Network Resilience in Virtualized Architectures

Diomidis S. Michalopoulos[1], Borislava Gajic[1], Beatriz Gallego-Nicasio Crespo[2], Aravinthan Gopalasingham[1], and Jakob Belschner[3]

[1] Nokia Bell Labs, Germany and France
{firstname.lastname}@nokia-bell-labs.com
[2] ATOS Research and Innovation, Spain
beatriz.gallego-nicasio@atos.net
[3] Deutsche Telekom Technology Innovation, Germany
jakob.belschner@telekom.de

Abstract. Network resilience represents one of the major requirements of next generation networks. It refers to an increased level of availability, which is of high importance especially for certain critical services. In this work, we argue for resilience as an intrinsic feature that spans multiple network domains, thereby providing a network-wide failsafe operation. Particular focus is put on virtualized architectures envisioned for 5G and beyond. Contrary to traditional architectures where all network functions were hardware-dependent, a virtualized architecture allows a portion of such functions to run in virtualized environment, i.e., in a telco cloud, allowing thus for a wider deployment flexibility. Nonetheless, parts of this architecture such as radio access might still have strong hardware dependency due to, for instance, performance requirements of the physical nature of the network elements. Capitalizing on this architecture, we shed light onto the techniques designed to guarantee resilience at the radio access as well as the telco cloud network domains. Moreover, we highlight the ability of the envisioned architecture to address security-related issues by applying threat monitoring and prevention mechanisms, along with proper reaction approaches that isolate security intrusions to limited zones.

1 Introduction

Next generation networks are expected to be able to cope with stringent requirements in terms of reliability, latency and throughput. Despite their diverse nature, such requirements need to be addressed by using a common network infrastructure, since, otherwise, the cost of deploying separate networks for distinct services would be prohibitive. Such common infrastructure needs thus to provide sufficient flexibility in terms of deployment and operation, such that diverse services are supported without substantial change on the hardware. The solution towards this end is derived from the concept of *Network Slicing* [1, 2], in conjunction with that of *Network Function Virtualization (NFV)* [3]. This results in virtualized network architectures, where the utilization of the available resources is optimized and can be flexibly allocated to the different network slices, for the purpose of the given service.

One of the major challenges associated with virtualized architectures is that of resilience. In this context, the resilience is translated into network robustness to different kinds of unexpected events and problems during the network operation. Resilience is particularly important for industrial applications and mission critical services, which operations have a very low fault tolerance. The problems that might jeopardize the network operation can be related to many aspects e.g. software, virtual or physical infrastructure, the actual implementation, deployment and configuration of the network functions. Thus, the next generation networks need to be built in a resilient way, capable of mitigating problems with critical impact on network operation.

Network resilience comprises a set of approaches, techniques and tools for ensuring the mitigation of network problems. To address this issue in future networks, it is important to adjust such design to the mode of operation in each part of the network. Specifically, it is anticipated that a part of the network functions, particularly those corresponding to high level functionalities and to the higher layers of the RAN protocol stack, are implemented in a virtualized infrastructure. On the other hand, network functions that are part of the lower layers of the Radio Access Network (RAN) often require an implementation in specialized hardware, hence they are implemented in a traditional, non-virtualized infrastructure. As a result, for attaining a sufficient end-to-end resilience level, both non-virtualized hardware and virtualized cloud environments (referred to as telco clouds henceforth) need to demonstrate the required level of robustness. These two domains have potentially different resilience issues and the approaches for achieving resilience might differ accordingly. However, resilience in both domains (i.e., RAN and telco cloud) are important building blocks for achieving overall network service resilience.

The remainder of this paper is structured as follows. A literature overview in resilience and security of existing networks and its connection to future deployments is provided in Section 2. Section 3 showcases the directions towards resilience in the RAN domain, while section 4 highlights the basic approaches followed for achieving resilience in the telco cloud. Section 5 illustrates the main security mechanisms devised for providing an advanced security level of next generation networks, while our final concluding remarks are given in Section 6.

2 Technological Advances and Challenges in Resilience and Security

In this section we elaborate on the technological progress in the domains of RAN and telco cloud related to resilience, along with security issues associated to the deployment of next generation networks.

2.1 The challenge of high RAN reliability

In the RAN domain, the dominant challenge with respect to a reliable operation is managing the highly dynamic radio channel. Providing an Ultra-Reliable Low

Latency Communications (URLLC) service requires dedicated approaches to combat e.g. a packet loss due to short-term fading. To this end, a relatively novel approach used to increase the reliability of the RAN domain is multi-connectivity [4], [5].

Multi-connectivity is a well-known concept that is used already in the LTE standards, where the main objective is to aggregate two independent radio connections for increasing the overall throughput [6], [7]. However, the main concept behind devising multi-connectivity for RAN reliability is to exploit the inherent macro-diversity effect of multiple simultaneous connections, such that the probability that at least one connection is sufficiently strong is increased [8]. As such, multi-connectivity takes a distinct role than the one used in LTE, since the packet flow is now being *duplicated* across multiple links, instead of aggregated. This entails challenges in regard to the system design since special coordination is needed between the links where duplicated data is sent. We shed light onto such design challenges in Section 3.

2.2 The challenge of resilient virtualized networks

Resilient network needs to be able to recover after an unexpected event and to resume its normal operation, without affecting the user experience. This capability is of paramount importance for network reliability and providing a service with satisfying performance especially for critical communication type such as envisioned in URLLC slice.

Advantages of SDN Software-defined networking (SDN) is growing rapidly in telecommunications due to its capability to efficiently manage end-to-end networks by decoupling control-plane and data-plane. Such scalability and flexibility can bring benefits to network management and maintenance. In general, SDN brings several advantages to mobile network architecture such as high flexibility, programmability, complete control of the network from centralized vantage point, and enables operators to deploy easily new applications, services and fine tune network policies. SDN and NFV are two closely related technologies that are often used together in cloud paradigm to complement and benefit from each other.

The integration of SDN framework in Cloud RAN (C-RAN) can provide several advantages such as dynamic control over fronthaul transport network to allocate available capacity while maintaining overall QoS requirements, realization of centralized SON (e.g., Coordinated scheduling) and configuration and load-balancing between virtual base band units (vBBUs) [9]. Although SDN is a quite matured technology, most of the SDN frameworks have been designed and developed with the major focus on supporting several use cases in fixed and transport networks. However, SDN is an important aspect that can enable dynamic control of radio and networking resources in telco cloud by re-programming/reconfiguring VNFs in real-time. Due to the stringent QoS requirements of 5G mobile networks, the SDN framework has to have low latency, resilience and scalability in order to be adapted as a control framework.

Network fault management in telco clouds In the telco cloud domain, there exist different approaches for increasing the overall resilience. Some of the common techniques for mitigating the network faults in traditional network are self-healing SON solutions [10]. Self-healing SON aims at automatizing the mitigation of outages on the level of individual network cells, including outage detection and root cause analysis. Within such framework different improvements of detection and diagnosis processes can be applied as presented in [11, 12]. The introduction of virtualization in network design and deployment brought new challenges in handling the network faults. As the faults can occur on different deployment layers, e.g. physical, virtual, application, the fault management needs to be enhanced in order to master the increased complexity in fault localization and isolation. The work targeting the fault management issues in virtualized environment has been presented in [13] where distributed fault management approach has been chosen.

However, despite the considerable progress in this field, the majority of 5G network architecture proposals did not explicitly or to a large extent target addressing the resilience levels of URLLC. The requirements on resilience has mainly been implicitly addressed by the management and control entities and mechanisms that are designed in a way to promptly react to unexpected events. For instance, as reported in [14], after a violation of QoS requirements is detected on centralized controllers, the problem mitigation is attempted through network reconfigurations. This might involve reconfigurations of network functions parameters, as well as link reconfigurations. In the case that this was not sufficient to overcome the problem, the centralized controllers send a trigger to Management and Orchestration (MANO) blocks, such as the Orchestration entity, in order to perform the action needed for problem mitigation. This might include scale out actions if the resources of network functions are scarce, as well as relocation of existing functions and deployment of new functions.

Although such architecture is capable of reacting to unexpected traffic/network events and mitigate their negative influence to a certain extent, the architecture and mitigation mechanisms are not built under the concept of resilience. In other words, there is no detailed resilience consideration intrinsic to the network design, in the sense that there is no specialized network functions for empowering the resilience or service-specific resilience requirements built in to the network design. Therefore, the aforementioned problem mitigation actions and processes are suboptimal and cannot meet different reliability requirements in an efficient way. In this regard, in Section 4 we elaborate on the most prominent challenges and envisioned solution approaches in the context of resilient virtualized networks and the scalability of its control framework.

2.3 The challenge of security in future networks

In additional to resilience, security is an important factor of the design of next generation systems. In particular, the increased number of connected devices anticipated for future networks poses an certain threats on security, in addition to

threats already existing in LTE. Moreover, such threats become even more important in mission critical applications, which are expected to play a vital role in the 5G ecosystem. In this regard, advanced security mechanisms need to be deployed, aiming at preventing and, if this is not possible, minimizing the effects of unexpected events originated deliberately by a human. Such man-made network disruptions either compromise fundamental security properties e.g., integrity, confidentiality, availability in the network or entail other deliberate misuse of the network that can turn into a security threat with major consequences.

Whereas the baseline of the 5G network architecture has been set through different research and standardization organizations and activities, a detailed elaboration on the means for achieving resilience has not been conducted. In Section 5 we address this need for a more detailed view on 5G network resilience and provide first insight on the means for achieving the desired level of resilience in 5G networks.

3 RAN Reliability Approaches

Next generation RAN shall allow a higher access reliability level, which is targeted especially for URLLC use cases. From the perspective of the RAN protocol stack design, this is translated into new RAN functionalities that aim at minimizing the radio link outage probability. As discussed in Section 2.1, this requirement can be addressed by specially tailored multi-connectivity based solutions that involve data duplication across the radio links [5], [8, 15].

In the remainder of this section, we highlight the technical features of implementing data duplication in next generation networks. We first discuss the deployment characteristics of data duplication, seen as an extension of LTE's dual connectivity; then, we elaborate on the particular protocol features of its implementation.

3.1 Data Duplication in Heterogeneous Networks (HetNets)

A typical deployment scenario used for the dual-connectivity approach in the LTE standards to increase the throughput is the Heterogeneous Network (HetNet) approach [7], which is also anticipated to provide coverage for data duplication. With this approach, the User Equipment (UE) connects simultaneously to both a macro cell and a small cell, which usually operate in different frequency bands. It is also assumed that next generation networks will adopt a centralized architecture, where networks functions are split between two RAN units, namely the Central Unit (CU) and the Distributed Unit (DU) [16].

An illustration of the HetNet deployment in the centralized architecture[4] is provided in Fig. 1. As can be seen from Fig. 1, the coverage area of the small cell falls within that of the macro cell. Typically, the location of the small-cell base

[4] We adopt "Option 2" from the candidate function split options provided in [16] since it is the most suitable to the use of data duplication.

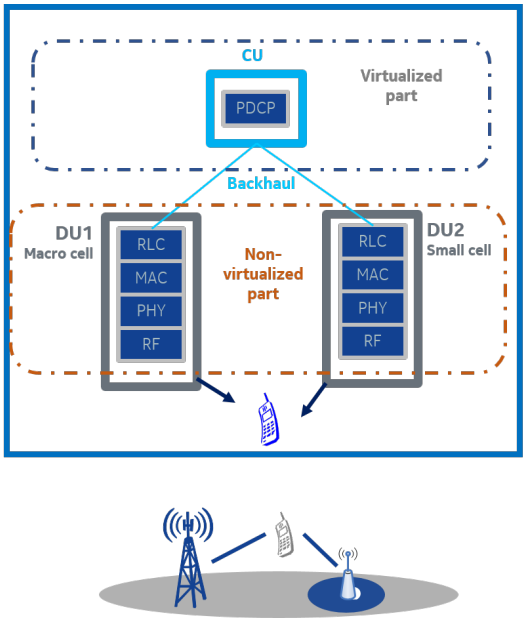

Fig. 1. HetNet deployment under the centralized architecture, where network functions are split between the CU and the DU.

station is carefully selected so as to fill in coverage gaps from the macro cell. On the basis of the centralized architecture [16], the lower layers of the protocol stack of both the macro- and the small cell take place at the corresponding DUs. Then, the integration of the signal flow to both links involved is carried out at the CU, which contains the higher RAN layers. It is noted that, in the context of NFV, the CU can run in a virtualized implementation, such that it represents part of the telco cloud itself. In such case, the orchestration of the CU resources follows the properties of the telco cloud management, as described in Sections 2 and 4.

3.2 RAN Protocol view of Data Duplication

The implementation of data duplication requires special coordination of the signal flow at the CU. In particular, the CU needs to take care that duplicate packets are delivered correctly to the UE, and that the overhead of the extra resources needed is minimized. In this regard, we highlight two major points where data duplication differs from existing approaches, from the perspective of the underlying technology.

– *Introduction of Packet Data Convergence Protocol (PDCP) acknowledgments.* In LTE standards, the packet acknowledgment feedback (ACK) sent from

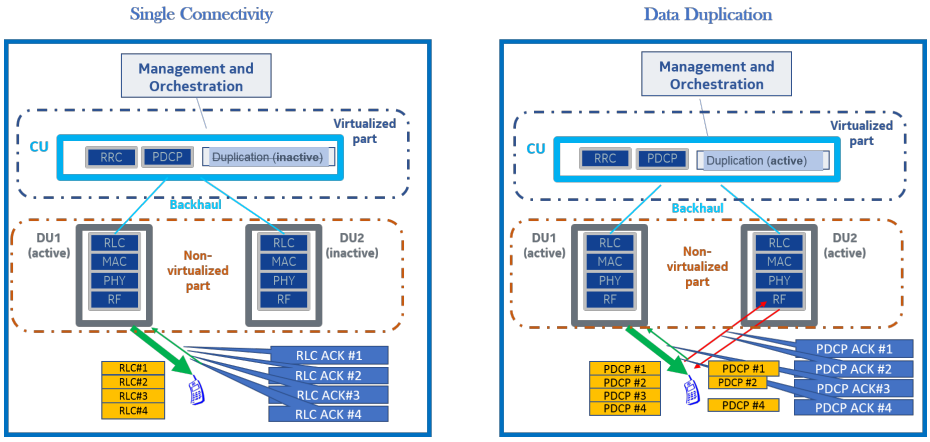

Fig. 2. Single connectivity versus data duplication, as seen via the prism of the new signaling involved within the RAN, as well as to and from the management and orchestration network layer.

the receiver to the transmitter in order to indicate whether the transmission was correctly received is carried out in two layers: At the Medium Access Control (MAC) layer by means of Hybrid Automatic Repeat Request (HARQ), and at the Radio Link Convergence (RLC) layer by means of outer Automatic Repeat Request (ARQ). On the contrary, given that the RLC layers of the two involved links do not process the exact same packet sequence (i.e., RLC packet number #2 for DU1 is not necessarily identical to RLC #2 for DU2), in the data duplication case feedback should be sent to the PDCP packet numbering instead. This process is expected to be introduced to 5G systems, and is illustrated in Fig. 2.

– *Management and Orchestration.* The activation of the data duplication process is followed by utilization of additional resources which require special administration and control. In this respect, the data duplication function that resides in the CU (c.f. Fig. 2) is orchestrated by a higher level entity which resides in the MANO layer. Besides the overall orchestration of the virtualized resources, this entity is responsible for deciding whether the data duplication function should be activated, and if so, what is the amount of virtualized resources allocated to it. The RAN Radio Resource Control (RRC) entity is then assigned the task of allocating radio resources between the two involved links, based on the needs of the underlying service.

4 Resilience in Telco clouds

In order to better address the resilience needs of particular network slice types, e.g. URLLC slices or industrial enterprise slice, the target of this work is in

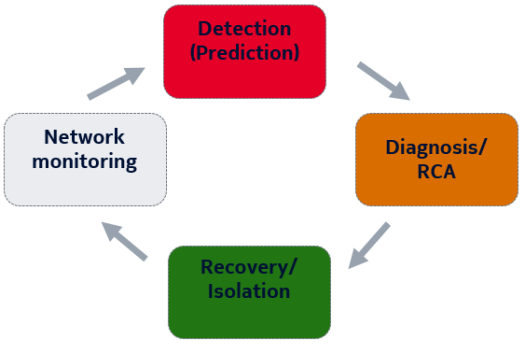

Fig. 3. Main processes and actions involved in network fault management.

enabling and integrating service-specific resilience and reliability aspects intrinsically in the 5G architecture. Rather than being an afterthought the service-specific resilience needs to be one of the main properties of the 5G network design.

In addition to RAN reliability which has been presented in Section 3, in this work we further elaborate on resilience in the telco cloud. In this context, we focus on two main aspects that need to be carefully considered, namely a) *Network fault management*, taking into account virtualized network functions, and b) Improving the resilience of individual network elements and functions, with emphasis on the *centralized network controller*.

4.1 Resilient Network Design and Network Fault Management

The main goal of network fault management is to enable the resilience to network failures by monitoring the network state and provide solution to the problems that cause the network performance degradation or failure. As a first step, the detection of changes, potential problems and anomalies in network behavior needs to be performed based on input from monitoring tools. Furthermore, the actual cause of the problem needs to be determined in order to perform the suitable recovery actions. The root-cause analysis enables the localization of the actual problem and consequently its isolation such that the propagation of fault effects and impact to the rest of the network can be minimized. Fig. 3 illustrates the main processes and actions involved in the fault management. Such fault management techniques need to be adapted and extended towards the 5G network slicing context. The fault management characteristics and parameters need to be adjusted to the actual service that is supported. This might include e.g., the service-aware design of triggers and thresholds for alarms creation, start of recovery actions, etc.

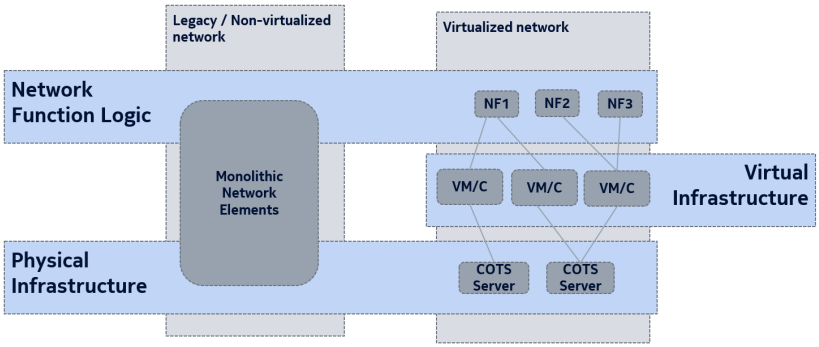

Fig. 4. Layered view of virtualized network: physical, virtual and network function logic layers.

The virtualization of traditional network elements broke up the tight coupling between hardware and software and introduced additional complexity in handling the faults of network functions. In virtualized networks three layers of deployment can be identified: network function/service logic, virtual infrastructure (e.g. virtual machines, containers) and physical infrastructure (e.g., COTS servers, compute and storage components) as illustrated in Fig. 4. In such an environment there might be different implementation and deployment options for network functions, i.e. there can be many to many relationships between layers of network functions logic, virtual infrastructure and physical infrastructure where the network function resides. Such layered implementation of network function requires enhanced fault management logic which takes into account the actual deployment and interrelations between the layers.

In general, the network fault should be handled at the layer where it occurs, ideally discovered before the major effects take place and/or propagate among different layers. As the faults can be related to different layers of network function deployment the correlation between fault occurring at different layers is essential for root cause analysis in virtualized networks. Furthermore, the correlation between the resource failures and the impact on the service performance and ultimately on the user satisfaction can create a baseline for better resource provisioning, prioritization and maintenance. However, the correlation is complex task due to many-to-many relations between infrastructure and network functions, service providers, deployments in multi-site and multi-domain data centers etc.

Despite the fact that fault management might be more complex in virtualized networks, the virtualization can be seen as a facilitator for network resilience through much easier and cost-effective redundancy implementation. As the network functions can be implemented on the commodity hardware the network functions can be more easily multiplied and moved across the network. Further-

more, adding redundancy in virtualized environment is more cost-effective as the infrastructure resources of redundant network functions can be more easily reused. Adding redundancy is especially important for critical network functions or network functions with higher importance/priority. For example, the SDN controllers which have central role in network control might be designed with more redundancy than other network functions, as the outage in network controller might have severe impact on overall network operation. Nevertheless, careful considerations on trade-offs in applying redundancy, e.g. in terms of overprovisioning and resource reservation, needs to be done in order to design efficient and resilient network.

4.2 Resilient and Scalable SDN Control FrameWork

The earliest SDN controller frameworks such as NOX, FOX, Floodlight, Ryu, Beacon considered the architecture to be centralized. Later, with the introduction ONOS and ODL, the control framework can also be deployed in distributed mode avoiding single point of failure and also improving performance, scalability and resilience [17]. The distributed architecture is a key feature of ONOS to support both scaling and fault-tolerance by instantiating and linking multiple instances in the cluster. In such approach, each instance can be an exclusive master for set of switches and failure of any instance leads to the selection of new master for those set of switches by the other instances. Raft consensus [18] algorithm is used for data synchronization and state management between distributed instances in ONOS. ODL has a similar clustering model build with Infinispan NoSQL data-store.

Although the distributed design is intended to improve the control layer resilience, it introduces challenges related to timing, consistency, synchronization and coordination for its adaptability in low latency and time constraint mobile network infrastructure such as telco cloud. In telco cloud, the VNFs corresponding to RAN and Core of particular network slice can be deployed across distributed cloud segments such as Front End Unit, Edge and Central Cloud located in different locations. Moreover, each slice can have different QoS requirements, for example the URLLC slice requires low latency through out its life cycle management starting from deployment to resource allocation. In such scenarios, the control framework needs to have different level of performance and behavior corresponding to different deployment scenarios and use cases.

The current implementation of both ONOS and ODL has its drawbacks by not considering the current and future load in the selection of master control instance for set of devices along with higher data synchronization time i.e., in milliseconds. In summary, as shown in Fig. 5 the successful realization of SDN for telco cloud requires a controller framework that is able to provide scalability and resilience, while satisfying the stringent performance requirement of each use cases. Such framework needs to be load aware and load predictive in selecting master controller instance for each set of devices.

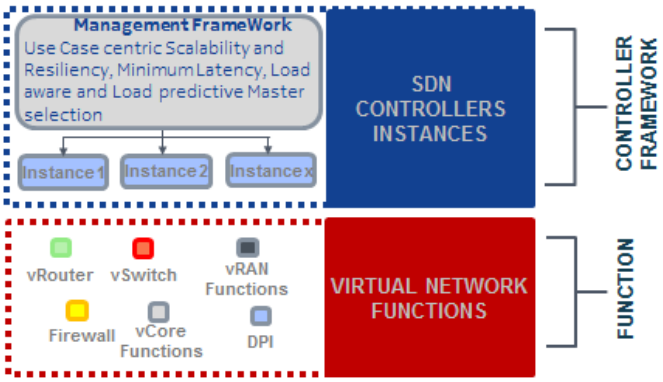

Fig. 5. Use Case and Load aware Scalable and Resilient Control Framework.

5 Implementing Security on top of Resilience

Security always comes at the extent of high resources consumption and impact on the normal operation of a system. Security mechanisms aim at protecting the system, e.g. by putting additional layers of hardware or software around the ones needed for just providing the functionalities the system was created for. This protection can be implemented in very efficient ways such that the impact on performance is minimized, but the impact per se cannot be avoided (e.g. performance decrease at peak times). In addition, depending on the criticality of the assets to protect, some countermeasures could cause a complete disruption of the network service operation, by completely isolating a portion of the network in order to prevent propagation of attacks or security flaws.

5.1 Security Threats: Prevention, Detection, and Reaction Methods

Any system exposed to the environment and the human interaction is subject to be a target of attacks. Depending on the degree of exposure and the nature of the elements that compose the system, some threats are more likely to occur than others. In the case of IT services based on 5G network infrastructures, there is a wide range of threats that both network tenants and telco operators must be prepared to deal with [19]. Since different technologies are involved, intertwined by multiple software and hardware infrastructure layers, the number of critical assets to protect increases. As a result, the vulnerabilities and weaknesses that can be exploited increase as well. With regard to privacy regulations, data breaches becomes *public enemy no. 1*, and dealing with such threat category makes it necessary to involve not only IT departments within an organization, but Human Resources and Legal Counseling (at least) as well, in order to overcome the so-called *human factor*.

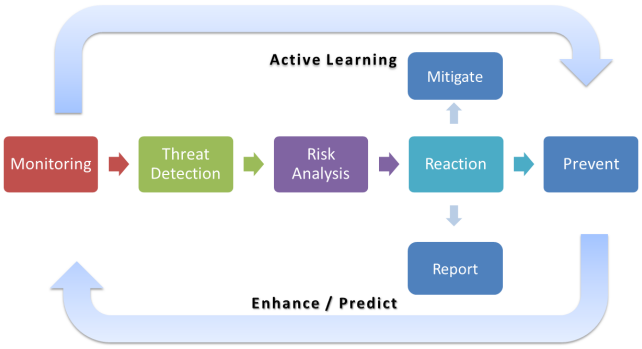

Fig. 6. Security Monitoring and Active Learning process

In addition to complexity, some security incidents may have a huge impact on the overall service operation. For instance, in *Man-in-the-Middle* attacks, a user session could be hijacked and used to insert rogue data into a mobile connection to maliciously exhaust network resources. Denial of Service (DoS) attacks are one of the top incident patterns responsible for causing disastrous business downtime, loss of data and application service, with an enormous economic impact, let alone the negative impact in the brand image [20].

An exemplary strategy With this in mind, it is important to implement a proper strategy which a) methodologically identifies the threats that may affect the system under analysis and b) applies the most appropriate mechanisms to address them. In this respect, Fig. 6 depicts an exemplary strategy, which comprises a combination of continuously monitoring of the landscape and active learning.

The importance of the strategy shown in Fig. 6 is explained as follows. On the one hand, looking for known security incident patterns allows for their detection as soon as they occur. It also allows taking the appropriate countermeasures with a minimum delay, minimizing the impact and avoiding propagation. On the other hand, by actively learning from the analysis of anomalous behavior, in contrast to the legitimate or normal behavior, allows to come up with new patterns or evolutions of known ones. Overall, this active learning process is a way to autonomously enhance the knowledge database, adapt to dynamically changing attack vectors and prevent from future security incidents.

Security monitoring Security monitoring is a conservative mechanism that relies on well proven security directives that permit detecting an (attempt of an) incident with high accuracy. However this is not sufficient nowadays. Advanced attackers put a great deal of efforts in evolving their malicious techniques fast,

circumventing any new patch or security obstacle deployed in the system, and making the recently updated detection rules outdated shortly after these are rolled-out. This is the case of Advanced Persistence Threats (APTs), which exemplify the advanced cyber threat due to increasing frequency, sophistication, importance and difficulty in countering in recent years [21].

Threat prevention Prevention mechanisms aim to overcome this problem since these permit learning from experience and enhance detection rules and reconfigure the security monitoring infrastructure to adapt to new scenarios. However, the main drawback of prevention mechanisms based on machine learning algorithms is the high rate of false positives. The reliability of the alarms raised by such tools is usually not high (especially when the training data is not extensive, rich or varied enough) and thus, the triggered countermeasures must be just preventive rather than reactive. As such, these signals should be used to prepare the system for the worst scenario, which can last for a predefined period of time or until the preventive system identifies that the threat is no longer probable to materialize.

Reaction to security threats The above methods are used to monitor, detect and possibly preventing attacks, which are mainly derived from the complex and dynamic nature of 5G infrastructures. Nonetheless, the major challenge remains to apply automated responses to cybersecurity incidents in a timely and automated manner. The network slicing concept calls for security architectures that are able to work autonomously within a slice, even in a disconnected way (e.g. at a cloud edge) [19]. Security Trust Zones (STZs) is a concept introduced in [22] to describe an architectural security solution for 5G networks that enhances the so-called AAA (Authorization, Authentication and Accounting) security functions at edge clouds.

The operation of STZs can be additionally equipped with the necessary mechanisms to detect security incidents, take decisions and apply custom countermeasures locally and fast. This *prescriptive security* is based on automating simple and specific threat analysis tasks with sophisticated machine learning and artificial intelligence [23]. In addition, STZs shall have the capabilities to share certain threat intelligence with other zones to avoid propagation and remain self-defending. STZs may cover multi-geographic areas and spread across different network slices, therefore, an inter-slice security management function would be required to govern and orchestrate the overall security response.

5.2 Compromise between Security and Resilience

Security and Resilience are two related concepts with mutual effect on one another. In particular, a large number of security-related threats can affect to different extent the resilience and functionality of the network fault management. For example, the DoS attack can result in unavailability of machines and network functions running on top of affected machines. Such effect will be detected

by the network fault management which will attempt to solve such issue using its restoration capabilities.

If redundant machines, network functions and links are available, the security threat might be mitigated using the existing redundancy. However, this may lead in lowering the current redundancy and consequently resilience level of the network. Depending on the actual service and agreed SLAs with the network tenant as well as the actual severity of the security threat, this might or might not be acceptable. In certain cases, lowering the resilience level for handling the threat might be unacceptable. This is true, for example, in situations where the security threat is assessed to be minor and does not jeopardize the normal network operation, whereas redundancy needs to be kept at the certain level due to risks of software and hardware problems. In such case a security might be compromised for achieving the required resilience/redundancy. On the other hand, as certain security threats might result in severe problems in functionality of individual network functions or the network as a whole, handling such threats might have highest priority, even at the cost of lowering the current redundancy/resilience level. In such case, the resilience might be compromised for security.

In general, measures need to be put in place to guarantee that a certain degree of resilience could pose new threats or attack paths that could be exploited with malicious purposes. Duplicating network resources to ensure availability of a service operation could give attackers another entry point to the system, if such resources are not properly secured. Nevertheless, the solution may not be as straightforward as simply duplicating the security as well, i.e. applying the same security mechanisms to the duplicated network branch. On the contrary, it requires a re-design of the security strategy of the system as a whole, which includes the duplicated network branches and any other plausible resilience mechanism.

6 Conclusions

In this paper the different aspects of network resilience in virtualized architectures were discussed. Specifically, this comprises the RAN reliability challenge of providing URLLC services over a radio link subject to fading, along with the challenge of providing service robustness in the telco cloud. Additionally, the main security challenges of future networks were put forward as an important and related topic. In this context, potential solutions to these challenges were presented. With respect to RAN reliability, multi-connectivity approaches involving data duplication were discussed as a means to reduce the probability of errors. In a telco cloud domain the resilience can be empowered by improved virtualization-aware and service-specific fault management as well as robust and scalable SDN control framework. We also showed that new security threats need enhancements in monitoring, prevention and reaction approaches, taking into account network slicing concept and increasing the level of automation.

An additional topic that was raised is the required compromise between security and resilience, which will mainly represent part of our future work. In addition, our future work plans include proposing a flexible 5G architecture that

describes how the concepts and solutions of the individual aspects can jointly form a resilient multi-service network.

Acknowledgment

This work has been performed in the framework of the H2020-ICT-2016-2 project 5G-MoNArch. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortiums view, but the consortium is not liable for any use that may be made of any of the information contained therein.

References

1. Nokia Networks, *Dynamic End-to-End Network Slicing for 5G*, White Paper, 2016.
2. P. Rost *et al.*, *Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks*, IEEE Communications Magazine, vol. 55, pp. 72-79, May 2017.
3. ETSI NFV, *Network Functions Virtualisation (NFV): Network Operator Perspectives on Industry Progress*, White Paper, 2014.
4. A. Ravanshid et al., *Multi-connectivity functional architectures in 5G*, 2016 IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur, 2016, pp. 187-192.
5. G P Koudouridis, P Soldati and G Karlsson, *Multiple Connectivity and Spectrum Access Utilisation in Heterogeneous Small Cell Networks*, International Journal of Wireless Infor-mation Networks, March 2016, Volume 23.
6. 3GPP TR 36.808, *Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Carrier Aggregation; Base Station (BS) radio transmission and reception (Release 10)*, Jul, 2013
7. 3GPP TR 36.842, *Study on Small Cell Enhancements for E-UTRA and E-UTRAN Higher layer aspects (Release 12)*, Sep, 2014
8. D. S. Michalopoulos, I. Viering and L. Du, *User-plane multi-connectivity aspects in 5G* ,23rd International Conference on Telecommunications, ICT 2016, Thessaloniki, Greece
9. A. Gopalasingham, L. Roullet, N. Trabelsi, C. S. Chen, A. Hebbar, and E. Bizouarn, *Generalized Software Defined Network Platform for Radio Access Networks*, IEEE Consumer Communications and Networking Conference (CCNC), Jan 2016, Las Vegas, United States. 2016.
10. S. Hämäläinen, H. Sanneck, C. Sartori, *LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency*, John Wiley and Sons, Dec. 2011.
11. S. Novaczki, *An Intelligent Anomaly Detection and Diagnosis Assistant for Mobile Network Operators*, 9th International Conference on the Design of Reliable Communication Networks (DRCN), Budapest, Hungary, June 2013
12. S. Novaczki, P. Szilagyi, *An Improved Anomaly Detection and Diagnosis Framework for Mobile Network Operators*, demo presented at the Second International Workshop on Self-Organizing Networks, Paris, 2012.
13. M. Miyazawa, M. Hayashi, R Standler, *vNMF: Distributed Fault Detection using Clustering Approach for Network Function Virtualization*, IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, Canada, 2015

14. F. Z. Youusaf et al, *Network slicing with flexible mobility and QoS/QoE support for 5G Networks*, IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 2017
15. H. Martikainen, I. Viering, A. Lobinger, B. Wegmann, *Mobility and Reliability in LTE-5G Dual Connectivity Scenarios*, IEEE Vehicular Technology Confernce (VTC) Fall 2017, Toronto, Canada
16. 3GPP TR 38.801, *Technical Specification Group Radio Access Network; Study on new radio access technology: Radio access architecture and interfaces (Release 14)*, Mar, 2017
17. S. H. Sandra, *Design and deployment of secure, robust, and resilient SDN Controllers*, Network Softwarization (NetSoft), 2015 1st IEEE Conference on. IEEE, 2015.
18. D. Ongaro and J. Ousterhout, *In search of an understandable consensus algorithm*, In Proceedings of the 2014 USENIX conference on USENIX Annual Technical Conference (USENIX ATC'14), USENIX Association, Berkeley, CA, USA, 305-320.
19. D. S. Michalopoulos, M. Doll, V. Sciancalepore, D. Bega, P. Schneider, and P. Rost, *Network Slicing via Flexible Function Decomposition and Flexible Network Design*,IEEE Personal, Indoor, and Mobile Radio Communications Conference (PIMRC), Workshop on New Radio Technologies, Oct 2017 .
20. Verizon Threat Research Advisory Center, *Data Breach Digest. Perspective is Reality*,Verizon Cybercrime Case Studies,Available online: http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/ 2017.
21. ENISA, *ENISA Threat Landscape Report 2016*,https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, February 2017 .
22. B. Han, S. Wongy, C. Mannweiler, M. Dohler, H. D. Schotten, *Security Trust Zone in 5G Networks*,24th International Conference on Telecommunications (ICT), May 2017 .
23. A. Grigory et al., *Digital Vision for Cybersecurity*,Atos Whitepaper,Available online: https://atos.net/content/dam/uk/white-paper/digital-vision-cyber-security-opinion-paper-new.pdf, September 2017 .