Enhancing network slice security via Artificial Intelligence: challenges and solutions

Luis Suárez, David Espes, Philippe Le Parc, Frédéric Cuppens, Philippe Bertin, Cao-Thanh Phan

Enhancing network slice security via Artificial Intelligence: challenges and solutions

Luis Suárez, David Espes, Philippe Le Parc, Frédéric Cuppens, Philippe Bertin and Cao-Thanh Phan

IRT b<>com
1219 avenue Champs Blancs
35510 Cesson-Sévigné, France

Abstract. At this moment, the management of a network proposes new challenges for communication service providers (CSP). There is no human workforce capable to perform FCAPS (fault, configuration, accounting, performance and security) administration satisfying the exigent service level agreements to customers and keeping the same pace with respect to business. For 5G, one key challenge is the management of the security of network slices. The objective is to provide a review of Artificial Intelligence techniques applied to security in networking as well as a focus on the security challenges in network slicing, paying attention on how AI would help to solve the associated security issues for this enabling technology for 5G.

Keywords: Network slicing · automation · security management · artificial intelligence · 5G.

1 Introduction

Network operators have been challenged to provide more services and more capabilities with less budget for capacity and operation tasks. The service offer has widen as well as the number of devices and entities that interact to make this happen. Not only providing a service is challenging, but also the support of the complexity to manage the service, perform failure detection, troubleshooting, resolution and the management of the security. All of this, within the short timescales involved in the cycle from design and implementation to the service deployment. There is no operations team, network operation center, or security operation center in a CSP with the human workforce required to deal with all these problems. It is required to embrace schemes and paradigms that aid to perform these tasks in an automated way. Artificial Intelligence (AI), powered by machine learning techniques are envisioned to provide this features, in order to strengthen the management of the different components and features of the CSP network. It is of our interest to analyze the techniques that AI can provide to enhance the network security, specially regarding the future use cases for 5G that leverage on network slicing for its realization: Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communications (URLLC), and

Massive Machine Type Communications (mMTC). This paper is structured as follows: Section 2 will present an introduction to 5G, network slicing and the representative architectures of this enabling technology. Section 3 will present the network slicing security challenges. Section 4 will present principal approaches in the usage of AI to secure network slices. Section 5 will concentrate on the challenges of AI techniques when used into a network slicing architecture. The paper ends with future work and conclusions about the subject on Section 6.

2 5G and network slicing

Right now 5G is getting a great role in industry and academia, because of the envisioned use cases, versatility and key features that enhance current network features and performance. The 4G network that we use at this moment is good enough, but its foundational architecture makes it difficult to scale and evolve as needed. This is an obstacle now that we need to evolve from the current mobile broadband use case into other types of applications and connectivity schemes. This is the motivation for 5G, and at this moment technological tools are available to make it happen: software defined networking (SDN), network functions virtualization (NFV) and cloud computing. These concepts allow the function, networking and resource pooling abstraction to realize the network slicing concept.

2.1 The network slicing concept

The network slicing concept was conceived first by the next generation mobile networks (NGMN) alliance, who defines the network slice as an entity that wraps network functions and contributes to the realization of a communication service [30].

More concretely, it is a recursive entity, which provides the optimized and necessary resources to realize a complete service, meeting the desired requirements of a concrete use case scenario, which is powered by a business purpose.

Technically, it contains resources (compute, storage, connectivity), instantiated network functions (load balancing, routing, switching, firewall, monitoring systems, etc), along with configurations for its operational parameters (bandwidth, operating protocols, IP addressing, etc), and specification of its quality of service requirements in form of key performance indicators (maximum tolerable latency and delay, throughput, bandwidth threshold). These specifications are no different from the ones used in fixed networks, the difference is the new level of abstraction used and the "softwarized" nature of the constituent components of the networks.

5G architecture will use network slicing as one of its design principles spanning the radio access network (RAN), core network (CN) and operations, administration and management (OAM) [29]. This design strategy helps to improve: **(i)** network capabilities (data rate per user, end to end mobility, mobility); **(ii)** operational sustainability (automation to enhance self-organizing network (SON)

approach); and **(iii)** business agility (to support more services besides mobile broadband). These improvements help to realize the use cases envisioned for 5G, by allowing flexible functions and capabilities, supporting new value creation and incorporating security and privacy as a building principle from the design stage.

2.2 Architectures for network slicing

The most important architectural designs to implement the network slicing concept are from standard developing organizations (SDO). Three of the most important are the ones proposed by NGMN, the 3rd generation partnership project (3GPP) and the 5G infrastructure public private partnership (5G-PPP), as we will show in the following subsections.

NGMN: This SDO, besides providing the first definition of the network slicing concept, depicted a high level architecture, which is shown in Figure 1. On it, we

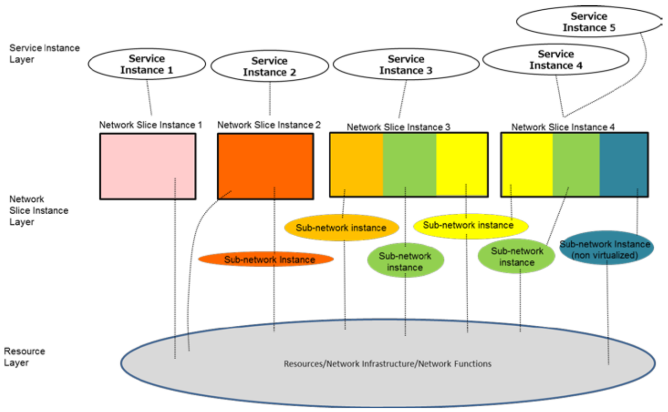

Fig. 1. Network slicing conceptual outline, according to NGMN [32].

can observe that it is composed of three layers: **(i)** service instance layer, which represents the services, denoted by a service instance; **(ii)** network slice instance layer, which provides network characteristics which are required by a service instance; and **(iii)** resource layer, which covers resources (physical or logical) on the network infrastructure. The service instance on the top is composed of network slice instances, which group together network functions and required resources to meet a characteristic of the desired service required by the customer.

3GPP 3GPP proposes an architecture to enable next generation systems to support network slicing, which is shown in Figure 2 [2] . Since their field of

expertise reside in the mobile network, their interest is to show the functional entities that are needed to connect a user equipment (UE) to a desired network slice. The components of the architecture are:

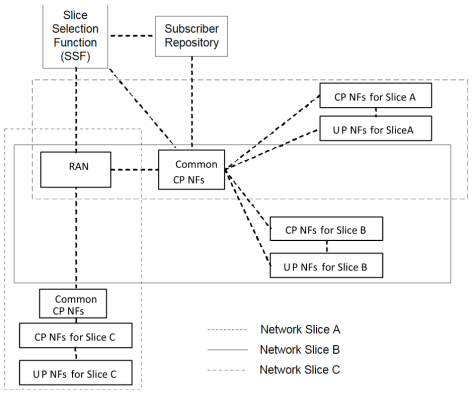

Fig. 2. Control plane (CP) architecture for network slicing according to 3GPP [2]

- Subscriber repository function: contains customer subscription information, UE usage type, service type and UE capabilities.
- Network functions (NFs), which can be:
  - Slice selection function (SSF): selects an appropriate slice for the UE based on the UE's subscription information.
  - Common CP NF (CCPNF): CP entry function, which at least includes the MM (Mobility Management) function, AU (authentication) function, and NAS Proxy function. The Common CP is shared parts among different slices.
  - Slice specific CPNF: the NFs which are located on the non-shared Slice parts.

In order to perform management and orchestration, 3GPP specifies management functions for the communication service, network slice and network slice subnets [4]. Their duties consider:

- Communication Service Management Function (CSMF): Acts as a translator from the communication service related requirements to network slice related requirements.
- Network Slice Management Function (NSMF): Performs management and orchestration of the network slice instance and derives network slice subnet requirements from network slice requirements.
- Network Slice Subnet Management Function (NSSMF): Responsible for management and orchestration of network slice subnet instance.

The document also specifies a high level plan to perform the life cycle management (LCM) of a network slice, considering: **(i)** preparation phase; **(ii)** commissioning; **(iii)** operation; and **(iv)** decommissioning. Details about this process and the implementation is out of the scope of 3GPP, so it is necessary to have an interaction with other framework, such as ETSI MANO [3].

5G-PPP They have a broad business view, aiming to propose use cases for industries and verticals to show the viability of 5G. For this purpose, they provide a 5G network architecture (shown in Figure 3) that uses network slicing as an important component to make the use cases a reality. Focusing on the

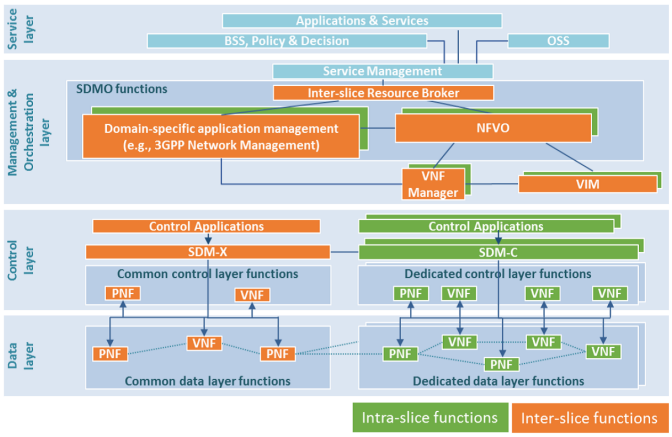

Fig. 3. Architecture functional layers for 5G, considering network slicing, according to [6].

network slicing concept, it is developed on the management and orchestration layer via a component called inter-slice resource broker. This entity would receive resource-facing service descriptions from the service management entity, which acts as a translator of the customer-facing service descriptions received from the service layer. According to the type of control of the service that is desired by the customer, the architecture can offer two different types of network slices: **(i)** provisioning of virtual infrastructures (VI), which resembles an infrastructure as a service (IaaS) approach; and **(ii)** enables the tenant to instantiate their own network services over the shared infrastructure. This architecture uses explicitly components from NFV architecture such as the network function virtualization orchestrator (NFVO), virtual network function manager (VNFM) and the virtual infrastructure manager (VIM) into their proposed management and orchestration layer. This built-in interaction eases the LCM of the network slices and its inner components.

2.3 Summary

From the presented architectures, the ones proposed by 3GPP and 5G-PPP are identified by their hands-on approach, either addressing the mobile network use case or addressing other usages for diverse verticals and stakeholders. Besides the service, they consider also management functions and interaction with the infrastructure over which the network slices are instantiated.

The network slicing implementation has challenges that span areas such as the radio access network (RAN), resource management, quality of service and security, which would be our focus. This will be the topic of the next section.

3 Security challenges in network slicing

Security spans all layers of a network architecture including the end user (human being or device). The inclusion of a new abstraction level into the design of a 5G service provides advantages but also poses risks and security issues that must be tackled.

Among the challenges, one of them refers to the detection of anomalous behavior in a network slice. It may be in terms of traffic, interactions or performance, which can give a clue that an attack is being developed. In order to do so, it is necessary to build a behavioral profile of a network slice, that is a difficult task due to the different services that can be deployed on it [13].

5G slices will host services with multiple actors and stakeholders interacting with each other, so we need schemes to **(i)** authenticate those entities to avoid impersonation attacks against a network slice instance and different network slice managers [13]; and **(ii)** provide proper accounting and non-repudiation of actions and decisions regarding a service [21].

Regarding the resources used for the network slices, it is expected that they have different security levels and policies since they could be managed and administered by different providers. The challenge is how to enforce network slice security in the case that a network function or slice is compromised when infrastructure from different providers is used [24]. Since resource sharing will become common in a CSP network, the challenge consist in providing an intelligent access and sharing of those assets, as suggested in [33].

Usually security is linked with the concept of isolation, which is a complex topic because it can be applied to different layers of a network architecture.

One important challenge refers to inter-slice isolation, that would help to: **(i)** guarantee that an attack on a slice will not affect other network slices (when certain control functions are shared [24]); **(ii)** guarantee that, when an end device uses several slices at the same time, it is not used as a bridge to move data from one slice to another [13]; and **(iii)** avoid the propagation of an attack when using shared functions by the "cascade effect" [8]. A related challenge refers to the intra-slice isolation, that seeks to control the behavior of the components inside the network slice. This control can be implemented by running a virtual manager function as part of the slice, tuned to manage the desired isolation property

[24]. Another interesting challenge regarding isolation refers to the formalization of its specification, in order to establish properly its parameters and possible configuration values. This way, not only interoperability will be achieved, but also the assurance that the isolation achieves the proposed objective [21].

As we presented in section 2 the network slicing architectures and the interaction between constituting components renders its management to a high complexity task. To deal with this issue, it is desirable to provide capabilities such as self-awareness, self-configuration, self-optimization, self-healing and self-protection. These are capabilities enabled by cognitive network management powered by machine learning (ML) techniques or artificial intelligence methods [35]. Security is one important part of the management categories. As networks get bigger, as they leverage on diverse technologies and as they span a large amount of use cases, the control of all security aspects becomes increasingly difficult. The challenge is to have coordinated monitoring between different domains and systems, with tools not only to detect and react to threats, but also to predict them [1].

A summary of the security problems and challenges regarding network slicing is shown in Table 1. Since these challenges are unresolved at this moment, it is the occasion to analyze how AI can help to provide a solution for them, as it will be presented in next section.

4 Opportunities for AI to secure network slices

Among the literature, the application of AI techniques is very diverse. Focusing on network environment, it spans the areas of self organizing networks (SON) [37], IP traffic classification [31], data collection techniques [25], optical network optimization [27], wireless network optimization [20], intrusion detection systems [9] [34] [12], security incident event managers [22], anomaly detection in protocols [11], cyber-crime detection and prevention [10] and network scan detection [12], among others.

Something common among the fields of security where these AI techniques are applied, is that the AI techniques perform a comparison between "signatures" of a experienced behavior (traffic pattern, file pattern, radio propagation) and the desired one. According to those differences, a solution is proposed in an intelligent way and executed in an automated fashion. Following this logic, there are AI applications that can be re-used (such as the ones used for traffic classification, cyber-crime and intrusion detection and prevention, management of incidents and scan detections) in order to solve the challenges in security for network slicing that are unattended at this moment.

For example, to control network slice behavior, we could have a traffic-performance baseline of a network slice depending on the service it provides. An IoT slice would show lower CPU usage and short bursts of traffic. If we notice that the behavior changes, the system could trigger an alert and search for abnormal traffic, recent authentication attempts to the system, source and destination of traffic and provide a remediation to that situation automatically.

Table 1. Summary of challenges related to security

Reference	Challenge	Summary
[13]	Control the slice	Create schemes to guarantee that slices behave properly among them, and that misuse of resources does not affect other slices.
[13]	Authenticate involved entities	Ensure that only authorized entities are allowed to perform actions over infrastructure and orchestrator.
[21]	Accounting and non-repudiation	Map relationships between stakeholders according to business models to assign responsibilities and non-repudiation of actions.
[24]	Share resources	Secure share of resources between network slices with different security levels and policies.
[24], [13]	Inter-slice isolation	An attack on a slice should not affect other slices. Techniques to isolate the network slices in case an UE needs access to several slices. Sharing of functions without compromising the security of network slices.
[21], [13]		
[8], [33]		
[24]	Intra-slice isolation	Monitor and enforce isolation parameters inside a slice.
[21]	Standardize isolation parameters	Establish common parameters, measurements and tuning to guarantee an isolation assurance level to customers.
[35], [34]	Manage slicing ecosystem	Security related data has "the 5V"[25]. Important tasks: monitoring, fault detection and remediation, under fast changes of resource utilization. Effective and in-time response is needed.
[1]	Monitor the security	Impossibility to manage all the variables and analytics to detect and react to a security incident, but most importantly, to predict it.

Regarding accounting and non-repudiation, we could have a map of relationships between entities in a network slice and the stakeholders that interact there. We could detect abnormal access to resources or the usage of abnormal protocols or functions, deviate traffic or block it according to some policy, without affecting service to the end user. This approach could be used also to detect and stop abuse of privileges.

Besides these approaches, there are several projects that leverage on AI to provide an integral solution to the network management and management of the security of network slices, in order to attend a concrete use case scenario in 5G.

One of the projects is SELFNET [5], which was created to "design and implement an intelligent management framework for 5G mobile networks"[18]. It addresses the limitations of the SON approach, which deals with static network resources, it is purely reactive, provides no prediction or prevention and does not consider its dynamics powered by network slicing and multi-tenancy environments. SELFNET proposes an architecture equipped with: **(i)** sensors

and monitors (to extract network data); **(ii)** actuators and an orchestrator (to execute corrective-preventive actions); **(iii)** a network intelligence entity (for diagnosis and tactical decision making). These elements constitute a control loop of the network intelligence, which is shown in Figure 4. The network intelligence

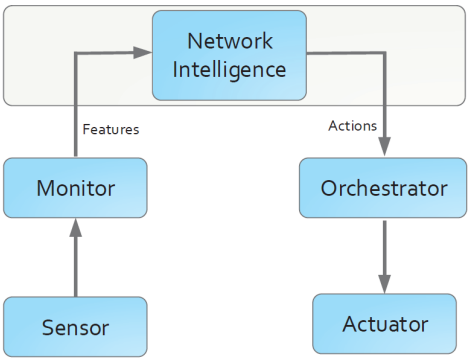

Fig. 4. Control loop of SELFNET's network intelligence [18]

enables the autonomic management of 5G networks. This allows a prompt reaction to detected problems and at the same time a proactive management of predicted problems. There are two enablers for the network intelligence loop: **(i)** Feature selection, used to utilize only the most important features from a data set in order to perform a more focused and fast analysis. The Relief-F algorithm is used in order to minimize the dimensionality of the data before building the learning machine. **(ii)** Classification, in order to find out to which category belongs a certain observation. Algorithms considered for this are Decision Tree (DT), Support Vector Machine (SVM) and Nearest Neighbor. This way, SELFNET achieves one of the proposed used cases regarding self protection against cyber-attacks, as shown in [26].

A second important project is called SliceNet [7] which, leveraging on network slicing, addresses challenges in management, control and orchestration of new services for verticals. Specifically, they seek to close existing gaps for the implementation of slicing, such as the end-to-end nature, lack of focus on the management plane (current approaches cover just the control plane), provide easy migration to verticals-industries to adopt 5G and the quality of experience (QoE) for the users. According to their vision, shown in Figure 5, the focus is centered on the cognitive network management and control for all slicing operations and services running over multiple domains. In order to achieve this objective, this cognitive network management block will use machine learning, not only to understand network behavior, but to modify the behavior to the desired state [7]. For SliceNet, cognition is used to learn the best actions to achieve the QoE objectives of the verticals. This learning is achieved by enhancing the monitor-

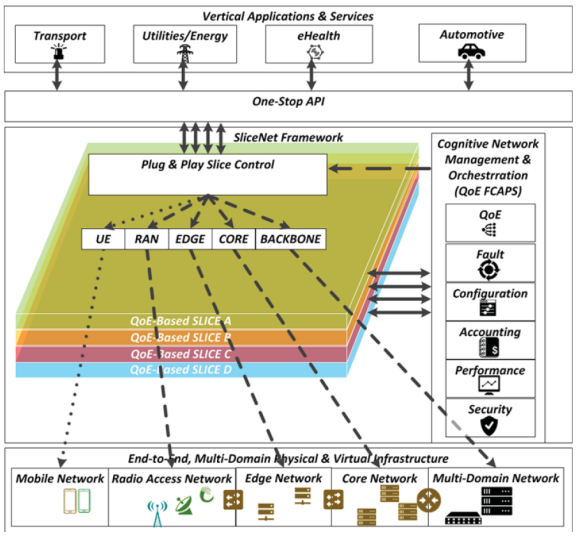

Fig. 5. SliceNet Vision [36]

analyze-plan-execute (MAPE) model with policy and knowledge, enhanced by ML control models such as Recurrent Neural Network (RNN). Multi-domain slicing is achieved thanks to collaboration between multiple MAPE cognitive loops, which not only exchanges data, but information and "wisdom". Important challenges addressed by this project, related to the security of network slices, consist in how to perform their security management. More concretely, the task is related to the instantiation of network functions for security monitoring, exposition of access rights and authentication credentials, detection of security threats and notification to upper layers about this incident.

One last project that is gaining inertia is the ETSI Industry Specification Group (ISG) on Experiential Networked Intelligence (ENI), whose objective is to improve "the operator experience, adding closed-loop artificial intelligence mechanisms based on context-aware, metadata-driven policies" [16]. The project specifies use cases that use this approach, being the most representative for our studies the ones that refer to **(i)** policy based network slicing for internet of things (IoT) security; and **(ii)** network slice management [14].

For the first use case, it is envisioned that there are going to be a high amount of connected devices, that leverage on network slices to access to certain services. Since the devices could perform diverse functions, and slices could have adaptability and expansible capabilities, the possibilities of attack increase over time. To tackle this scenario, ENI will use AI to indicate whether the traffic corresponds to a distributed denial of service (DDoS) attack and automatically isolates the devices object of the attack.

The second use case addresses the necessity to perform network resource allocation and the corresponding scaling of VNFs belonging to network slices.

To this end, the AI mechanisms will analyze collected data (traffic load, service behavior, constraints of the VNFs, usage of resources and their capabilities) in order to generate a placement policy. This is fed to the network slice management entity, specifying when, where and how to place a network slice instance along with the changes of resource reservation.

The concept that is envisioned for this project is shown in Figure 6. Cognition management is an important building block, which allows ENI to understand collected data taking into account the context where it was captured. Then, it can generate or change the knowledge, perform inference, understand the current situation, infer risks and prompt for actions to ensure accomplishment of the goals of a system. ETSI considers security and privacy as one of the service

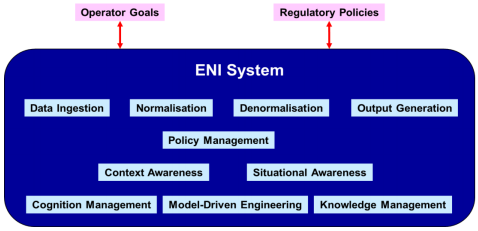

Fig. 6. ETSI ENI conceptual architecture[16]

and network requirements for this framework [15]. Among the requirements, besides detection, identification, isolation and removal of a corrupted device, it specifies the usage of AI to also detect abnormal traffic patterns that can lead to unavailability of services or security threats. ETSI is studying the ML techniques, in order to assess their complexity and how to apply them into real-time management scenarios.

The previously mentioned initiatives and projects show that the academia and SDOs are moving forward into adopting AI to solve security challenges for network slicing. Table 2 presents a summary of these findings. Nonetheless, incorporating AI has challenges that must be taken care of. Next section explores these challenges.

5 Challenges for the AI techniques

The application of AI techniques pose several challenges that could slow down their adoption into security management for network slicing:

– **Data collection:** Most of the research initiatives focus on the algorithms used to process the data, but do not tell which is the right data to capture, how often it has to be collected and how much of it is sufficient in order to have a representative result [19]. This challenge is important specially in the case when personally identifiable information (PII) is involved. This

Table 2. Relationship between network slice challenges, threats, current approach and the added value of the AI mechanisms to address the challenge.

Network slice challenge	**Related cyber-threat**	**Current approach**	**Possible AI mechanisms**	**Added value**
Control of the network slice	DoS; DDoS; resource exhaustion	Role based access; isolation of domains	Traffic detection via ML	Deployment of countermeasures before attack gets stronger; event forecasting
Authenticate involved entities	Spoofing of identity	AAA; mutual authentication; certificates; two factor authentication	Biometrics; learning of behavior pattern	Intelligent detection of impersonation via behavior analysis. Can prompt to revoke credentials if behavior deviates from usual pattern.
Accounting and non repudiation	No traceability and no responsibility for actions	Log systems and AAA to track actions; certificates to assure identity	Learning and correlation similar to SPAM detection	Detection of impersonation by behavior correlation; scalability of process in order to track and analyze actions from a high number of devices
Share resources	Information disclosure, due to usage of resources on different security levels	Encryption; mutual authentication; access control	Learn and enforce an encryption policy according to placement of NF	Modification of policies to secure slices, strict access control. Generate-update of placement policies.
Isolate network slices (Inter & intra slice)	Confidentiality and integrity of data	Traffic isolation; encryption; network segmentation; firewalls	Traffic detection and modeling via ML	Arbitration of traffic; triggered troubleshooting
Standardize isolation parameters	Obstacle to seamlessly manage the slice	Each use case and provider defines its own parameters	Mapping of requirements via artificial neural networks	Build proactive mapping from service specification to network configuration
Manage slice ecosystem	Lack of real-time response to threats	Reservation of high amounts of computing and storage capacity to process data as fast as possible and prompt a reactive response	Feature selection before applying ML	Less data to process and to feed to the model. Learning process is faster.
Monitor the security	Lack of threat prediction	Reactive approaches; delayed deployment of countermeasure	ML to predict security breaches	Minimization of attack window; ideally no downtime

type of data is important for use cases related to user traffic redistribution or intelligent placement of resources according to the service required by an user. The collection of the data must be done intelligently, guaranteeing its security, integrity and access only by authorized, trusted entities [9]

– **Active data collection:** The collection of security related data should be done in real-time in order to minimize the attack opportunity window before it is detected and mitigated. But using current collection techniques can pose a performance penalty on equipment and lead to add extra traffic over transmission links. It is necessary to create security-related data collection techniques that are less intensive over the network resources [9].

- **Model of acceptable behavior:** An attack can be identified by a deviation of the normal behavior of a service. Envisioned 5G networks and network slices leverage on heterogeneous resources to provide diverse types of services. By itself, there are several service types that have different usage patterns according to the customer. The corresponding training data becomes very large and in consequence, increasing the time it takes to train the model. The situation is worse when service behavior changes, which leads to perform a new training procedure to update the model [10].
- **Black box behavior:** Some CSP are resilient to adopt AI techniques because there is a sense of loosing control of the operation of the network. This is due to the fact that the internal structure is hidden and does not show the reasoning behind the taken decisions. It is necessary to understand better the internal structure of AI and its evolution, in order to increase the confidence on the system. This way, the operator intervention during the "human in-the-loop" stage becomes less demanding, achieving full automation.
- **Knowledge accuracy:** The data destined to train the AI model should be accurate, valid and trusted. Feeding the AI techniques with erroneous data leads to big problems in the behavior of a service and render it to a critical state[28]. We must have care with which entity or stakeholder is authorized to train the model, since an attacker can induce bias in the outcome of the algorithm. The learning process can be made more resilient to attacks via adversarial machine learning techniques [38].
- **Distributed and decentralized intelligence:** security-related data is captured from multiple locations in the network. Decisions are taken and enforced at different places. It is necessary to analyze the cost of the transfer of data from the edge to the core of the network, as well as the privacy and security implications of transporting such sensitive data. The best use of local or global data should be assessed and determine how to distribute learning to the nodes [17].

6 Conclusion

The use of network slices to construct the use cases envisioned for 5G networks provides great management and economic benefits for CSP. Besides the great advantages like the no need for dedicated physical networks and more options for resource management, mobility management, service provisioning and management, administration and orchestration, there are intrinsic consequences like complicated configurations, difficult management and how to guarantee the service level agreement with the customer under those stringent situations.

The envisioned 5G network powered by network slices has more options to deal with predefined intelligent problems, but lacks of the ability to interact with the environment in order to perform a better informed decision taking process. It also carries security risks that must be addressed properly in order to make the proposed use cases a business reality.

There are challenges that are difficult to solve because they involve a great amount of variables, of stakeholders and use cases that pose a challenge to collect

information, assign parameters, analyze it and prompt actions in an intelligent way.

These facts constitute an opportunity to use AI techniques, which can provide novel knowledge and help to solve the security issues in network slicing implementation for 5G networks. They provide the ability to learn form the environment, plan response actions and perform the proper configuration to solve issues [23]. Future works must consider building trust on the CSP side, by opening "the black box", giving the reasoning of the taken decisions and finding mechanisms to perform benchmarking between AI techniques. With this, AI will not be used for all network security problems, but select the most suitable technique according to the situation.

By solving the described challenges, the usage of AI techniques would become more commonplace, posing opportunities for their adoption in 5G networks.

References

1. 5g ppp white paper, phase 1, security landscape (2017)
2. 3GPP: Specification # 23.799 (2016)
3. 3GPP: Specification # 28.800 (2018)
4. 3GPP: Specification # 28.801 (2018)
5. 5G-PPP: SELFNET, Definition of the different APIs and Interfaces of the different components of the system (2016)
6. 5G-PPP: View on 5G Architecture (Version 2.0) (2017)
7. 5G-PPP: Slicenet D 2.2. Overall Architecture and Interfaces Definition (2018)
8. Arfaoui, G., Vilchez, J.M.S., Wary, J.P.: Security and Resilience in 5G: Current Challenges and Future Directions. In: 2017 IEEE Trustcom/BigDataSE/ICESS. pp. 1010–1015 (Aug 2017)
9. Buczak, A.L., Guven, E.: A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys Tutorials **18**(2), 1153–1176 (Secondquarter 2016)
10. Dilek, S., Çakır, H., Aydin, M.: Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications **6**(1), 21–39 (Jan 2015)
11. Ding, Q., Li, Z., Haeri, S., Trajković, L.: Application of Machine Learning Techniques to Detecting Anomalies in Communication Networks: Datasets and Feature Selection Algorithms. In: Cyber Threat Intelligence, pp. 47–70. Advances in Information Security, Springer, Cham (2018)
12. Dua, S.: Data Mining and Machine Learning in Cybersecurity (Apr 2011)
13. Dutta, A.: Security Challenges and Opportunities in SDN/NFV and 5G Networks (2017)
14. ETSI: ETSI GR ENI 001 V1.1.1 (2018-04) (2018)
15. ETSI: ETSI GS ENI 002 V1.1.1 (2018-04) (2018)
16. ETSI: ETSI ISG ENI, Creating an intelligent service management solution p. 55 (2018)
17. Fersman, E.: Artificial intelligence and machine learning in next-generation systems (2018)
18. Jiang, W., Strufe, M., Schotten, H.D.: Intelligent network management for 5G systems: The SELFNET approach. In: 2017 European Conference on Networks and Communications (EuCNC). pp. 1–5 (2017)

19. Kaloxylos, A.: Application of Data Mining in the 5G Network Architecture (2018)
20. Kibria, M.G., Nguyen, K., Villardi, G.P., Zhao, O., Ishizu, K., Kojima, F.: Big Data Analytics, Machine Learning, and Artificial Intelligence in Next-Generation Wireless Networks. IEEE Access **6**, 32328–32338 (2018)
21. Kotulski, Z., Nowak, T., Sepczuk, M., Tunia, M., Artych, R., Bocianiak, K., Osko, T., Wary, J.P.: On end-to-end approach for slice isolation in 5G networks. Fundamental challenges. In: 2017 Federated Conference on Computer Science and Information Systems (FedCSIS). pp. 783–792 (Sep 2017)
22. Lee, S., Shin, Y.: The Direction of Information Security Control Analysis Using Artificial Intelligence. In: Advances in Computer Science and Ubiquitous Computing, pp. 872–877. Lecture Notes in Electrical Engineering, Springer, Singapore (Dec 2017)
23. Li, R., Zhao, Z., Zhou, X., Ding, G., Chen, Y., Wang, Z., Zhang, H.: Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. IEEE Wireless Communications **24**(5), 175–183 (Oct 2017)
24. Li, X., Samaka, M., Chan, H.A., Bhamare, D., Gupta, L., Guo, C., Jain, R.: Network Slicing for 5G: Challenges and Opportunities. IEEE Internet Computing **21**(5), 20–27 (2017)
25. Lin, H., Yan, Z., Chen, Y., Zhang, L.: A Survey on Network Security-Related Data Collection Technologies. IEEE Access **6**, 18345–18365 (2018)
26. Manuel Gil Pérez, A.H.C.: Report and Prototype Implementation of the NFV and SDN Sensors and Actuators related to the Self-Protecting Use case (2017)
27. Mata, J., de Miguel, I., Durán, R.J., Merayo, N., Singh, S.K., Jukan, A., Chamania, M.: Artificial intelligence (AI) methods in optical networks: A comprehensive survey. Optical Switching and Networking **28**, 43–57 (Apr 2018)
28. Movahedi, Z., Ayari, M., Langar, R., Pujolle, G.: A Survey of Autonomic Network Architectures and Evaluation Criteria. IEEE Communications Surveys Tutorials **14**(2), 464–490 (Second 2012)
29. NGMN: 5G White Paper (2015)
30. NGMN: Paper on 5G End-to-end Architecture Framework (2017)
31. Nguyen, T.T.T., Armitage, G.: A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys Tutorials **10**(4), 56–76 (2008)
32. Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M.A., Samdanis, K., Sayadi, B.: Mobile network architecture evolution toward 5G. IEEE Communications Magazine **54**(5), 84–91 (May 2016)
33. Rost, P., Mannweiler, C., Michalopoulos, D.S., Sartori, C., Sciancalepore, V., Sastry, N., Holland, O., Tayade, S., Han, B., Bega, D., Aziz, D., Bakker, H.: Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks. IEEE Communications Magazine **55**(5), 72–79 (May 2017)
34. Sohail, S.: Automation of Network Management with Multidisciplinary Concepts. International Journal of Computer Technology and Applications **01** (Nov 2010)
35. Tudzarov, A., Gelev, S.: 5G and software network paradigm. In: 2018 23rd International Scientific-Professional Conference on Information Technology (IT). pp. 1–5 (Feb 2018)
36. Wang, Q., Alcaraz-Calero, e.a.: SliceNet: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks. In: 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). pp. 1–5 (2018)

37. Wang, X., Li, X., Leung, V.C.M.: Artificial Intelligence-Based Techniques for Emerging Heterogeneous Network: State of the Arts, Opportunities, and Challenges. IEEE Access **3**, 1379–1391 (2015)
38. Zorzi, M., Zanella, A., Testolin, A., Grazia, M.D.F.D., Zorzi, M.: Cognition-Based Networks: A New Perspective on Network Optimization Using Learning and Distributed Intelligence. IEEE Access **3**, 1512–1530 (2015)