Telco Cloud Resilience: Synergies Between Fault and Security Management

Borislava Gajic*, Ruben Trapero†, and Diomidis S. Michalopoulos*
*Nokia Bell Labs, Munich, Germany. Email {firstname.lastname}@nokia-bell-labs.com
†Atos Research and Innovation, Madrid, Spain. Email: {ruben.trapero}@atos.net

***Abstract*—This work capitalizes on the concept of network function virtualization at the telco cloud, and presents a joint study between fault management and security management. Specifically, the commonalities of fault and security management are put forward, along with a resource allocation study in common slice deployments. In this regard, a security threat analysis is presented, which sheds light onto the impact of security threats on network fault management. The interdependence between security and fault management is highlighted via three use cases, where distinct levels of resource trade-offs are identified. Along with such use cases, the paper provides also an overview of the resulting resource allocation process, where the requirements of the corresponding slice are analyzed towards an overall efficient resource usage.**

I. Introduction

Unlike their predecessors, 5G networks are associated with an increased level of resilience. This stems from the stringent requirements of certain 5G use cases, particularly those related with industrial applications, which put forward the need for a seemingly faultless operation of the network [1], [2]. Moreover, this trend towards error-free networks continues even to next generations (namely beyond 5G networks), where the first discussions on such systems put resilience and reliability as key network elements (see, e.g., [3], [4]).

Resilience and Network Function Virtualization

An aspect which is particularly relevant with the concept of resilience in 5G and beyond systems is that of network function virtualization. This implies that certain network functions will not be implemented in the traditional, hardware form, but rather executed in a virtualized form in so-called telco clouds. As a result, the overall resilience of the network operation will to a large extent depend on the reliable operation of the telco clouds. In other words, achieving high levels of network resilience requires a robust telco cloud, in the sense that network faults within the telco cloud are minimized.

In this regard, fault management techniques have been proposed in the literature aiming at mitigating the effect of network faults at the telco cloud [5], [6], [7]. In principle, telco cloud fault management involves monitoring the network performance and posing certain acts to identified network degradation, thereby minimizing the impact of faults to network operation. Besides network fault management, security management is another critical aspect of the uninterrupted operation of the telco cloud. Security management is responsible for detection, reaction, and prevention from security attacks originating from malicious users of the network.

In legacy networks, the two domains (security and fault management) are usually handled separately. The emergence of 5G networks, however, broke up the monolithic implementation of network elements and introduced virtualization concepts in the implementation of network elements. This enabled more flexibility, along with a more cost effective mitigation from both network faults and security attacks. As virtualized resources are used by both domains, the need for a joint consideration became evident.

Contribution and Structure

This paper introduces the joint consideration of network fault and security management at the telco cloud. In this respect, the main aspects of a common resource allocation process in virtualized environments are highlighted. The aim of this study is to provide insight on the impact such domains to one another, along with potential resource trade-offs.

The commonalities between fault and security management are provided in Section II, highlighting the motivation for their joint study. Section III discusses network design considerations with respect to a network slicing approach, followed by Section IV which elaborates on concrete use case examples of joint security and fault management implementations. Section V sheds light onto the resource allocation aspects associated with the inter- and intra-slice resource management. Section VI provides the final concluding remarks.

II. Commonalities of Fault and Security Management in 5G Networks

In mobile networks the security and fault management entities are focusing on network problems which can have different root causes. However, the resulting effects on the network functionality might be common, e.g. unavailability of a certain network entities or even an entire service.

A. Common Root Causes

In many cases, a security threat might lead into problems in network functionality that will be detected by the fault management in addition to the security management. That is, a single threat (root cause) affects both domains of security and fault management. A typical example is the case of denial of service (DoS), which besides the typical security threat it can result in unusual patterns that will be detected at fault

management as a network anomaly. Further commonalities between security and fault management can be seen in the anomaly detection procedures which in both cases generally rely on monitoring of current network performance and comparing such inputs with pre-defined normal states, i.e. profiles of the network in order to identify any anomaly in network operation.

B. Common Mitigation Actions

Common approaches can be applied for mitigation for identified network problems, e.g. network function reconfiguration, and relying on existence of virtual replicas of affected network functions which is of particular interest in our joint security and fault management study on virtual resource optimization. Such virtual replicas are used for temporarily or permanently transferring the functionality of the affected network function to another network function. In order to enable such mitigation approach some level of network over-provisioning/redundancy needs to be supported by network planning. Over-provisioned network functions can take over the functionality of network functions affected by either security attacks or network faults in the case of unexpected events. However, applying the over-provisioning is associated with increased costs in the network deployment as well as operational complexity.

C. Network Function Virtualization and Network Slicing

Virtualization of network functions enables more efficient realization of over-provisioning as network functions might be deployed on less expensive underlying infrastructure and more easily be replicated or migrated. However, even with applying the virtualization a certain cost needs to be accounted when deploying redundant network functions. Thus, utilizing virtualization in order to enable redundancy in the network needs to be carefully implemented in order to enable efficient utilization of underlying resources and minimize resource costs. In other words, the over-provisioned resources need to be shared and re-used as much as possible. Thus, the commonalities between security and fault management can be exploited for optimization of resource usage.

Furthermore, the concept of network slicing envisions existence of multiple logical networks that are sharing a common infrastructure, thus the resources that can be used to handle security and network fault issues need to be shared among network slices. This fact emphasizes further the need for joint security and fault management considerations for efficient resource utilization and fulfillment of reliability requirements. Different network slices might have completely different reliability requirements that may lead to different levels of security and fault resilience. In addition, the actual usage of available shared resources for security or fault management purposes needs to be in line with according security/resilience slice requirements of a slice, as well as with the overall SLAs agreed with the tenants.

III. Cross-Slice and Cross-Domain Considerations

The aforementioned commonalities between security and fault management can be a valuable input in resource optimization process. A paradigm of such process is included in the framework of the EU-funded project 5G-MoNArch [8], [9]. This includes deriving suitable decisions on resource allocation during the slice preparation phase as well as during the run-time of the network slice.

A. The X-Slice and X-Domain Network Entities

In view of the above, the entities cross-domain and cross-slice security and resilience management, referred to as x-domain S&R and x-slice S&R, respectively, have been identified in [8] and [9]. Such entities perform the joint security and fault management considerations and derive the resource allocation and re-allocation decisions. Such decisions may have cross-domain/intra-slice scope as they apply within a single network slice. Furthermore, the resource allocation and re-allocation decisions may have the cross-slice scope and apply to set of network slices.

In some cases the same common resources can be used for handling events from security and fault management even across different slices, e.g. when the root cause of the event is the same. On the other hand, in order to guarantee slice-specific required level of robustness against security threats, certain amount of available over-provisioned resources might need to be foreseen/anticipated for handling the security threats within a given slice. The same principle applies for network fault problems and their recovery within a particular slice. However, the amount of over-provisioned resources needs to be minimized, and carefully provisioned based on a specific use case, e.g., slice requirements, Service Level Agreements (SLAs), amount of available resources, network state and likelihood for network problems, etc. The x-domain and x-slice S&R Management entities take into account the aforementioned constraints and anticipates the amount of over-provisioned resources (within a single slice and across different slices) to be used for recovery from security threats and network faults.

B. Security Threat Analysis - Impact on Network Resilience

Studying the impact of security threats on network resilience involves additional aspects to consider, namely their detection and mitigation. 5G networks add an additional level of complexity when dealing with security protection mechanisms, specially because the number and type of devices and services provided over the same infrastructure multiplies. Threat models are typically used to identify and evaluate potential security threats. In general, threat modelling for critical infrastructures like 5G networks are complex and typically always incomplete. There is no guarantee of being protected against 100% of the potential security threats. However, a protection on the basics is always required, which guarantee the proper management of the most common security threats.

TABLE I: Security threats analysis: detection, mitigations and resilience

Attack	Details	Likelihood in 5G infrastructures
Unusual activity	**Description**: Generic category including anomalous activities such as many login attempts **Detection**: In Linux based machines Linux Pluggable Authentication Modules (PAM) can report authentication attempts. HSM based devices can also report about unauthorized activities. **Mitigation**: Block requests from certain sources after n unsuccessful attempts.	High: being exposed to public networks, many devices are exposed to this type of attacks (traffic lights, cell phones, environmental sensors).
Denial of Service (DoS)	**Description**: Flood devices with packages, exhausting them and affecting their normal operation, resulting in lower performance or decreased availability. **Detection**: NIDS sensors can detect flood attacks by analyzing network traffic. **Mitigation**: Different possibilities: (1) Create firewall rules to redirect malicious traffic. (2) Instantiate virtual replica of attacked infrastructure to redirect and isolate attack.	High: DoS are common attacks in all domains, and very likely affecting 5G infrastructure as well.
Slow Distributed DoS	**Description**: Send small packages spaced in time, occupying connections slots and not releasing them, and blocking the attacked device that is not able to open additional connections. **Detection**: logging requests and checking request headers tags and timeout values. **Mitigation**: If vulnerable to these attacks, a simple modification to the server configuration helps to mitigate this attack.	Medium: Although, in principle, SlowDoS attacks have the same effect than DoS attacks, this type of attacks are less probable in infrastructure with high capacity in terms of resources. However, still mobile phone and personal devices with limited resources (e.g., IoT devices) can be exposed to this attack.
DoS in wireless spectrum	**Description**: Alter wireless spectrum provoking interference in certain frequencies (e.g., jamming attacks) **Detection**: Specific antijamming hardware devices are required to detect these incidents **Mitigation**: Change devices to connect through different frequencies. Difficult to react as long as the physical source of the attack is not located. Current research tries to react to these attacks by reconstructing the jammer signal to mitigate the interference.	High: Similar to DoS, these types of attacks are targeting wireless devices. Considering that most of the devices deployed at a 5G infrastructure are using the wireless spectrum (such as hand-held devices) the exposition to this type of attacks is high.
Privilege escalation	**Description**: Gain privileged permissions by users not entitled to get them. **Detection**: FIM File Integrity Monitoring can be used to detect system changes. HIDS - Host-based Intrusion Detection Systems (e.g. OSSEC) can monitor users activities within a host. **Mitigation**: Change file permissions and user privileges.	Low: It is expected for a 5G infrastructures to have a robust configuration of permissions and privileges. It is unlikely that outsiders are capable of exploiting this threat. Insider attacks with privileges would be capable of exploiting it, although, in general, insider attacks have a low probability to happen.
Botnets	**Description**: Infected machines that perform attacks under the control of a master **Detection**: IDS to identify unauthorized machines. **Mitigation**: Block unsolicited inbound traffic at firewalls.	Low: Similar to privilege escalation, this threat is more probable by insiders rather than outsiders. Therefore, it remains with low probability to happen.
Service Discovery	**Description**: Attempt to discover running services using port scanning and ARP requests **Detection**: NIDS sensors detect network scanning by analyzing network traffic **Mitigation**: In principle it is not possible to mitigate these incidents. However, the are two possibilities: (1) Scanning from outside. Scans can be mitigated by closing access to any port (2) Scanning from inside. Not possible to be detected. However, MAC filtering can be used to allow to access to the network just to authorized MAC addresses.	High: Service discovery by exploiting port scanning is very common in all domains, being very often the first action that an attacker performs prior to a more sophisticated attack.
Data and device tampering	**Description**: Device manipulation to modify, either physically (e.g., device destruction) or logically (e.g., upload and deploy unauthorized applications) **Detection**: Once gained access to the system the detection of data manipulation is difficult. Data tampering can be detected using forensic analysis methodologies, which can provide with an estimation of an attack with a certain probability (e.g., detecting installation of new applications out of scheduled maintenance time frames). To this end, NIDS detectors can alert about installation of software in certain machines, such as Linux based machines that use synaptic repositories. **Mitigation**: Once gained access to upload and deploy applications to the server, the mitigation is difficult. Rather than mitigation, data tampering can be prevented by updating and patching potential vulnerabilities, checking and limit privileges for executing applications or installing new ones. Device tampering can just be mitigated with physical sensors (e.g., turning off device when the manipulation is detected)	High: Considering that many devices deployed in the seaport infrastructure are in public areas, the probability of manipulation is quite high.
Malware	**Description**: Infect devices with malware, e.g., insertion of infected USB devices **Detection**: Antivirus and antimalware detectors **Mitigation**: Detected malware should be automatically detected and removed by antivirus and antimalware tools. Devices that have been successfully infected must be isolated or even turned off till the threat has been controlled to prevent propagation.	High: In all 5G infrastructures there are elements that contains physical interfaces (such as USB). This include computers in control rooms, personal devices (computers, tablets, mobile phones), etc. Therefore, tt is very likely that, either deliberately or not, these devices are exposed to these malicious events

While it cannot be considered a comprehensive analysis of all the potential incidents threatening a 5G network, Table I and Table II provide with a good approximation about how to handle the most important ones. Table I summarizes the evaluation carried out for ten of the most important potential attacks against a 5G infrastructure. For every attack it is described how to detect it (such as the security probes required to detect it) and possible mitigation actions to react to every attack. Table II extends the analysis by adding the resources needed to enforce the mitigation and the impact of the mitigation in the infrastructure. Additionally the impact of such mitigation on the network resilience (i.e. impact on the network functionality which is commonly reflected through the network fault management operation) is also included.

IV. Security and Fault Management Use Case Examples

The analysis summarized in Table I and Table II represents the baseline for joint security and fault management considerations in virtual resource optimization. In a nutshell, in order

TABLE II: Security threats analysis: Mitigation and resilience aspects

Attack	Resources required to mitigate	Impact when Mitigating	Impact on network resilience (network fault management)
Unusual activity	Capability to remotely perform actions against devices (i.e., SDN/NFV capabilities such as OpenContrail) using protocols such as Netconf or openflow)	Low: Easy to deploy rules for blocking requests, with no real impact on the infrastructure. False positives might be considered when blocking requests	High: might cause a change in performance of affected network function, e.g. due to overload
DoS	Capability to remotely modify firewall rules or to instantiate virtual devices through NFV	Depending on the mitigation: (1) Firewall rules: Low. Simple, not affecting to the current infrastructure. (2) Virtual replica: Medium. Time to deploy virtual replica might take time. However, it allows for the isolation of the attack and further study and forensics	High: might cause a change in performance or even a failure of a certain network function or multiple network functions running on affected machine
Slow Distributed DoS	Capability to remotely change the configuration of the server.	Low: A simple modification and restart of the server is required.	High: might cause a change in performance of affected network function
DoS in wireless spectrum	Capability to remotely change the frequency that wireless devices uses to operate. However, considered that the spectrum might be not available this is quite difficult. In case of signal based mitigation it is required the capability of deploy and start the device that builds and emits the signal.	High: It might be required to modify the configuration of many devices, many of them might not be accessible or easily reconfigurable (for example very resource constrained ones).	High: might cause a change in performance of affected network function
Privilege escalation	Capability to remotely perform actions against devices (i.e., SDN/NFV capabilities such as OpenContrail).	Low: Simple modification of some system permissions would be required.	Low: privilege escalation per se should not impact the resilience as long as the malicious user (using the new privileges) does not deliberately cause the failure of network functions or hosts.
Botnets	Capability to remotely modify firewall rules.	Low: A simple modification of a firewall is required.	High: might impact the functionality of switch/router.
Service Discovery	Capability to remotely modify firewall rules	Medium: Although this type of incidents are in principle harmless (as this attack is just detecting services and not attacking them), it can be considered as Medium impact in case critical services are detected, discovering potential vulnerabilities and exploiting it	Medium: hacker might use learned vulnerabilities to deliberately cause failure of network function or host/infrastructure
Data and device tampering	Capability to remotely perform actions against devices (i.e., SDN/NFV capabilities to turn off devices or uninstall packages)	High: Given the difficulty to mitigate the impact is high as it might entail to roll back to the situation before the modification of the data (restoring backups), checking permissions and patching software or restoring physically the device.	High: deployment of new application may cause failure of network function or host/infrastructure
Malware	Capability to remotely perform actions against devices to install/configure/update anti malware protection.	Low, Medium: Depends on the detection. If the threat has not been detected by an antimalware the impact increases as it requires to isolate (disconnecting from network or turning off) affected devices.	High: might impact the functionality of network functions and infrastructure

to perform the resource optimization, the x-domain and x-slice S&R Management entities need to determine the need for over-provisioned virtual resources to be used for mitigation purposes. This should consider the expected network fault and security issues, as well as their inter-dependencies, both in terms of resource requirements as well as likelihood of concurrent appearance.

As described in Table I and Table II, different security attacks can imply different resource requirements for performing the mitigation. Furthermore, security attacks may have different impact on the fault management. For example, certain attacks such as malware, DoS, and tampering, can be concurrently identified by a network fault management, as they have impact on the network resilience functionality. In such situations, the common virtual replica may be used to mitigate occurred security and consequently fault management issues. Such inter-dependencies need to be considered so that common resources may be allocated for mitigation purposes. In some other cases, where there is no strong impact of a security attack on the network resilience, the resource allocation may need to be performed differently.

Consequently, from the resource optimization point of view it is of high importance to identify such use cases based on the inter-dependencies between security and network resilience, especially with respect to the resource requirements and event concurrency. Such use cases can be further mapped to the resource allocation and re-allocation policies within or across network slices. With this respect the following use cases can be identified (also illustrated in Fig. 1):

- *Use case 1:* No over-provisioned virtual resources are needed for fault and security mitigation, i.e. when the mitigation is done by re-configuration of available resources/NFs. For example this use case comprises the mitigation of security threats such as unusual activity by blocking the requests from certain sources after n attempts, or compensation of cell outage by reconfiguration of neighboring cells. *This use case is not relevant for joint security and Fault Management (FM) study on resource optimization as it does not have impact on virtual resources.*
- *Use case 2:*. Certain additional/over-provisioned virtual resources are needed for security mitigation of a NF, which do not correspond to having an exact/full replica of that

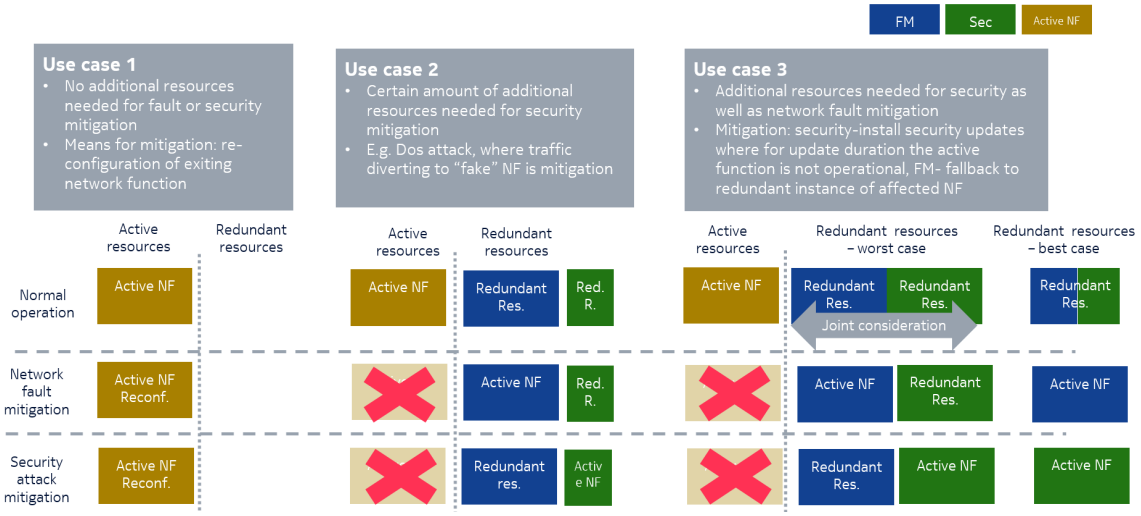

Fig. 1: Use cases considered by x-domain and x-slice S&R Management in virtual resource allocation and optimization

NF. E.g., for security attacks such as DoS certain amount of additional resources is needed for mitigation, however, this amount of resources does not correspond to having a full copy of the active NF instance, but it is usually used to create a fake copy of the active NF in order to divert the traffic towards it and make the attacker believe that the attack is still successful. *This amount of resources need to be taken into account for estimation on overall amount of required over-provisioned resources, thus it is relevant for joint security and FM (fault management) resource optimization.* Note: for handling the potentially concurrent network faults (identified by fault management) the amount of resources needed for mitigation are dependent on the actual network fault, e.g. may be done by re-configuration without resource requirements or fail-over using the NF replica. Fig. 1 shows the latter case. For simplicity reasons, in the following we assume that mitigation from the network faults always requires additional virtual resources as this is more relevant for our joint security and fault management study.

- *Use case 3:* Exact/full virtual replica of NF is needed in order to overcome the network fault or security issues. E.g. faults in VM running the NF may require standby VM that can take over the functionality of failing NF, or in the case of performing required security patches in case of malware, the active NF may need to be taken out of operation during certain period of time. During that time, the redundant NF needs to take over the operation. In this use case both domain require extensive amount of additional/over-provisioned virtual resources in order to perform the mitigation operation. This use case is of particular interest for joint security and fault management study due to the larger amount of resources required for mitigation, thus the need and potential for resource optimization. In this use case the x-domain and x-slice S&R Management need to determine the trade-offs in actual resource over-provisioning and the level of resilience to network faults and security problems that can be achieved, i.e. while minimizing the actual amount of over-provisioned resources the x-domain and x-slice S&R Management needs to assure the fulfillment of slice requirements with respect to resilience.

Use case 3 shows how different amount or over-provisioned resources may be allocated. In this use case resource pre-provisioning can be either 100% or 200% compared to active (currently used resources) for the purpose of mitigation from network fault and security problems. As provisioning of 200% more resources is very expensive, 100% seems as more suitable approach, especially if the temporal unavailability of redundant resources is acceptable from fault or security management point of view for a given network slice and network context. Furthermore, as some of security attacks may have high impact to resilience and will be concurrently identified by fault management, using a common resources for mitigation (accounting for 100% over-provisioning) may be more suitable approach. The exact amount of over-provisioned resources is computed by the x-domain and x-slice S&R Management based on slice requirements, network context, likelihood of problem appearance, inter-dependencies from resource and impact point of view, as well as the tolerance to fault and security problems which are defined through resilience requirements. This amount and allocation of resources can be changed during network slice runtime.

Based on the initial estimation on the likelihood of use cases 1-3, the x-domain and x-slice S&R Management can allocate certain amount of resources. Such resources considered 100% over-provisioning for a certain NF for use case 3, used for either network fault or security issues. If during the runtime of a slice the considered NF experiences considerably higher number and severity of security attacks, the x-domain S&R Management will exploit the following options. i) Re-

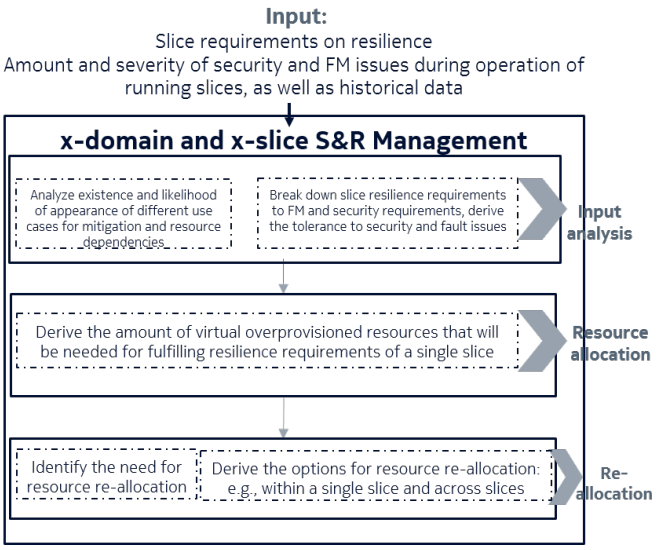

Fig. 2: x-domain and x-slice S&R Management: Actions performed for joint resource optimization

allocate a portion of redundant resources from other subnets of the same network slice, where the redundant resource were underutilized, i.e. the initial resource allocation was higher that the actual current need. ii) If such corrective action is not possible due to the current network state the x-domain S&R Management will request from x-slice S&R Management additional resources that are currently over-provisioned for other slices but may be unutilized. Based on the network states and agreed SLAs across slices the x-slice S&R Management may temporarily or permanently grant such requests.

V. On the Resource Allocation Process

In order to perform the resource allocation during the slice preparation phase, as well as resource re-allocation during the slice runtime phase, the actions needed to be performed by x-domain and x-slice S&R Management are described below and illustrated in Fig. 2.

Input analysis phase: The slices requirements along with agreed SLAs with the tenant regarding the slices resilience are analyzed. Then, the tolerance to security and network fault issues is derived, based on the received slice requirements. Furthermore, the existence and likelihood of appearance of different use cases for mitigation and resource dependencies is analyzed (c.f. Table II and use cases 1-3 as described above).

Resource allocation phase: Based on the input analysis step, the amount of virtual over-provisioned resources that will be needed for fulfilling requirements of a single slice (x-domain S&R Management) and multiple slices (x-slice S&R Management), is derived.

Resource re-allocation phase: The need for re-allocation of (over-provisioned) resources of different subnets and network slices during runtime of the slice (based on the input on the amount and severity of events coming from network monitoring) is detected. Then, the different possibilities for (runtime) re-allocation of over-provisioned resources among different subnets and network slices are identified. Furthermore, the most efficient option for (runtime) re-allocation of over-provisioned (currently idle) resources is chosen, given the current network state, utilization of underlying infrastructure, slice KPIs, and agreed policies with the tenant. For example, the re-allocation of redundant resources can be done within a single network slice or across different network slices.

Learning phase: Finally, the system learns from resource allocation and prioritization during the operation. Optionally, such information is provided to other network slice management functions for resource provisioning optimization.

VI. Conclusion

Security management and fault management are two domains which share common characteristics in terms of their impact to network performance, as well as in terms of their root causes and mitigation actions. The analysis provided in this paper identified the major elements of a joint study which lead to synergies towards an efficient resource management. In particular, depending on the considered use case, resource re-allocation issues were put forward, highlighting thus the potential of a joint fault and security management study to render telco cloud resilience effective, as well as cost efficient and thereby attractive to telco operators.

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 view of the consortium, but the consortium is not liable for any use that may be made of any of the information contained therein.

References

[1] IEEE Future Networks Technology Roadmap Working Group. IEEE 5G and beyond technology roadmap white paper, Oct 2017.

[2] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet of Things Journal*, pp. 1–1, 2018.

[3] Z. E. Ankarali, B. Pekz, and H. Arslan, "Flexible radio access beyond 5G: A future projection on waveform, numerology, and frame design principles," *IEEE Access*, vol. 5, pp. 18 295–18 309, 2017.

[4] D. Sahinel, C. Akpolat, M. A. Khan, F. Sivrikaya, and S. Albayrak, "Beyond 5G vision for iolite community," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 41–47, January 2017.

[5] A. Hilt et. al., "Availability prediction of telecommunication application servers deployed on cloud," *Periodica Polytechnica, Electrical Engineering*, vol. 60, no. 1, pp. 72–81, January 2016.

[6] T. Alexandrov and A. Dimov, "Software availability in the cloud," in *ACM Proceedings of the 14th International Conference on Computer Systems and Technologies*, 2013, pp. 193–200.

[7] D. S. Michalopoulos, B. Gajic, B. G.-N. Crespo, A. Gopalasingham, and J. Belschner, "Network resilience in virtualized architectures," *Interactive Mobile Communication, Technologies and Learning*, Feb 2018.

[8] H2020 ICT 2016 project 5G-MoNArch, "Deliverable D3.1: Initial resilience and security analysis," Jun 2018. [Online]. Available: http://5g-monarch.eu

[9] ——, "Deliverable D2.2: Initial overall architecture and concepts for enabling innovations," Jun 2018. [Online]. Available: http://5g-monarch.eu