IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 October 2023, accepted 6 November 2023, date of publication 14 November 2023,
date of current version 22 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3333209

RESEARCH ARTICLE

Automated Generation of 5G Fine-Grained Threat Models: A Systematic Approach

DANIELE GRANATA[1], MASSIMILIANO RAK[1], AND WISSAM MALLOULI[2]
[1]Department of Engineering, University of Campania Luigi Vanvitelli, 81031 Aversa, Italy
[2]Department of Research and Development, Montimage EURL, 75013 Paris, France

Corresponding author: Daniele Granata (daniele.granata@unicampania.it)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 952672 (SANCUS); and in part by the University of Campania Luigi Vanvitelli through the Program Valere 2019 and 2020, Project Semantic, Secure and Law Compliant e-Government Processes (SSCeGov) and Project Cleopatra, under Grant B68D19001880005.

ABSTRACT Fifth-generation technology standard for broadband cellular networks, 5G, delivers a significant increase in data speeds and capacity, as well as new capabilities such as higher energy efficiency, lower latency, and the ability to connect a large number of devices. These advances come with a new set of security challenges, as 5G networks will be more complex and integrated with critical infrastructure than previous generations. In order to correctly address such challenges there is the need for **fine-grained threat models**, that collect a set of well-detailed threats, each of them clearly addressing a system component, taking into account how components are connected and interact with each other, the specific technology and/or the protocols are involved. A fine-grained threat model can be used to support the definition of a penetration testing plan or to identify and verify the effectiveness of technical countermeasures. This paper extends an existing automated threat modelling methodology focusing on 5G architecture and defines a process to build in a systematic way the catalogue of threats on which the technique relies. In order to obtain such results, we extended our modelling technique, in order to model 5G architectures, defined a process to extend our methodology to address additional domains and applied the approach to a concrete case study, applying our technique to a common 5G open-source architecture proposed by our industrial partner. The main contribution of this paper can be summarized as follows: 1) technique to systematically produce an extension of our modelling technique and a threat catalogue for a specific Domain; 2) 5G systems threat catalogue; 3) 5G systems graph-based modelling technique. As an additional result, we validated our approach, applying our technique in a real context and involving industrial experts for the evaluation of the generated fine-grained threat model.

INDEX TERMS 5G, threats, threat catalogue, security, security assessment.

I. INTRODUCTION

5G has the potential to revolutionize the way of interacting with the world. It promises faster speeds, greater capacity, and lower latency compared to its predecessors. With 5G, a wide range of new applications and services increase, such as autonomous vehicles and smart cities. As a counter-benefit, as we move towards a more connected world, we must ensure the security of 5G networks and the data they transmit.

However, security is a very generic term, which includes different issues (e.g. the definition of security requirements, identification of security functionalities to include, identification of malicious behaviours, identification of vulnerabilities, ...) and many different practices, like threat modelling, countermeasure identification, vulnerability identification, and penetration testing. In this paper, we focus on threat modelling, which is defined as *a process used to identify, communicate, and understand threats and mitigations within the context of protecting something of value* [1]. It is a proactive approach to security that focuses on identifying, analyzing, and mitigating threats before they can be

The associate editor coordinating the review of this manuscript and approving it for publication was Prakasam Periasamy.

exploited. Through threat modelling, organizations can assess the potential risks and vulnerabilities posed by their systems and take the necessary steps to reduce them. This process helps organizations to understand their systems better and take measures to protect them from malicious attacks. Based on existing technologies, some threat modelling techniques can provide important support for identifying security issues and reducing costs. There are at least three approaches to threat modelling: attacker-centric, system-centric, and asset-centric. The first is based on the attackers, their specific goals, and how they are trying to achieve those goals. The second focuses on systems and the way they are designed and developed. The third is based on assets (i.e. components to be protected).

Recently, many threat modelling tools (MS threat modelling tool, SLA generator, ...) are being developed in order to help system designers to model the target systems and identify possible threats, a survey of such tools and approaches is available in [2]. Such tools enable *fine-grained* modelling of the target system and, accordingly, a more detailed description of the possible threats. It is worth noticing that such tools are less than ten years, and only recently there has been a broader adoption of such modelling techniques as an effect of the *security-by-design* best practice; in most of the cases, threat models were simple lists of high-level threats.

In order to distinguish the two different approaches to threat modeling we need to clarify the concepts involved and the associated terminology. Accordingly, a threat is a malicious behaviour (i.e. an action that broke confidentiality, integrity and/or availability requirements) obtained by a threat agent against a target system or a specific asset. We use the term **high-Level threat model** to identify a list of generic threats, i.e. when the malicious behaviour does not refer to specific technologies, protocols and/or system components. Conversely, a **fine-grained threat model**, collects a set of well-detailed threats, each of them clearly addressing a system component, distinguishing among different instances of the same software, taking into account how components are connected and interact with each other, the specific technology and/or protocols are involved. Examples of attacks implementing the threats are commonly available.

It is worth noticing that, a *fine-grained threat model*, can be used to support the definition of a penetration testing plan, like proposed in [3], or to identify and verify the effectiveness of technical countermeasures as presented in [4]. As a counter-benefit, there is a loss of generality of the models and a need for deep knowledge of the target system: the analyst needs to know in detail how the target system is configured. Moreover, a little change in a system implementation may affect the threat model and vary the impact and the behaviour of some of the threats. Defining and validating a *fine-grained threat model* is a complex and time-spending process.

Conversely, **high-level threat models** commonly refer to target system reference architectures or to simplified layering of the system architecture, in some cases, threats refer to the type of components involved. **High-level threat models** are typically static, predefined with respect to the target system to be designed and can be used for risk analysis at very early development stages, to identify security objectives and requirements (as happen in common criteria certification process.[1] However, a **high-level threat model**, is of little use when building a detailed penetration testing plan and/or in comparing different design choices.

Focusing on 5G networks, as outlined in section II, the topic is complex, due to the amount of different technologies and protocols involved. The analysis of the state of the art illustrates the availability of a multiplicity of **high-level threat models**, organized with respect to different layers and more or less detailed. However, there are no examples of *fine-grained threat models*(supporting both 5G components and protocols involved), the more common tools rarely support 5G-related assets (and, consequently, are not able to identify 5G-specific threats).

The main goal of this research work is to propose a technique able to generate in an (almost) automated way a *fine-grained threat model*, relying on a graph-based model of a 5G system. The modelling technique must be simple and flexible, enabling a description of the target system at the level of detail of interest (and according to the knowledge) of the analyst. The core idea relies on a **threat catalogue** that collects in a structured way the existing **high-level threat models** and can be used to instantiate specific and detailed *fine-grained threat model* putting together the high-level descriptions and the target system model.

Such an approach was tested in different contexts (cloud, IoT) [5], [6], [7] and enabled an automated risk analysis process [8] based on OWASP risk rating technique [9], in order to calculate the risk (i.e., a probability that a threat may happen) for each threat selected during the threat modelling phase. Risk values are taken into account in the countermeasures selection phase in order to prioritize the security control selection. However, in previous works, the catalogue was built in a non-systematic way and from practical experience during European projects.

This paper extends the existing threat modelling methodology focusing on 5G architecture and defines a process to build in a systematic way the catalogue of threats on which the technique relies. In order to obtain such results, we extended our modelling technique, in order to model 5G architectures, defined a process to extend our methodology to address additional domains and applied the approach to a concrete case study, applying our approach to a common 5G open-

[1]ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model.

source architecture proposed by the French MONTIMAGE company.

The main contribution of this paper can be summarized as follows:

- A technique to systematically produce an extension of our modeling technique and a **threat catalogue** for a specific Domain
- A reusable 5G systems threat catalogue
- A 5G systems graph-based modelling technique
- An example of 5G fine-grained threat model on a real case study

As an additional result, we validated our approach, applying our technique in a real context and involving industrial experts for the evaluation of the generated fine-grained threat model.

The remainder of the paper is organized as follows: next section II summarizes the existing related work and outlines the missing of *fine-grained threat models* for 5G systems and Section III outlines the threat catalogue data model and our technique for *fine-grained threat model* generation. Section IV introduce the methodology we adopt to extend our techniques to new technological domains. Section V introduces the 5G main components and protocols and our extension to the modelling technique. Section VI shows the systematic search approach and findings applied to 5G. Section VII describes the analysis of the threats resulting from the methodology. The extended technique has been applied on a real testbed, as described in section VIII. Finally, section IX summarizes our conclusions and future work.

II. RELATED WORK

The main goal of our paper is to produce *fine-grained threat models* for 5G systems, in an almost automated way. In this section, we will focus mainly on 5G threat models, while we invite the interested reader to check the paper [2] for a detailed analysis of threat modelling tools and the techniques adopted to generate this kind of threat model.

As anticipated, the analysis of the state of the art, outlined to us that in literature there are many examples of **high-level threat models** for 5G infrastructures, but there are no examples of *fine-grained threat models*. Moreover, we checked all the threat modeling tools reported in [2], finding that no one of them explicitly supports 5G components (at least at the moment of the paper submission).

Table 1 summarizes the papers that contain a **high-level threat models**, considering the year of publication, its typology (e.g. if it is a survey, review, white paper, etc), a brief description of the methodology used and the assets involved, and the number of references and collected threats. It is worth noticing that there is no standard and commonly accepted way to produce a threat model, as a consequence, some papers are scientific surveys very detailed, while other papers, instead simply collect threats in an unstructured way.

It must be noted that the following list of papers is a subset of the systematic Literature Review (SLR) we conducted to build up our threat catalogue, described in detail in the following section VI.

We selected for this comparison the papers that contain surveys summarizing clearly the evolution of the 5G security challenges. it is important to point out that the aim of our work is more specific: obtain the data needed to build a catalogue containing threats affecting 5G components.

The state-of-the-art analysis outlines that the possible approach can be organized in the categories described in the table 9. Some reviews or white papers propose surveys listing and describing threats affecting all (or a part of) 5G components. Also, ENISA 5G Threat Landscape has been included as *Similar works* as it provides a 5G threat taxonomy with 48 threats and maps all the threats to each 5G component. It is worth noting that ENISA detailed each threat with some additional information (i.e. threat detailed), but, according to the scope of our work, we consider the high-level description of each threat [10]. As ENISA, a small taxonomy of threats has been produced by Dutta et Al [13]. The work describes some threat categories (e.g. the ones that affect Confidentiality, Integrity, Control, etc.) and, for each category, proposes some threats using a specific description of the compromised 5G assets or interfaces. Unlike these ways of modelling threats, some other approaches focus on 5G layers. A layered analysis is provided by S.Sullivan et al. [14] that focused on threats and security issues compromising each ISO layer. They summarized threats and vulnerabilities organized by ISO layers. The choice of using ISO layers is due to the need of taking into account security issues by design and helping organizations focus their capital expenditure. In particular, they focused on specific layers (which most of the threats have been associated with): the physical layer. In fact, as even described in literature [11], *the physical layer between the base stations and users' device increased opportunities for attacks*. Some other authors [16] do not focus on the OSI layer, but organize 5G threats with architectural layers. For instance, some threats can affect the Service Layer, compromising, for example, the cloud server and store, or even the Core Network. Since 5G is a technology standard connecting devices (e.g. IoT), some threats can compromise Device and Edge Layers, but also the communication between devices and Edge servers (i.e. Radio Access Layer). A different layer-based approach is provided by Madi et al. [18] that took into account threats inside an NFV:

- intra-layer, if it instruments a unique layer and impacts an asset within the same layer
- inter-layer if it affects a specific layer and affects indirectly another layer.
- multi-administrative domain, if it spans multiple administrative domains.

According to the analysis made above, the layered approach is very heterogeneous since there are different ways of dividing and classifying layers, but in some cases, some threats related to each 5G component can be indirectly derived. Unlike the others, some surveys [15], [17] list

TABLE 1. Similar surveys.

Article	Year	Type	Analysis	References	Threats
[10]	2019	White Paper	The papers present a threat taxonomy related to 5G architecture.	-	48
[11]	2019	Short Survey	The short survey presents a description of physical threats related to 5G-IoT systems.	101	13
[12]	2016	Short Survey	The paper presents a description of the main threats and security requirements introduced in IoT middleware systems caused by 5G systems.	44	10
[13]	2020	Review	The papers present security challenges about 5G and a small threat taxonomy.	13	13
[14]	2021	Review	The article describes each layer and protocol involved in the 5G architecture (OSI model) and for each layer, they underline the vulnerabilities and threats.	138	32
[15]	2020	Survey	The survey describes the security issues for each domain(e.g. Network slicing, Access Network, DoS attacks) and also for the overall core network. The authors also focused on explaining the attacks on Virtual Network Functions, Virtual Machines, Orchestrators, and Hypervisor.	378	54
[16]	2022	Review	The authors list all the threats for each 5G layer: Device, RAN, Edge, Core, Service)	40	59
[17]	2021	Short Survey	The papers used the threats identified by Cloud Security Alliance (CSA) in 2016 for the 5G services. They evaluated the applicability of each threat to some stakeholders (Mobile operator, Tenant, and Subscriber)	109	10
[18]	2021	Short Survey	The authors provided a threat taxonomy that takes into account three different layers: intra-layer (threats at the same layer), inter-layer(threats between different layers), and multi-administrative domain. Also, a stakeholder analysis is carried out.	200	40

all the threats affecting 5G high-level assets (e.g. 5G Core, RAN, etc) or custom Domains (e.g. Network Slicing, Access Networks, each network function) without detailing specific 5G assets. Anyway, all the analyzed state-of-the-art literature describes some threats affecting 5G but does not directly specify detailed and complete information about the compromised assets and the 5G protocols that can lead to security issues. In some cases, the threat analysis is carried out (also) taking into account the compromised stakeholders [17], [18]. In this case, the papers identify all the stakeholders (who are interested in protecting the infrastructures) and each threat is associated not with the compromised asset, but with the potentially damaged part.

As anticipated, the literature analysis outlines that *no results at the state of the art offer a solution to dynamically produce threat models for custom 5G deployments*, as proposed in this paper, but they offer an interesting collection of possible threats that we used to set up our structured threat catalogue (described in detail in the following sections).

III. BACKGROUND: GENERATION OF FINE-GRAINED THREAT MODELS

The idea of generating *fine-grained threat models* from a graph-based model and a threat catalogue relies on some preliminary works [8], [19], [20], [21] that use some static, but well-known sources, like OWASP top threats and the most relevant scientific papers. A part of the catalogue was built in the context of the MUSA H2020 project. The main limit of the approaches proposed above was related to the difficulties in build, maintaining and validating the threat catalogue.

The paper [22] describes in detail the process for generation of the threat model generation. in the following, we briefly summarize the catalogue data model and the generation algorithm, in order to improve readability, but we invite the interested reader to find the details in the referred paper.

As a starting point, the technique relies on a high-level description of the target system architecture. The models we adopt rely on the Multipurpose Application Composition Model (MACM), proposed initially in [23] for Cloud applications, then adopted in many different contexts [2], [3], [7], [24]. MACM relies on a graph-based approach, representing the main assets (formally everything that has a value, technically any component in the system) as nodes of the graph and the edges outlining the relationships among the assets. MACM defines asset types (e.g. the type of nodes to be involved) and relationship types (e.g. the kind of relationship among assets) through labels and imposes limits with respect to the kind of relationship and assets that can be linked to each other. A detailed description of the mode will be given in section V, where we extend the model in order to support 5G assets.

The threat catalogue we adopt has a structure that is independent of the specific technology, described in 2: the **Behaviour** field contains a description of the high-level malicious behaviour while the **Asset Type** the name of the *class* of assets subject to that specific threats. It is worth noticing threats are also related to the protocols, that in our modeling technique are associated with relationships. Accordingly, the threat catalogue has a field to be used when a threat applies to a protocol: instead of the **Asset Type** field, the protocol will be reported in the **Protocol** field. Moreover, the MACM relationship type involved in the MACM must be reported and the *Role in the relationship*, i,e, if the threat compromises the source, the destination of the relationship (MACM is a directed graph) or both.

The threat modeling technique [22], [24] provides an algorithm to select the threats that compromise the software components and another algorithm used to select the threats that compromise the data. The algorithm requires a MACM as input and returns all the threats the components are subjected

TABLE 2. Threat catalogue: the schema of the threat table.

Threat Catalogue Field	Description
Threat	A synthetic high-level label of the behaviour
Asset Type	The asset typology to which the threat is subject
Relationship	Relation Type
Protocol	Protocol used in the communication
Role in Relationship	Role in communication
Behaviour	Detailed description of the threat
PreCondition	How much confidentiality, integrity and availability have to be compromised in order to perform the threat
PostCondition	How much the threat compromises the confidentiality, integrity and availability.
STRIDE	Stride Classification [27]
Compromised	Which assets the malicious behaviour compromises

to, by constructing the threat model in three consecutive steps. In the first step, for each component (i.e. the asset), the algorithm selects the malicious behaviours collected in the new threat catalogue, indexed by AssetType; in the second step, the algorithm selects all the threats that indirectly compromise the asset due to the nearby component; in the last step of the algorithm considers all the protocols specified by each *uses* relationship of the asset.

As anticipated, for a more detailed description of the fields and of the algorithm, we invite the interested reader to check the paper [22] for such details.

IV. MODEL AND THREAT CATALOGUE EXTENSION FOR SPECIFIC DOMAINS

The *fine-grained threat model* generation technique relies on our modeling technique and on the threat catalogue: both of them should be able to represent the assets and threats involved in the target system domain (cloud, IoT, 5G,..).

Moreover, the correctness of the generated models relies on the completeness of the threat catalogue, but it is created on a best-effort approach and there are no ways to guarantee that all possible threats were considered.

Our idea is that, instead of granting completeness, we can offer a systematic approach that grants repeatability of the results, an easy way to update the catalogue and coherence of results when repeating the procedure. Accordingly, we developed a process that enables us to extend our modeling process to new application domains (in this paper the focus is on 5G infrastructures) and accordingly build the threat catalogue for such a domain following a systematic process, based on the technique commonly used for systematic literature reviews.

Figure 1, describes the steps of our methodology: (i) Domain Analysis, (ii) Systematic Review and (iii) Threat data Analysis; the final result is an extension of our modelling technique, which will be able to describe the target systems and the new Threat Catalogue.

Domain analysis aims to identify the main asset types (i.e. the hardware/software components and the protocols) adopted in the target domain systems and their relationship. Reference Architectures are the documents that mainly offer such information, they are available in scientific papers, typically surveys, in standard documents (like the [26] documents adopted in this paper) or in white papers. The main result of the Domain analysis is an extension of our modeling technique (MACM), in order to define the new set of asset types in order to let the analyst describe the system deployments. Next Section V will detail this step, applying the domain analysis to the 5G Infrastructures. In the same section, we will briefly summarize our modeling technique and illustrate the 5G extension.

The Systematic Threat Search aims at collecting security threats from the scientific literature: the core idea is to adapt the Systematic Literature Review methodology ([27]) in order to select all papers that contain a description of threats related to the target domain (in this case 5G). It is worth noticing that threat models in literature are expressed in many different ways and threats are described in natural languages. The systematic Threat search will result in a large collection of papers, each describing some of the possible threats. Different papers may propose the same threats with different names and/or with little changes in the behaviour.

The Systematic Threat Search will end (similarly to the systematic literature review) with a data extraction phase, that will propose a list of threats and their possible taxonomies.

The Threat Data Analysis will collect all the data extracted by the Systematic Threat Search and describe the threats according to our model, identifying the compromised asset, the threat behaviours the possible threat agents and all the other information that we store in our catalogue (as described in detail in section III. In this phase, we will solve the possible threat duplicates and other incoherence that may appear when comparing the different sources of data. The produced threats will enrich our Threat Catalogue.

As a final result, we will obtain:

- The extension of our modeling technique for the target domain
- the list of threats applicable to the model (The Threat Catalogue) needed to generate fine-grained threat models.

It is worth noticing that commonly we produce both a spreadsheet and a relation DB version of the Threat Catalogue, in order to have an easy way to consult it and/or tools for automation of the processes.

V. 5G DOMAIN ANALYSIS

The main goal of this paper is to offer an automated way to produce threat models for 5G systems, taking into account the way in which they are configured. Accordingly, we need a way to model in a simple and clear way different instances of 5G infrastructures. In order to address such a goal, in the following we briefly summarize the 5G reference architecture, that outlines the main components and their interactions, then we propose an extension to our graph-based model (MACM - multi-application composition model) in

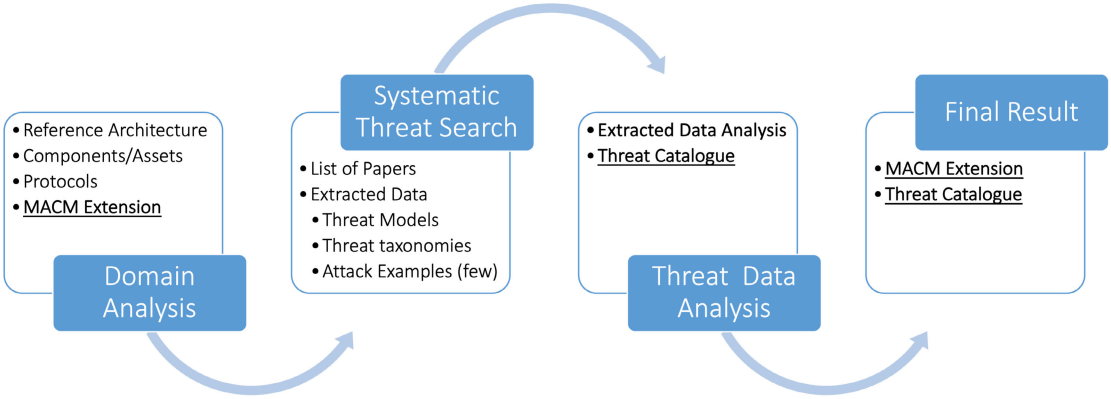

FIGURE 1. Methodology to build catalogue and extend MACM.

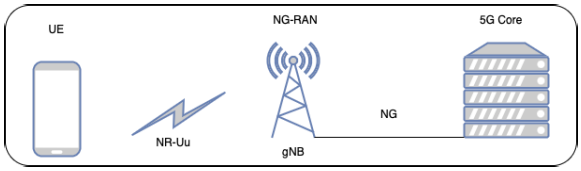

FIGURE 2. 5G high level architecture.

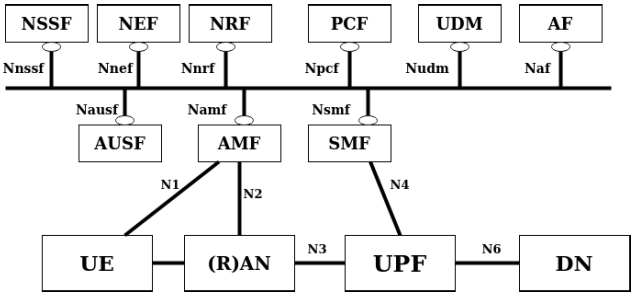

FIGURE 3. 5G system architecture - Source 3GPP.

order to describe 5G systems and automatically produce *fine-grained threat models* according to the process described in section III.

A. 5G ARCHITECTURE OVERVIEW

The evolution of 5G mobile networks towards a service-based architecture (SBA) comes with the emergence of numerous new challenges and objectives. First, 5G deployment introduces a brand-new set of technologies, such as the network function softwarization enabled by software-defined networking (SDN) and network functions virtualization (NFV), Mobile edge computing (MEC), and Network Slicing (NS). These require to be tested from a functional point of view; but, also from a non-functional point of view to determine the sanity of the system based on indicators such as data throughput performance, latency, scalability, robustness, etc.

As the previous generations of Mobile systems, a 5G architecture is composed of User Equipments (UEs), Radio Access Network (NG-RAN) and the Core Network (5GC), as briefly summarized in figure 2.

The NG-RAN collects the 5G technologies for the radio access network, its main entity is the radio transmitter (gNB, g stands for *5G*, NB for *Node B*) which is connected to the 5G core Network (5GC) with dedicated interfaces (NG).

The main innovations for the 5G Architecture rely on the way in which both the NG-RAN and the Core Network are organized and the kind of interfaces involved among them. As a matter of fact, the architecture aims at respecting a lot of strict requirements described in the 5GPP white paper,[2] which lead to innovative networking solutions like Network slicing. Moreover, the architecture enables interaction among different core networks and/or with NG-RANs of different providers.

It is out of the scope of this paper to detail all features and innovative ideas after the 5G architecture, for which we suggest the interested reader focus on [28]: Our main goal, according to our threat modelling process illustrated in section III, is the identification of the main*assets* of a typical 5G architecture.

The 5G architecture relies on a *Service-Based Architecture* (SBA) framework, where the architecture elements are defined in terms of ‘‘Network Functions’’ (NFs) rather than by ‘‘traditional’’ Network Entities. Via interfaces of a common framework, any given NF offers its services to all the other authorized NFs and/or to any ‘‘consumers’’ permitted to use these provided services. Such an SBA approach offers modularity and reusability. Figure 3, extracted from ‘System architecture for the 5G System (5GS)’ (TS 23.501) [29], shows the network functions of a 5G architecture. According to the terminology we adopt in our security modelling

[2]Read more at: https://5g-ppp.eu

processes, each Network Function is a different type of asset, subject to possible attacks/threats and that should be adequately protected. In technical terms, each NF will be a service, implemented by some code deployed in an execution environment.

The customer uses a device (User Equipment) to connect to the network through an Access Network (AN) to access the Data Network (typical external networks, e.g. Internet). Note that the AN can be 5G (NG-RAN), but may even be an older technology enabling interaction among new infrastructure and legacy systems. The Core network manages the system resources through the NFs illustrated in the figure and briefly listed above, enabling the management of the full network infrastructure.

- **UPF**, User Plane Function, handling the user data
- **AMF** Access and Mobility Management Function, that enables accesses of the UE and the (R)AN in the signalling plane
- **DN**, the (external) Data Network
- **AF**: The Application Function controlling the application(s)
- **SMF**: The Session Management Function handles the calls and sessions, and contacts the UPF accordingly
- The Network Slice Selection Function (**NSSF**).
- **UDM**: The Unified Data Management functionally similar to 3G and 4G's HSS (and 2G's HLR)
- **PCF**: The Policy Control Function controls that the user data traffic does not exceed the negotiated bearer(s) capacities.
- **NRF** The Network Repository Function "controls" the other NFs by providing support for NF register, deregister and update service to NF and their services.

For what regards the security functionality of the network, the 5G Core includes a Network Exposure Function (**NEF**), Authentication Server Function (**AUSF**) and Security Anchor Functionality (**SEAF**).

For a detailed analysis of the behaviours of each function and their interaction, we invite the interested reader to check the already cited standard TS 23.501 [29]. For the goals of this paper, it is relevant to outline the list of identified components of the architecture (the NFS) and their interactions, outlined by the protocols reported on the connection lines among the NFs.

B. 5G PROTOCOLS

5G Networks are Mobile networks and they offer new and innovative protocols for radio communications, but such protocols, which mainly affect communication among UE and NG-RAN are of little interest to this study, which focuses on 5G Infrastructure. In fact, 3GPP defines not only the air interface but also all the protocols and network interfaces that enable the entire mobile system: call and session control, mobility management, service provisioning, etc. Thanks to this approach 3GPP networks can operate in an inter-vendor and inter-operator context.

As already outlined the 5G architecture relies on a Service Based architecture, accordingly the NFs communicate with each other through dedicated protocols, defined at the application level. The core protocols involved in the standard are listed again in figure 3, even if they have names that are not particularly meaningful: **N1**, **N2**, **N3**, **N4**, **N6** for the interaction of the core assets distributed among Access Network and Core Network and the protocols offered by each of the NFs (named as N followed by the NF acronym) for the other components.

As a matter of fact, such protocols, defined in the 5G specifications and publicly available, (all references can be found in TS 23.501 [29]) are REST-based protocols, based in HTTP/HTTP2 having SCTP as the transport protocol.

Moreover, the protocols offered by the NFs reuse/adaptation of many of the existing application protocols. In the following, we briefly summarize a list of protocols involved in 5G, which should be considered later for threat modeling.

- **NAS**: the non-access stratum (NAS) is the highest stratum of the control plane between UE and MME at the radio interface. The main functions of the protocols that are part of the NAS are the support of mobility of the user equipment (UE) and the support of session management procedures to establish and maintain IP connectivity between the UE and a packet data network gateway (PDN GW).
- **AKA**: The authentication and key agreement protocol is a key exchange protocol between the UE, the serving network (SN) i.e., the antenna, and the home network (NH) i.e., the service provider.
- **RRC**: The Radio Resource Control (RRC) protocol is used in UMTS, LTE and 5G on the Air interface. It is a layer 3 (Network Layer) protocol used between UE and Base Station. The major functions of the RRC protocol include connection establishment and release functions, broadcast of system information, radio bearer establishment, reconfiguration and release, RRC connection mobility procedures, paging notification and release and outer loop power control.
- **Diameter**: The Diameter Protocol provides authentication, authorization, and accounting (AAA) messaging services for network access and data mobility applications in 5G networks.
- **SS7**: Signaling System Number 7 (SS7) is a set of telephony signalling protocols that are used to set up most of the world's public switched telephone network telephone calls. The main purpose is to set up and tear down telephone calls
- **HTTP2**: When 3GPP set out to define the 5G core network (5GC), it used all the latest web technologies to radically reshape core network architecture. One tiny part of this is the use of HTTP/2 for signalling between functions.
- **SCTP**: many of the NFs of the 5G core rely on SCTP as transport level protocol, instead of TCP. This choice is motivated by the flexibility that the protocol offers

and the protection integrated into the protocol against the most common attacks (e.g. 4-way handshake again SYN floods).

C. MACM 5G EXTENSION

Our Modelling technique relies on the MACM (Multi-Application Composition Model) formalism [30], a graph-based model in which each node of the graph represents an asset of the system, and each edge characterizes the existing relationship between two different assets. The MACM offers a simple way to synthesize an application architecture, focusing on its main assets, thus enabling the automation of the security evaluation for the assessed systems.

In the MACM formalism, a node models an asset and it is characterized by a primary label, that identifies the asset class and may have a secondary label, which further specifies the primary class. Note that Labels affect the relationship in which a node can be involved. Moreover, each node has a set of properties that better describe more specific attributes. A mandatory property is the *Asset Type*, which specifies the functional behaviour of the asset. The allowed *Asset Types* for a node depends on the labels. The *Labels* and the supported *Asset Types* are (partially) listed and described in Table 3.

It is worth noticing that we extended the MACM model introducing assets that are specific for the 5G (outlined in bold in the table): i) Core and RAN as networks, and ii) Each element of the Service-Based Architecture (e.g. Network Functions). Accordingly, the MACM was extended introducing a new secondary label *5G*, to be used together with the new components and that can be used together with the **service** primary label (for the system components that the 5G network adopts) or with the **Network** primary label when referring to the 5G assets adopted for connections.

Therefore, the service-based architecture can be modelled using service and 5G as respectively primary and secondary labels, and *Service.5G.NetworkFunction* to model all the service-based architecture (e.g. Service.5G.AMF). Network types, instead, can be related to a RAN (e.g. CRAN, VRAN or ORAN ad described in section V) or Core. We used *NetworkxRAN* or *Network.Core* to model all the *5G Network*. Tab. 4 summarizes the MACM relationships for the supported systems. It is worth noting that, the model supports different relationship labels, indicating different kinds of interaction. An example is the *hosts* relationship among two services, which outlines that a service is offered by another service. 5G extension to MACM is outlined by the new labels *Network.5G.x* and *Service.5G.x* in the table. Note that, a CSP can directly provide a Radio Access Network (e.g. Cloud RAN) or the overall Core Network. Moreover, each 5G service normally uses other 5G services but also can use other cloud services (SaaS). According to our modelling approach, we can describe the system in different levels of detail: considering the network function of 5G Core (Service Level), describing the overall Core as a Network without specifying all the network functions (Architectural Level), identifying all the 5G Network as a *Network.5G* asset type (High Level).

TABLE 3. MACM node labels and assets.

Primary Label	Secondary Label	Asset Type(s)	Description
CSC		CSC.Human	A customer that uses services
CSP		CSP	A service Provider like Amazon, Google, or a telecom provider
service	*IaaS*	VM, Container	Virtual Machine or Containers
service	*PaaS*	VM, Container	Virtual Machine or Containers
service	*SaaS*	Service.Web, Service.DB, Service.IOTGW, Service.MQTTBroker	Software (typically COTS) offered as a service
service	**5G**	**Service.5G.AMF, Service.5G.SMF, Service.5G.UPF, Service.5G.AUSF, Service.5G.NSSF, Service.5G.UDM, Service.5G.PCF, Service.5G.NRF, Service.5G.NEF, Service.5G.NWDAF Service.5G.RAN**	Components of a 5G Network offered as a service
Network	WAN	Internet	A wide area Network, typically the Internet
Network	LAN	Network.WiFi, Network.Wired	Local Access Network, the assets differs depending on the involved technologies
Network	PAN	Network.BLE, Network.ZigBee	Personal Area Network, the assets differ depending on the involved technologies
Network	**5G**	**Network.CRAN, Network.VRAN, Network.ORAN Network.Core Network.5G**	5G Network: CloudRAN, VirtualizedRAN, OpenRAN, Core Network, 5G Network as a whole
HW		HW.server, HW.PC, HW.UE HW.micro, HW.IOTDevice	A physical hosting hardware

TABLE 4. Relationship in MACM models.

Relationship	Start Node(s)	End Node(s)
uses	CSC, IaaS, SaaS, PaaS, IOTDevice, IoTGW **Service.5G.x**	IaaS, SaaS, PaaS, IOTDevice, IoTGW, HW **Service.5G.x**
provides	CSP	IaaS, SaaS, PaaS, Network, **Network.5G.x** , **Service.5G.x**
hosts	IaaS, HW, PaaS	SaaS, PaaS
connects	**Network.5G.x**	IaaS, IOTDevice, IoTGW, HW

The proposed extension allows the modeller to describe a more complex 5G scenario and obtain all the security issues based on the level of detail provided in modelling the system.

VI. SYSTEMATIC THREAT SEARCH

The core of the methodology relies on the threat catalogue, which should collect all the threats affecting the 5G systems. Completeness of the threat catalogue is an open issue and,

at the state of the art, there are no ways to guarantee that all possible threats are correctly described and collected in a threat model. It is worth noticing that even the tools adopted for automating as much as possible the process does not grant any completeness and rely on a *best-effort* approach.

We propose to adopt the Systematic Literature Review by Kitchenham et al. [27] approach in order to collect all the threats in literature and systematically integrate them into the catalogue: such an approach will grant repeatability and provability of the catalogue, being clear the process for collecting and organizing the threats. Moreover, repeating the process will help to update the catalogue according to changes in the literature. As a concluding action, all threats will be related to the concepts (*asset types* and *protocols*) adopted in the MACM extension for the target domain (5G).

A. ADAPTING SLR TO BUILD A THREAT CATALOGUE

As proposed by Kitchenham, the SLR will be conducted in three phases: Planning, Conducting, and Reporting. The first phase consists of developing a protocol used for searching articles from the sources, including and excluding papers from the overall results to answer some research questions. In the Conducting phase, we apply the rules developed in the protocol to obtain the list of the accepted papers suitable for answering research questions previously developed. The last phase involves writing up the results of the review and circulating the results to potentially interested parties.

The aim of conducting our SLR is to create a taxonomy of the threats that affect 5G architecture and a catalog of threats related to the 5G components and protocols.

In order to implement the PLAN phase, we identified a few research questions on which we relied to set up our search protocol. Accordingly, the SLR aims to offer a reply to the following questions:

- **RQ1**: Is there a complete threat model involving 5G architecture?
- **RQ2**: Which methodologies are used to produce a threat model of 5G architecture?

We translated the reply to such questions in a clear search in the literature search engines: ACM, Scopus, Springer, IEEE, and Google Scholar.

```
(''5g security'') OR
(''5g'' AND ''threat classification'') OR
(''5g'' AND ''threat model'') OR
(''5g'' AND ''threat modelling'') OR
(''5g'' AND ''threat analysis'') OR
(''5g'' AND ''threat classification'') OR
(''5g'' AND ''threat taxonomy'') OR
(''5g'' AND ''threat'') OR
(''5g'' AND ''threats'')}
```

It is worth noticing that the queries can be adapted to different application domains, identifying a keyword different from 5G for the domain. We noticed (through repetitive queries) that the keyword 5G (case insensitive) was enough to identify all papers that address this domain. In other cases, a more complex selection could be necessary.

TABLE 5. Inclusion criteria chosen for the review.

Inclusion Criteria	Motivation
The paper contains a threat model/classification related to overall 5G	Including a full threat model is our scope.
The paper contains a threat model/classification related to a single part of 5G	A threat analysis related to few (or just one) 5G components can be useful to extract data.
The paper contains a State of Art Review about 5G	Including the surveys is needful to the analysis of similar works.

TABLE 6. Exclusion criteria chosen for the review.

Exclusion Criteria	Motivation
It is not written in English	International readability and reproducibility.
It is not mainly concerned with 5G	Some papers can meet the search string because 5G is used just as a buzzword.
It is not about security	Since the research questions are related to a particular security process (i.e. threat modelling), all papers not related to security are excluded.
It does not contain threats/attacks	Since the aim is to collect threats and attacks, all the other works are excluded (e.g. the ones related to vulnerabilities and countermeasures).

We also needed eligibility criteria to select the relevant works that can answer the research questions. All the chosen criteria are shown in the tables 5 and 6. The papers from which data are obtained are the ones that contain threat models or classifications related to a single part or the overall 5G architecture. Also, white papers, reviews and surveys have been used to obtain threats. Once the papers have been selected using the inclusion/exclusion criteria, the form fields used for the Data Extraction are described in the table 7. By collecting these data, we expect to get both an exhaustive overview of threat modeling approaches used in the literature and a complete threat classification related to 5G architecture.

The Conduction phase has included three steps: i)Study identification, ii) Selection, iii) Extraction. The first step consists of identifying the studies by following a search strategy. We decided to use some sophisticated search strings based on Boolean expressions, applying the rule defined above, on the main digital libraries (using their own languages). We also added to the overall search results some sources of evidence, like the white paper related to 5G provided by ENISA [10].

As a result, we identified 1911 papers from all the already mentioned sources, except for Google Scholar results. Most parts of the identified papers are from Springer (47 percent), then Scopus (37 percent), IEEE (15 percent) and ACM with only 8 papers (0,4 percent). The second step of the

TABLE 7. Data extraction field.

Data Extraction Field	Field Value Type
Threats associated with each 5G component/a single part of 5G	List of threats
If it provides a threat taxonomy	Yes, Not
Attack examples on 5G	List of attacks
Threats associated to each 5G-related protocol	List of threats
Which protocols Does it consider?	List of protocols
Which method is used to produce threat model?	Method (String)

Conduction phase is about the selection of the study. Now, the huge number of studies needs to be reduced considering the criteria defined in the Protocol. In this phase, all the abstracts are read and analyzed and only the papers that meet the inclusion criteria are accepted. Our approach relies on the easy to use of StArt tool that automatically takes the Bibtex files (automatically downloaded from each source engine) as input and then lists all the papers in an interactive view in order to obtain easily all the information needed (abstract, keywords, journal, etc.). In this phase, we introduced a new exclusion criterion by using the StArt tool. The authors of StArt described a value (greater or equal to 0) associated with each resulting paper (from the previous phase). This score number represents the *similarity index between the selected paper and the keywords chosen for the protocol*. From the usage of the tool, we have verified that the formula to calculate this score is:

$$score = 5 * numTitle + 3 * numAbstract + 2 * numKeywords$$

Considering this score (automatically calculated from the tool), we choose to set as *Rejected* the papers that have a score equal to 0. This new exclusion criterion allowed us to automatically reject many papers. As a result of this step, from the 1911 starting papers, we selected 90 papers as suitable for data extraction, while 976 papers were rejected considering the exclusion criteria. We also reported 56 papers as duplicated (The stArt tool was not able to report) and 789 out-of-scope (e.g. with a score equal to 0).

The third step aims at extracting data from the selected papers through careful reading. In this phase, we also have to assess the quality of the study providing more detailed inclusion/exclusion criteria. Reading the papers, we decided to include also the papers that describe the security issues related to 5G-related protocols, because we aim to enrich existing taxonomies to consider all the 5G assets. Moreover, many authors describe some architecture partially related to 5G or too specific, so we decided to exclude the papers that mainly concern too specific areas. From the reading of 90 extracted papers, applying all the criteria shown above, 42 percent (38) met the inclusion criteria, 52 percent (47) met the exclusion criteria, 2 percent (2) were duplicated, 3 percent

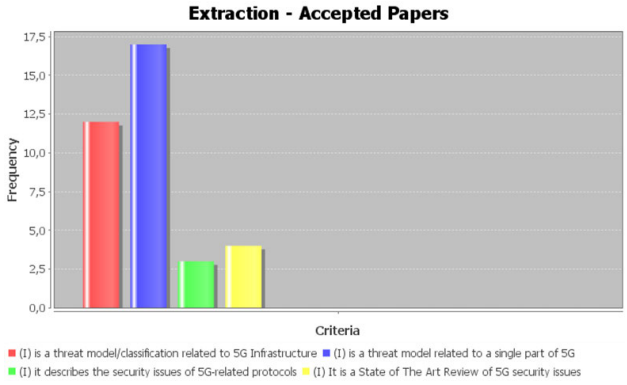

FIGURE 4. Bar chart representing the frequency of each inclusion criteria.

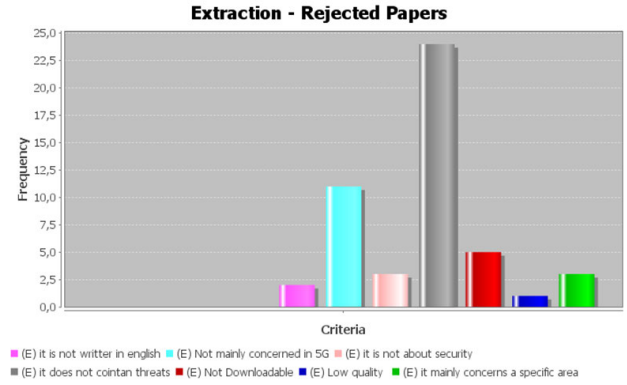

FIGURE 5. Bar chart representing the frequency of each exclusion criteria.

(3) instead was not available for the download.[3] Analyzing the accepted papers in detail, it is worth noting that most of them regard threat models related to a single part of the overall 5g architecture, as shown by the bar chart in figure 4.

A similar bar chart (shown in figure 5) has been produced by the StArt tool to describe the frequency of the exclusion criteria. The chart outlines how most of the rejected papers do not contain any information about threats. It also shows that some authors use *5G* only as a keyword, but not the main topic of the work.

From the 42 extracted papers, we selected 6 papers included as a state-of-the-art review of 5G security issues.

B. ANALYSIS OF RESULTS

The results of the SLR can be divided according to the RQ1 and RQ2: the first is an overview of the threat modeling approaches used in the 5G literature, and the second is an analysis of threats and attacks in the literature, considering both the 5G components and the 5G protocols. Most of the selected papers contain a full or a part of threat models, as shown in table 8, but the assets involved were in some cases not specified.

[3]All the papers have been downloaded using *Universitá of Campania Luigi Vanvitelli* Institutional Sign In.

TABLE 8. Data extraction results.

Data Extraction Attribute	Papers
It provides a threat taxonomy on 5G	6
It contains a full or a part of threat model about 5G Architecture	26
It describes some attacks on 5G	11
It lists threats due to 5G-related protocols	4

TABLE 9. Threat modelling approaches used.

Threat Modelling Approaches	Papers
Surveys/Not-well defined	7
High-Level asset abstraction	6
Per-protocol/5G Interface	4
Layers-based	3
STRIDE-based	2
Component-based	2
Attack-centric	1
Attack-tree based	1

Moreover, an important result comes from the security analysis of the 5G protocols. The inclusion of threats related to protocols could be innovative compared to existing taxonomies (e.g. ENISA [10]). Just from the analysis of 4 papers [31], [32], [33], and [34] related to 5G protocols, we extracted 56 threats related to the protocols: GTP, AKA, NAS, RRC, SIP, Diameter, SS7, HTTP2, and DHCP. Note that some protocols (e.g. Diameter and SS7) are from 4G architecture, but are still relevant because can be used in a 5G architecture based on 4G infrastructures (i.e. Non Standalone 5G). On the other hand, these threats have been collected using different threat modelling approaches, as shown in table 9. It is worth noting that not all selected papers have been used to select threats, but just 26 of 42. This is due to the impossibility of linking each threat described in the paper to a 5G component for information missing.

Most of the selected papers [35], [36], [37], [38], [39], and [40] collected the threats linked to some high-level 5G assets or involved technologies (i.e. Core Network, Network Slicing, etc). On the other hand, some authors collected threats without specifying the threat modeling methodology they used. Literature analysis also outlines the common use of a layer-based approach [14], [16], [41] to produce a threat model. According to this technique [14], the architecture is divided into layers and threats are not linked to a single component but associated with each 5G layer. More detailed approaches instead use attack-tree [42], component-based technique [10], [43], or attack-centric methodologies [44] to collect threats. Differently from the other techniques, attack-tree and attack-centric techniques is based on *potential approaches to achieving an event in which system security is penetrated or compromised in a specified way*. Instead of analyzing each different threat, some authors [13], [45] rely on the STRIDE [25] approach through which a high-level classification is used to determine the threats each component can be affected. There are also some other threats collected from the surveys or from some works in which no specific threat modelling methodology is provided [37], [46], [47], [48], [49], [50], [51]. Analysed all the approaches used in literature, it is worth noting that most of the papers associate threats to high-level assets instead of focusing on each 5G component. This approach is due to the need of stakeholder [18] that depends on the level of granularity required. The threat modelling techniques analysis also favours approaches focused on the different layers (e.g. ISO/OSI model) and the communication protocols used, focusing on the communications between the 5G interfaces and the resulting threats.

VII. THREAT DATA ANALYSIS

The analysis of the selected papers were translated into an Excel sheet containing both the threats related to all the 5G assets (supporting different levels of detail) and all the 5G-related protocols extracted from the SLR.[4] All the 5G catalogue has been built in two steps: i) collecting the threats for each 5G asset and protocol; ii) Enriching each couple (*Asset*, *Threat*) with our data model fields described above: PreCondition, PostCondition, STRIDE, and Compromised. Also, a detailed description of the threat is provided. As a result, 167 threats related to the 5G components and 56 threats due to 5G protocols have been listed To clarify the results, we reported a part of the threat catalogue associated with some 5G components in the table 10.

The table shows some examples of threats affecting three different asset types: Access Management Function (*Service.5G.AMF*), Radio Access Network (*Network.5G.RAN*) and the User Equipment (*HW.UE*). As an example, the AMF resources can be exhausted and lead to unavailability or errors of AMF and all the services that use it (as expressed in the Compromised field). A list of the sources describing the threat in detail is also provided. RAN, instead can be affected by Denial of Services threats (e.g. Jamming), but also some packets can be eavesdropped on by attackers on control and bearer plane. The threat compromises both the network and all the virtual machines connected to it. Some attackers can also be interested in attaching compromised User Equipment(e.g. mobile phone) to compromise some services offered by the mobile network (e.g. AMF). Also, the mobile data can be exposed and, accordingly, the UE can be compromised. Similarly, a part of the threat catalogue related to some 5G protocols is shown in the table 11.

Unlike the previous table, threats are linked to the protocols (specified in the uses relationships of the MACM) and *Compromise* field describes if the threat affects the client of the communication (i.e. *source(uses)*) or the server (i.e. *target(uses)*). For instance, Information leak (e.g. UE IP leaks using packet injection methods) can compromise only the client of the GTP communication (e.g. User Equipment, RAN), while Denial of Service attacks (e.g. Resource Exhaustion) can compromise all the assets involved in the

[4]The Excel file will be made available as supplemental material and all the results are available by request to the corresponding author.

TABLE 10. Part of threat catalogue related to 5G components.

Asset	Threat	Description	STRIDE	CIA	Compromised	Sources
AMF	Misconfigured system	This threat concerns the inclusion by the seller of malicious or defective software.	Tampering, DoS	I,A	self	[10], [37]
	Resource Exhaustion	The threat involves the generation of a massive number of requests or with such traffic that the network becomes partially or completely unavailable.	DoS	A	self, source(uses)	[10], [13], [16], [43]
RAN	Jamming	An attack that attempts to interfere with the reception of broadcast communications.	DoS	A	self	[13], [16], [48], [51], [54]
	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plane	Information Disclosure	A	target(connects)	[13], [16], [44]
UE	Hardware Manipulation	Compromised UE can communicate with the 5G infrastructure and harm the system.	Tampering	I,A	target(uses)	[16]
	Mobile data exposure	A lot of mobile applications, even coming from trustworthy stores, can expose user data and compromise the user equipment that is connected to the mobile network.	Information Disclosure	C	self	[46]

TABLE 11. Part of threat catalogue related to 5G protocols.

Protocol	Threat	Description	STRIDE	CIA	Compromised	Sources
GTP	Information Leak	IP information of the UE can be discovered by packet injection method sent using ADB command in Android terminal.	Information Disclosure	C	source(uses)	[34], [35], [44]
	Resource Exhaustion	The threat involves the generation of a massive number of requests or with such traffic that the network becomes partially or completely unavailable.	DoS	A	source(uses), target(uses)	[35]
AKA	Message Monitoring	Message Monitoring is used by a malicious attacker to obtain the private information of the UE	Information Disclosure	C	source(uses)	[36]
	Sensitive Data leakage	This threat concerns the secrecy of the session master key, which should be known by MTC and serving network only.	Information Disclosure	C	source(uses), target(uses)	[33]
NAS	Integrity Spoofing	Verification of NAS message can be avoided by manipulating some NAS fields	Spoofing	I	source(uses)	[34], [44]

communication. (e.g. both RAN and UPF in the N3 interface). Some other threats related to AKA (the protocol used for Authentication and Key Agreement) and NAS (Network-attached storage) are described in the table.

As described, this section proposes a methodology aimed at both buildings a catalogue to take into account the threats affecting a specific domain (e.g. 5G) and extending a flexible model to correctly describe each possible test-bed architecture for each level of detail. The last step concerns the maintenance of the threat catalog over time. The need for maintenance is due to the continuous emergence of implementations and security problems in modern systems. To take into account the emerging threats, an integration of the SLR should be performed considering all the new papers but keeping the SLR protocol unchanged.

VIII. 5G FINE-GRAINED THREAT MODEL GENERATION

Validation of threat models is an open issue: a state of art, at best of the author's knowledge, there are no ways to grant that a threat model is complete (all threats are considered) and consistent (all threats are applicable). However, we tested the validity of our technique by producing a complete fine-grained threat model and asking the experts (our industrial partners) to check the catalogue and validate its usefulness. In this section, we will present the generic procedure aimed at generating a threat model from the MACM and we will apply the procedure to our 5G test bed.

A. THREAT MODEL GENERATION PROCEDURE

The threat model generator procedure, described in detail in our previous work [3], selects all the threats that affect the system described by the MACM as the list of a couple $CompromisedAsset, MaliciousBehaviour$: $TM = \{[A_i, B_i]_{i=1...n}\}$.

The algorithm takes a MACM model as input and produces the threat model for the system as output. It is worth noting that our previous work takes also into account the threat agents [8] (i.e. malicious users having an interest in compromising the system). Since threat agent analysis is out of our scope, we applied the algorithm just to select all the malicious behaviour the SuT is affected by. The procedure relies on the catalogue data model presented in section III and associates some threats for each asset (i.e. the software component) considering:

- Asset-type parameter;
- Protocol and role in communication;
- Compromised field.

Firstly, all the threats related to the asset typology are enumerated for each asset. As an example, a *Service.Web* asset-type has different threats compared to a *Service.DB*. Therefore, all the protocols described by the in-going and out-going arcs are taken into account: We use the direction of the edge among the node (MACM relies on a directed graph) in order to assign a *role* to each asset involved in the communication. For instance, if a client (CSC) and a web application via the HTTP protocol, the MACM model adds HTTP attributes to the *uses* relationship between them and gives the CSC the role of the HTTP client, while the application assumes its role from the server. The currently offered approach only supports client-server relationships between assets, in future work, the goal is to extend the approach to different paradigms. Once our algorithm has classified the client and server from the direction of the edge, role filtering can be applied. Since we consider assets the components of the system (and not the relationships), the field *Role* determines if a threat applies to the Client or the Server, or both. For instance, if a threat is related to a specific protocol, but the Role is *source*, the threat comprises only the Client of the communication protocol. Finally, the field *Compromised* takes into account the indirect threats (i.e. threats that affect a specific component and are propagated to the neigh-boards) related to a specific component. Compromise field can be *self* if it compromises that component, or it can have a specific template: *Role(relationship)*. The Role field, as described above, can be *source* or *target* and identifies if the threat compromises the in-going or out-going edges coming from the component. The relationship instead applies a filter to the relation type the threat can be propagated. As an example, if a couple *Asset*, *Threat* has *[self, source(uses)]* as Compromised field, it means that the threat compromises the asset and all the nodes using that asset. On the other hand, if Compromised field is *source(connects)*, the threat is applied to all the networks connecting the asset (e.g. a LAN network). It is worth noting that, taking the MACM as an input, our approach automatically derives all the threats without any manual effort. In the next subsections, we describe a 5G case study using our MACM model and we applied our automatic technique to the 5G MACM in order to generate the specific threat model.

B. CASE STUDY

As a case study, we describe a 5G architectural model based on some open-source implementations. We used Open5GS[5] as Core Network (all the Core components) and srsRAN as a RAN service implementation.[6] As previously described, the first step of the proposed methodology provides the formal modelling of the system under analysis. In Table 12 are reported the nodes of our case-study 5G application, whereas Figure 6 shows the complete MACM model for the application.

[5]available at: https://open5gs.org/
[6]available at: https://www.srslte.com/

TABLE 12. Assets and their types in the case study.

Node	Labels	Asset Type
UE	HW	HW.UE
Each Core Function	service:5G	Service.5G.x
RAN	Network:5G	Network.RAN
DN	Network:WAN	Internet
VMs	service:IaaS	VM
Server	HW	HW.PC

TABLE 13. Relation between components in the case study.

Start Node	Relation	End Node	Protocol
UE	uses	AMF	NAS
RAN Service	uses	AMF	NGAP
RAN Service	uses	UPF	GTP
UPF	uses	SMF	PFCP
PCF	uses	AF	HTTP2
SMF	uses	PCF	HTTP2
AMF	uses	UDM	HTTP2
SMF	uses	UDM	GTP
AMF	uses	SMF	HTTP2
AMF	uses	AUSF	HTTP2
AUSF	uses	UDM	HTTP2
DN	connects	UPF	-
RAN	connects	DN	-
RAN	connects	VM	-

Each label affects the colour of the nodes, while attributes are not visible in the picture. As anticipated, the system is composed of a Server (i.e. *HW.PC*) that hosts two different Virtual Machines (i.e. *IaaS VMs*). One VM hosts all the 5G Core network functions (AUSD, UDM, AMF, SMF, PCF, AF, and UPF), while another VM host the RAN Service (*Service.5G.RAN)*. On the other hand, User Equipment (e.g. smart phone supporting 5G) uses all the 5G core network functions through the RAN service (i.e. software hosted on a specific virtual machine that includes SA UE application and SA gNodeB capabilities). The Radio Access Network, modelled in green with *Network.5G* labels, allows the user equipment to connect to the Data Network (i.e. Internet). Note that the distinction between RAN Service and RAN network being modeled is due to different security issues. The ran service carries application-level threats, while the RAN network can be compromised by network threats.

Tables 12 and 13 summarize the model. Note that the table 13 shows only the *uses* and *connects* relationships for brevity's sake. Each host relationship (from Server to VMs and from VMs to NF) is shown in figure 6.

The table 4 was created considering only application-level layer protocols and sequences models data analyzed from the ETSI (European Telecommunications Standards Institute) official documentation [26].

C. THREAT MODEL GENERATION

According to our case study, the assets are the ones already anticipated above and summarized in tables 3 and 4. Applying the threat modelling approach we produce some lists of threats for each selection criteria described above. For

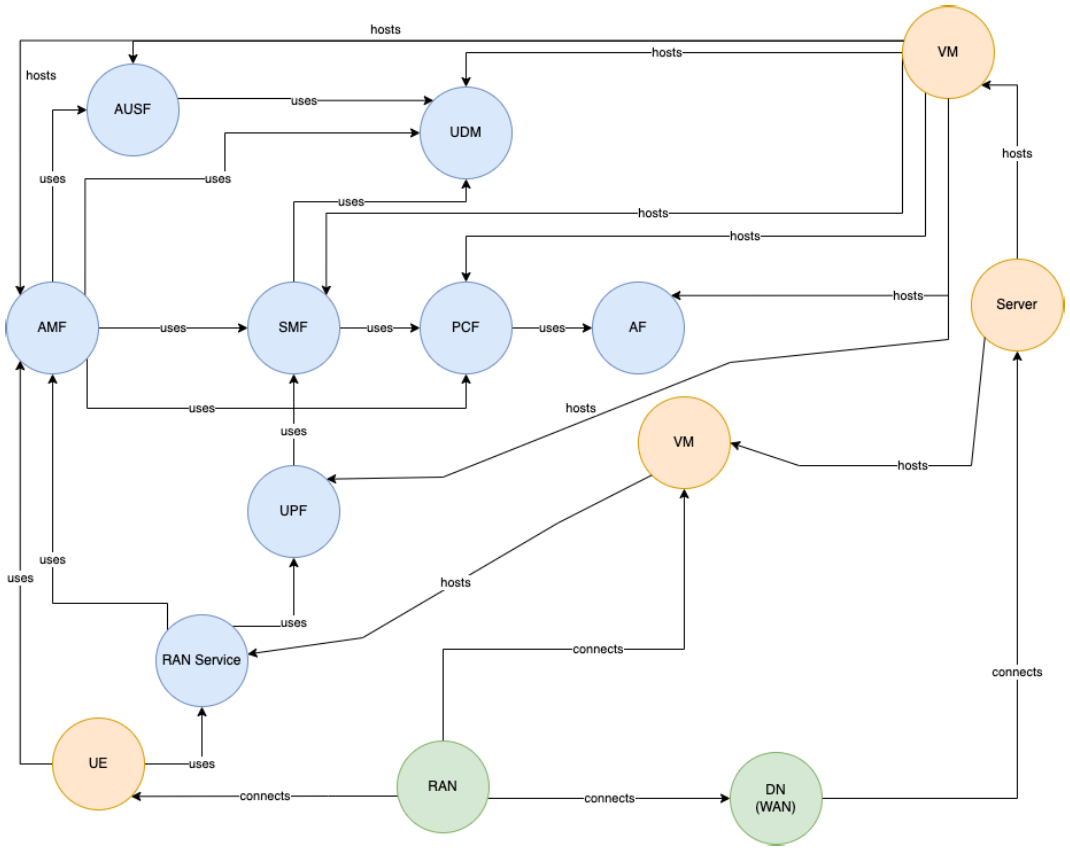

FIGURE 6. Case study MACM.

TABLE 14. Part of threat model per asset.

Threat	STRIDE	PostCondition	Asset
Resource Exhaustion	DoS	[n,n,p]	Core Service, RAN Service
Jamming	DoS	[n,n,p]	RAN, UE
Eavesdropping	Information Disclosure	[p,p,n]	RAN, UE, AMF, SMF, UPF
Data forging	Tampering	[n,p,n]	AMF, AUSF, PCF
Unauthorized Code Execution	Spoofing, Tampering	[p,p,n]	VMs
Crash	Tampering, DoS	[n,p,f]	Server
...	...	...	...

simplicity' sake we present three different lists of threats divided by the threat selection criteria described above. Since the full list of Threats is not compatible with the length of the paper, only a part of the threat model is shown. Firstly, the table 14 shows some threats affecting our system selected by the asset typology.

Analyzing the table it is possible to outline, as an example, that each Core service, but also the RAN service can be exposed to threats such as Resource Exhaustion: all the resources can be exhausted by a massive number of requests and it can partially or completely make the service unavailable. Also, Network and UE can be partially compromised by some Denial Of Services threats (e.g. Jamming). Some other threats affect only some Core Network services, as described in detail by ENISA: some data can be forged by a malicious user to compromise the integrity of AMF, AUSF and PCF. RAN instead can be subjected to Eavesdropping: an adversary can retrieve valuable data from the transmitted messages that are sent into the network. The eavesdropping threat can also compromise the UE and some core network services (e.g. AMF, SMF, UPF). Other threats that affect the VMs are linked to the execution of unauthorized code (e.g. Malware) that can also lead to Server Crash.

As partially shown in the table 15, we collected 25 new threats related to the protocol used in out test-bed (Standalone 5G). Unlike the asset-type threat model shown before, we added the *Protocol* field.

As an example, the GTP protocol used in the N2 interface (communication between RAN Service and AMF) and N10 interface(communication between SMF Service and UDF) can be the source of Impersonation and Information Leak threats but, since the *Role* field is *source*, it compromises only the clients in the communication: RAN Service and SMF. Moreover, the N1 interface can be exposed in some cases to Integrity Spoofing threats: the integrity verification of

TABLE 15. Part of threat model due to protocols.

Threat	STRIDE	Post Condition	Asset	Protocol
Impersonation	Spoofing	[p,n,n]	RAN Service, SMF	GTP
Information Leak	Information Disclosure	[p,n,n]	RAN Service, SMF	GTP
Integrity Spoofing	Spoofing	[n,p,n]	UE,AMF	NAS
Slow-rate DoS	DoS	[n,n,p]	AF, PCF, UDM, SMF, AUSF	HTTP2
Traffic decryption	Information Disclosure	[p,n,n]	AF, PCF, UDM, SMF, AUSF, SMF, AMF	HTTP2
...	...	...	...	...

TABLE 16. Some threats due to compromised field.

Threat	STRIDE	Post Condition	Asset	Due to
Traffic Modification	[n,p,n]	Tampering	UE	RAN Interface
Exploitation of software vulnerabilities	[n,p,p]	Tampering, Information Disclosure, DoS	VMs	AMF,SMF,RAN Service, AUSF, UDM, PCF
Crash	[n,p,f]	Tampering, DoS	Each Core Service	VM
Data breach	[p,n,n]	Information Disclosure	Each Core Service	VM
Impersonation	[p,n,n]	Spoofing	AMF	SMF
...	...	...	...	...

NAS messages can be avoided by modifying some message fields. The most common threats in the Core network are related to HTTP2 communication between the services. As an example, the availability of some services (e.g. SMF, AF, etc) can be compromised by sending malformed packets using a limited amount of attack bandwidth (Slow-rate DoS). Also, in some Core interfaces, the traffic on the network can be deciphered, leading to a data leak. The last part of the threat model contains propagated threats selected leveraging the *Compromised* field described above.

As shown in the table 16, Ran Interface can be subjected to *Exploitation of software vulnerabilities* threat, accordingly, UE integrity (i.e. the component that uses the RAN Service) can be indirectly compromised. Some threats can be due to possible implementation vulnerabilities of some Core services or the RAN Service, and they can compromise not only the services but also the Virtual Machines the services are installed on. Other threats, such as Crash or data breach, affecting the infrastructures (VM) can be propagated to the services hosted on them. Finally, a malicious user can impersonate an SMF by installing a trusted service that communicates with the AMF without the right permission.

IX. CONCLUSION AND FUTURE WORK

Although the use of the 5G Architecture paradigm offers important advantages in terms of latency reduction and the number of connected devices, it introduces new security issues. Therefore, this paper presents a methodology to extend our catalog and our model to support security assessment and (specifically) automated threat modeling for a specific field. The methodology is based on a systematic literature review aimed at collecting all the relevant threats and security issues. In particular, the methodology has been applied to a 5G scenario. Firstly, a detailed analysis of 5G architecture and the related protocols is carried out.

The analysis was useful to present an overview of the 5G architecture and to model the case study considering both the 5G components supported by our scenario and the used protocols. Then all the threats selected from the systematic literature review have been associated with both specific labels (i.e. asset types) and the 5G-related protocol to produce a complete 5G catalog.

The performed SLR analysed the threat modelling approaches used in literature in the context of 5G. The related findings state that most of the approaches use High-level descriptions of 5G assets due to the difficulty of modelling 5G components and related threats. Although ENISA provides a threat landscape about 5G, the document does not focus on protocols that can lead to some threats. Accordingly, the aim of our SLR was to extend the 5G ENISA threat catalogue considering all the protocols involved in the 5G interfaces and used it to produce automatically a threat model of (most of) 5G test beds. In order to do this,our modelling technique has been extended to support the 5G, and we applied the methodology to an open-source 5G test-bed proposed by the French MONTIMAGE company. The 5G architecture has been modeled using the extended MACM model and we applied the threat modeling generation technique to produce a threat model.

The result is a list of all the threats affecting each 5G component belonging to our test bed due to the 5G component typology, the protocols used in the communication or the compromised neighbours. In future work, we aim to apply our automated expert system [3] to generate penetration testing plans and implement them based on the produced threat model and the attacks selected from the SLR. Accordingly, our automated risk analysis technique [22] can be applied to the system to calculate the probability that an attack can happen and some standard controls can be suggested to mitigate (or reduce) the risks.

REFERENCES

[1] K. Wuyts, Z. Braiterman, A. Shostack, J. Marcil, S. de Vries, I. Michlin. (2020). *Threat Modeling Manifesto*. [Online]. Available: https://www.threatmodelingmanifesto.org/
[2] D. Granata and M. Rak, "Systematic analysis of automated threat modelling techniques: Comparison of open-source tools," *Softw. Qual. J.*, 2023.
[3] M. Rak, G. Salzillo, and D. Granata, "ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107721.

[4] A. Misuri, N. Khakzad, G. Reniers, and V. Cozzani, "A Bayesian network methodology for optimal security management of critical infrastructures," *Rel. Eng. Syst. Saf.*, vol. 191, Nov. 2019, Art. no. 106112.
[5] D. Granata, M. Rak, G. Salzillo, and U. Barbato, "Security in IoT pairing & authentication protocols, a threat model, a case study analysis," in *Proc. ITASEC*, vol. 2490, 2021, pp. 207–218.
[6] M. Ficco, D. Granata, M. Rak, and G. Salzillo, "Threat modeling of edge-based IoT applications," in *Proc. Int. Conf. Quality Inf. Commun. Technol.* Cham, Switzerland: Springer, 2021, pp. 282–296.
[7] M. Rak, G. Salzillo, and C. Romeo, "Systematic IoT penetration testing: Alexa case study," in *Proc. 4th Italian Conf. Cyber Secur.*, vol. 2597, 2020, pp. 190–200.
[8] D. Granata and M. Rak, "Design and development of a technique for the automation of the risk analysis process in IT security," in *Proc. 11th Int. Conf. Cloud Comput. Services Sci.*, 2021, pp. 87–98.
[9] J. Williams. (2020). *OWASP Risk Rating Methodology*. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
[10] ENISA, "ENISA threat landscape for 5G networks," White Paper, Attica, Greece, Nov. 2019.
[11] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
[12] R. T. Tiburski, L. A. Amaral, and F. Hessel, "Security challenges in 5G-based IoT middleware systems," in *Internet of Things (IoT) in 5G Mobile Technologies*. Cham, Switzerland: Springer, 2016, pp. 399–418.
[13] A. Dutta and E. Hammad, "5G security challenges and opportunities: A system approach," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 109–114.
[14] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G security challenges and solutions: A review by OSI layers," *IEEE Access*, vol. 9, pp. 116294–116314, 2021.
[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.
[16] M. N. I. Farooqui, J. Arshad, and M. M. Khan, "A layered approach to threat modeling for 5G-based systems," *Electronics*, vol. 11, no. 12, p. 1819, Jun. 2022.
[17] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera, "A stakeholder-oriented security analysis in virtualized 5G cellular networks," *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107604.
[18] T. Madi, H. A. Alameddine, M. Pourzandi, and A. Boukhtouta, "NFV security survey in 5G networks: A three-dimensional threat taxonomy," *Comput. Netw.*, vol. 197, Oct. 2021, Art. no. 108288.
[19] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "A novel security-by-design methodology: Modeling and assessing security by SLAs with a quantitative approach," *J. Syst. Softw.*, vol. 163, May 2020, Art. no. 110537.
[20] V. Casola, A. De Benedictis, M. Rak, and G. Salzillo, "A cloud secdevops methodology: From design to testing," in *Proc. Int. Conf. Quality Inf. Commun. Technol.* Cham, Switzerland: Springer, 2020, pp. 317–331.
[21] V. Casola, A. De Benedictis, M. Rak, and E. Rios, "Security-by-design in clouds: A security-SLA driven methodology to build secure cloud applications," *Proc. Comput. Sci.*, vol. 97, pp. 53–62, Jan. 2016.
[22] D. Granata, M. Rak, and G. Salzillo, "Risk analysis automation process in it security for cloud applications," in *Cloud Computing and Services Science*, D. Ferguson, M. Helfert, and C. Pahl, Eds. Cham, Switzerland: Springer, 2022, pp. 47–68.
[23] M. Rak, "Security assurance of (multi-)cloud application with security SLA composition," in *Proc. Int. Conf. Green, Pervas., Cloud Comput.* Cham, Switzerland: Springer, 2017, pp. 786–799.
[24] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in IoT systems," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100056.
[25] M. T. J. Ansari, D. Pandey, and M. Alenezi, "STORE: Security threat oriented requirements engineering methodology," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 2, pp. 191–203, Feb. 2022.
[26] *System Architecture for the 5G System*, document TS 123 501, V15.3.0, ETSI, Sep. 2018.
[27] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.
[28] 5G PPP Architecture Working Group, "View on 5G architecture," Heidelberg, Germany, Tech. Rep., Feb. 2020.
[29] *System Architecture for 5G Systems (5GS)*, document TS 123.501, 3GPP, 2020.
[30] M. Rak, "Security assurance of (multi-)cloud application with security SLA composition," in *Green, Pervasive, and Cloud Computing*. Cham, Switzerland: Springer, 2017, pp. 786–799.
[31] R. Giustolisi and C. Gehrmann, "Threats to 5G group-based authentication," in *Proc. 13th Int. Joint Conf. e-Business Telecommun.*, 2016, pp. 360–367.
[32] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *J. Internet Serv. Inf. Secur.*, vol. 10, no. 2, pp. 1–15, 2020.
[33] S. Park, B. Choi, Y. Park, D. Kim, E. Jeong, and K. Yim, "Vestiges of past generation: Threats to 5G core network," in *Proc. IMIS*, 2020, pp. 468–480.
[34] Z. Yan, C. Gu, and H. Huang, "Analysis for threat models and improvement scheme of 5G AKA protocol based on Petri-net," in *Proc. IEEE 21st Int. Conf. Commun. Technol. (ICCT)*, Oct. 2021, pp. 11–17.
[35] J. M. Batalla, E. Andrukiewicz, G. P. Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, and M. Imran, "Security risk assessment for 5G networks: National perspective," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 16–22, Aug. 2020.
[36] K. Cabaj, M. Gregorczyk, W. Mazurczyk, P. Nowakowski, and P. Zórawski, "Network threats mitigation using software-defined networking for the 5G internet of radio light system," *Secur. Commun. Netw.*, vol. 2019, pp. 1–22, Feb. 2019.
[37] R. Ettiane, A. Chaoub, and R. Elkouch, "Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102943.
[38] J. M. J. Valero, P. M. S. Sánchez, A. Lekidis, J. F. Hidalgo, M. G. Pérez, M. S. Siddiqui, A. H. Celdrán, and G. M. Pérez, "Design of a security and trust framework for 5G multi-domain scenarios," *J. Netw. Syst. Manag.*, vol. 30, no. 1, p. 7, Jan. 2022.
[39] H. A. Kholidy, "Multi-layer attack graph analysis in the 5G edge network using a dynamic hexagonal fuzzy method," *Sensors*, vol. 22, no. 1, p. 9, Dec. 2021.
[40] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5G networks," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT)*, May 2022, pp. 446–454.
[41] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 193–199.
[42] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G security threat assessment in real networks," *Sensors*, vol. 21, no. 16, p. 5524, Aug. 2021.
[43] H. Wang, Y. Lin, and W. Li, "Research on threat modeling for 5G network data analytics function," in *Proc. Int. Conf. Netw., Commun. Inf. Technol. (CNCIT)*, Jun. 2022, pp. 171–178.
[44] B. Santos, L. Barriga, B. Dzogovic, I. Hassan, B. Feng, N. Jacot, V. T. Do, and T. Van Do, "Threat modelling for 5G networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2022, pp. 611–616.
[45] D. Sattar, A. H. Vasoukolaei, P. Crysdale, and A. Matrawy, "A STRIDE threat model for 5G core slicing," in *Proc. IEEE 4th 5G World Forum (5GWF)*, Oct. 2021, pp. 247–252.
[46] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2020, pp. 1010–1015.
[47] A. Ghafoor, M. A. Shah, M. Mushtaq, and M. Iftikhar, "5G security threats affecting digital economy and their countermeasures," in *Proc. Competitive Advantage Digital Economy*, 2021, pp. 70–77.
[48] G. M. Køien, "On threats to the 5G service based architecture," *Wireless Pers. Commun.*, vol. 119, no. 1, pp. 97–116, Jul. 2021.
[49] J. Park, S. Rathore, S. K. Singh, M. Salim, A. el Azzaoui, T. Kim, Y. Pan, and J. Park, "A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions," vol. 11, p. 22, Jan. 2021.
[50] R. Piqueras Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019.
[51] M. Raavi, S. Wuthier, A. Sarker, J. Kim, J.-H. Kim, and S.-Y. Chang, "Towards securing availability in 5G: Analyzing the injection attack impact on core network," in *Proc. Silicon Valley Cybersecurity Conf.*, S.-Y. Chang, L. Bathen, F. Di Troia, T. H. Austin, and A. J. Nelson, Eds. Cham, Switzerland: Springer, 2022, pp. 143–154.

[52] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2018, pp. 1–6.

DANIELE GRANATA received the master's degree in computer engineering, in 2020. He is currently pursuing the Ph.D. degree with the University of Campania Luigi Vanvitelli, Aversa, Italy, under the supervision of Prof. Massimiliano Rak. His research interest includes cyber security, especially automatic threat modeling and risk analysis processes covering cloud and edge-based systems and the Internet of Things.

MASSIMILIANO RAK received the Ph.D. degree in computer engineering, in 2002. He is currently a Professor with the University of Campania Luigi Vanvitelli, Italy. He coordinated the SPECS FP7 European research project on security service level agreement in the cloud and participated in many projects focused on security in the cloud and the IoT systems. His research activity is reported in more than 150 scientific articles. His research interests include distributed systems performance and security evaluations. His research activities have recently focused on security assessment automation, trying to systematically use threat intelligence data as a basis for offering automation support to security evaluation processes.

WISSAM MALLOULI received the degree in telecommunication engineering from the National Institute of Telecommunication (INT), in 2005, and the Ph.D. degree in cybersecurity from Télécom and Management SudParis, France, in 2008. He is currently the CTO of Montimage EURL, Paris, France. His expertise covers continuous risk management and cyber-defense of critical systems and networks, including cloud-based systems, the IoT, and 4G/5G networks. He is working on several collaborative European research projects and has more than 50 scientific publications in popular conferences and journals.

Open Access funding provided by 'Università degli Studi della Campania "Luigi Vanvitelli"' within the CRUI CARE Agreement