] Ari Takanen and Petri Vuorijärvi and Marko Laakso and Juha Röning, "Agents of responsibility in software vulnerability processes," *Ethics and Information Technology*, 2004.

[16] G. Guemkam, C. Feltus, P. Schmitt, C. Bonhomme, D. Khadraoui, and Z. Guessoum, "Reputation Based Dynamic Responsibility to Agent Assignement for Critical Infrastructure," in *2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, vol. 2, 2011, pp. 272–275.

[17] C. Bonhomme, C. Feltus, and D. Khadraoui, "A multi-agent based decision mechanism for incident reaction in telecommunication network," in *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, 2010, pp. 1–2.

[18] C. Gaber, J.-L. Grimault, C. Loiseaux, M. Hajj, L. Coureau, and J.-P. Wary, "How increasing the confidence in the eSIM ecosystem is essential for its adoption." [Online]. Available: https://hellofuture.orange.com/en/how-increasing-the-confidence-in-the-esim-ecosystem-is-essential-for-its-adoption/

[19] G. Costa, N. Dragoni, L. Aliaksandr, F. Martinelli, F. Massacci, and M. Ilaria, "Extending Security-by-Contract wth Quantitative Trust on Mobile Devices," *International Conference on Complex, Intelligent and Software Intensive Systems*, 2010.

[20] G. Arfaoui, J. M. S. Vilchez, and J.-P. Wary, "Security and resilience in 5G: Current challenges and future directions," in *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 2017, pp. 1010–1015.

[21] ETSI, *NFV-IFA 011 VNF Packaging Specification*, ETSI Std., 2016.

[22] ——, *NFV-IFA 014 Network Service Templates Specification*, ETSI Std., 2016.

[23] B. Moran, H. Tschofenig, and H. Birkholz, "SUIT CBOR manifest serialisation format (draft)," IETF, Jul. 2019.

[24] E. Lear, R. Droms, and D. Romascanu, "RFC 8520 - Manufacturer Usage Description Specification," IETF, Mar. 2019.

[25] J. M. Sánchez, I. G. Ben Yahia, and N. Crespi, "Self-modeling based diagnosis of services over programmable networks," in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, 2016, pp. 277–285.

[26] T. Ciszkowski, W. Mazurczyk, Z. Kotulski, T. Hoßfeld, M. Fiedler, and D. Collange, "Towards Quality of Experience-based reputation models for future web service provisioning," *Telecommunication Systems*, vol. 51, pp. 283–295, 2012.

[27] L. Wen, P. Lingdi, W. Chunming, and J. Ming, "Distributed Bayesian Network Trust Model in Virtual Network," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, 2010, pp. 71–74.

[28] B. K. Mughal, S. Hameed, and B. Hameed, "Isolating Malicious Controller(s) In Distributed Software-Defined Networks with Centralized Reputation Management," *International Journal of Future Generation Communication and Networking*, vol. 11, no. 5, pp. 11–26, 2018.

[29] S. Betgé-Brezetz, G.-B. Kamga, and M. Tazi, "Trust support for SDN controllers and virtualized network applications," in *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2015, pp. 1–5.

[30] B. Isong, T. Kgogo, F. Lugayizi, and B. Kankuzi, "Trust establishment framework between SDN controller and applications," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2017, pp. 101–107.

[31] F. van Lingen, M. Yannuzzi, A. Jain, R. Irons-Mclean, O. Lluch, D. Carrera, J. L. Perez, A. Gutierrez, D. Montero, J. Marti, R. Maso, and a. J. P. Rodriguez, "The Unavoidable Convergence of NFV, 5G, and Fog: A Model-Driven Approach to Bridge Cloud and Edge," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 28–35, 2017.

[32] *ETSI GR NFV-SEC018 Report on NFV Remote Attestation Architecture*, ETSI Std., 2019.

[33] F. Brockners, S. Bhandari, T. Mizrahi, S. Dara, and S. Youell, "Proof of Transit," Internet Engineering Task Force, Internet-Draft draft-ietf-sfc-proof-of-transit-06, Jun. 2020, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sfc-proof-of-transit-06

[34] B. Yiğit, G. Gür, F. Alagöz, and B. Tellenbach, "Cost-aware securing of IoT systems using attack graphs," *Ad Hoc Networks*, vol. 86, pp. 23 – 35, 2019.

[35] N. Kheir, H. Debar, N. Cuppens-Boulahia, F. Cuppens, and J. Viinikka, "Cost Evaluation for Intrusion Response Using Dependency Graphs," in *2009 International Conference on Network and Service Security*, 2009, pp. 1–6.

[36] N. Kheir, A. R. Mahjoub, M. Y. Naghmouchi, N. Perrot, and J.-P. Wary, "Assessing the risk of complex ICT systems," *Annals of Telecommunications*, vol. 73, no. 1-2, pp. 95–109, 2018.

[37] A. Ridha Mahjoub, M. Naghmouchi, and N. Perrot, "A Bilevel Programming Model for Proactive Countermeasure Selection in Complex ICT Systems," *Electronic Notes in Discrete Mathematics*, vol. 64, pp. 295–304, 02 2018.

[38] C. Lee, K. M. Kavi, R. A. Paul, and M. Gomathisankaran, "Ontology of Secure Service Level Agreement," in *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*, 2015, pp. 166–172.

[39] W. Maurer, R. Matlus, and K. Parikh, "Outsourcing incentive and penalty best practices," *Gartner Research*, vol. 22, 2003.