Journal of Network and Systems Management (2022) 30:7
https://doi.org/10.1007/s10922-021-09623-7

Design of a Security and Trust Framework for 5G Multi-domain Scenarios

José María Jorquera Valero[1] · Pedro Miguel Sánchez Sánchez[1] · Alexios Lekidis[2] · Javier Fernandez Hidalgo[3] · Manuel Gil Pérez[1] · M. Shuaib Siddiqui[3] · Alberto Huertas Celdrán[1] · Gregorio Martínez Pérez[1]

Received: 21 December 2020 / Revised: 14 July 2021 / Accepted: 12 August 2021 /
Published online: 8 October 2021

Abstract

With the expansion of 5G networks, new business models are arising where multi-tenancy and active infrastructure sharing will be key enablers for them. With these new opportunities, new security risks are appearing in the form of a complex and evolving threat landscape for 5G networks, being one of the main challenges for the 5G mass rollout. In 5G-enabled scenarios, adversaries can exploit vulnerabilities associated with resource sharing to perform lateral movements targeting other tenant resources, as well as to disturb the 5G services offered or even the infrastructure resources. Moreover, existing security and trust models are not adequate to react to the dynamicity of the 5G infrastructure threats nor to the multi-tenancy security risks. Hence, we propose in this work a new security and trust framework for 5G multi-domain scenarios. To motivate its application, we detail a threat model covering multi-tenant scenarios in an underlying 5G network infrastructure. We also propose different ways to mitigate these threats by increasing the security and trust levels using network security monitoring, threat investigation, and end-to-end trust establishments. The framework is applied in a realistic use case of the H2020 5GZORRO project, which envisions a multi-tenant environment where domain owners share resources at will. The proposed framework forms a secure environment with zero-touch automation capabilities, minimizing human intervention.

Keywords Network security · Trust management · End-to-end security & trust framework · Threat models · 5G

✉ José María Jorquera Valero
josemaria.jorquera@um.es

Extended author information available on the last page of the article

1 Introduction

The fifth generation of mobile networks (5G) is currently being adopted as a solution to balance the rapidly evolving demand from users and tenants for network coverage, bandwidth, latency, and data capacity that could not be covered by the previous generations (i.e., 3G and 4G) [1]. Besides, the continuously increasing number of mobile devices requires more efficient use of mobile network infrastructures, being accomplished in 5G through the adoption of techniques such as Network Functions Virtualization (NFV). NFV leverages common hardware to develop a virtualization layer, which allows sharing network resources in different 5G infrastructure segments, such as the Mobile Core, Radio Access Network (RAN), Transport, or Mobile Edge (i.e., base stations).

Shared resources across the network infrastructure can be configured and connected to build multi-tenant logical networks, called network slices [2]. Network slices may belong to three main categories based on their application and network requirements. These categories are Enhanced Mobile Broadband (eMBB) for video and content streaming applications, Massive Machine-type Communications (mMTC) for large-scale applications with many connections, and Ultra-Reliable Low-Latency Communications (URLLC) for critical applications with real-time requirements. Depending on the requirements, each category includes diverse types of shared mobile resources whose functionality is usually virtualized with the so-called Virtualized Network Functions (VNF). The composition of resources and VNFs across shared 5G infrastructure segments is used to form a multi-tenant network. Moreover, resources can be either common functions, such as the Simple Network Management Protocol (SNMP), or dedicated, as the Constrained Application Protocol (CoAP) and Message Queue Telemetry Transport (MQTT) protocols for communication with specific Internet of Things (IoT) devices [3].

Despite the benefits that the increased number of mobile devices as well as the multi-tenant network slices bring, they also enable an exponential increase of threat landscape for 5G networks [4]. Additionally, multi-tenancy makes this landscape dynamic, as new zero-day threats are continuously introduced. In this context, adversaries may easily eavesdrop 5G network communications, gain unauthorized access to network slices, and then trigger malicious actions to compromise the mobile infrastructure operation or the exchanged data by users or tenants. The complexity of the NFV reference architecture as well as the multiple critical assets it contains make it prone to cyber-attacks [5] that, apart from the societal impact, lead to catastrophic consequences (e.g., financial, credibility losses) for Mobile Network Operators (MNOs), their tenants as well as Communication Service Providers (CSPs).

The lack of best practices for the protection of mobile infrastructures against cyber-attacks increases the security risks and holds back the 5G adoption [4]. Furthermore, they are mostly linked to authentication and authorization mechanisms, which can however be exploited by adversaries using existing vulnerabilities [6]. Similarly, the trust aspect is not adequately addressed in the literature as there are not enough trust models in 5G networks [7]. The reasoning behind this is that trust is a dynamic concept that should be continuously adapted to new requirements, technologies, and enforcement environments, with 5G ecosystems being an area where trust models will be fundamental in maintaining end-to-end security and trustworthiness connections among stakeholders; for instance, enabling a trustworthy Network Slice Orchestration across multiple domains [8] or building cross-domain trust in software-defined 5G networks [9].

To cope with these challenges, new security and trust mechanisms should be introduced to implement full isolation in network slices as well as prevent unauthorized and malicious entities from accessing the 5G infrastructure. Moreover, apart from the 5G infrastructure, the mechanisms should cover multi-domain scenarios, where each domain is specified according to the administrative point of view, i.e., the group of resources belonging to a specific resource owner. Hence, multi-domain scenarios tightly combine the set of resources of a given domain with another set of resources from another domain. Specifically, the variety of communication mechanisms and protocols that are used in the different segments of the 5G infrastructure, as well as the multi-domain environments, requires advanced detection techniques that can interpret the control and data plane commands, and distinguish the legitimate from the malicious ones.

With the goal of improving the previous challenges, this article proposes a novel framework for increasing the security and trust levels of the 5G infrastructure, shared by diverse multi-tenant network slices. Concretely, this framework is developed following the security and trust approach by the H2020 5GZORRO project [10]. 5GZORRO aims to design and build a security and trust framework to validate zero trust principles in distributed multi-stakeholder environments [11]. Besides, such a framework will be integrated with 5G service and resource management platforms, along with distributed ledger technologies and zero-touch automation solutions, to boost a flexible and secure composition of 5G networks. Therefore, this solution includes detection and protection schemes for each domain as well as the 5G network infrastructure. These schemes are sets of policies designed to enhance the resilience of both intra- and inter-domain environments against the possible cyberattacks suffered, guaranteeing a prompt response to incidents. To identify the main detection and protection schemes to be applied, a thorough threat model covering the threat landscape of multi-tenant 5G networks is required, being considered not only security but also trust threats. The proposed framework combines different mechanisms for network security monitoring, threat investigation, and end-to-end trust establishments in multi-domain and multi-tenant environments. As well, this work also contemplates essential trends such as zero-touch automation [12], to minimize human intervention, and zero trust [11], to downsize the attack surface by means of the trust model. In the end, the feasibility of the framework has to be demonstrated in existing multi-tenant use case scenarios and workflows, in which it allows the establishment of trustworthy 5G-enabled network slices (service layer, network function layer, and infrastructure layer). In this sense, the contributions of this article are as follows.

- A threat model that recognizes some of the principal multi-tenant 5G network threats. This threat model is divided into two different threat sets: a first one reporting threats that affect the trust relationships among network entities; and a second set reporting the security threats related to the different logical levels and components in 5G networks. By means of this threat model is boosted the need of solutions that enhances security and trust procedures in multi-tenant 5G networks.
- A novel framework that increases the security and trust levels of multi-tenant 5G networks. This framework follows a modular architecture composed by three components: the trust management module, which monitors, evaluates, and updates the trust chain generated among the different network entities; the intra-domain module, which monitors the domain network looking for potential threats or ongoing attacks, mitigating them if needed and possible; and the inter-domain module, which manages the security of the link connections with resources located at a third party's premises.
- A use case showing the framework application in an existing multi-tenant scenario based on the H2020 5GZORRO project. This use case is drawn as a real workflow of multi-domain interactions for resource leasing, detailing where the security and trust framework can be applied to ensure the selection of a reliable third-party provider and the resources involved, and a secure end-to-end network slice establishment.
- A discussion and comparison of the most recent security and trust frameworks found in the literature. From this comparison, a set of trends and challenges is extracted as guidelines for future work in the area, indicating the key questions to be considered to enhance the current state-of-the-art.

The rest of the paper is organized as follows. Section 2 provides a literature review of the existing security and trust models. Section 3 illustrates a threat model for multi-tenant 5G domains and Sect. 4 presents the framework that tackles the identified threats as well as increases the security and trust level in the 5G infrastructure. Moreover, Sect. 4 also demonstrates the application of the framework to existing multi-tenant scenarios. Section 5 discusses the challenges that are faced when applying the framework to such scenarios and links these challenges to standardization initiatives. And finally, Sect. 6 provides a summary of the article contributions as well as open perspectives for future work.

2 Current Security and Trust Models

Telecommunication Networks are a continuously developing field that needs to be kept up to date to cover novel security and trust requirements. The arrival of 5G networks has encouraged the emergence of new designs and technologies, as well as their associated properties and requirements. The previous security and trust models have become partially obsolete, and therefore, they require an iteration to adjust them to the new challenges brought by the 5G networks. Thus, this section performs a thorough review of trust models and/or trust management frameworks' state-of-the-art. Table 1 summarizes the most meaningful ideas of each proposal.

Such is the importance of security and trust models in future Telecommunication Networks that not only 5GZORRO [13] is a research project focused on addressing this area. 5G-ENSURE [14] developed a trust modeling platform for 5G networks in the context of operators sharing their network resources. 5G-ENSURE involved partners defined trust as a decision to accept (or not) risks arising from one or more threats by means of their Trust Builder tool. Another EU research project focused on trust establishment is INSPIRE-5G Plus [15]. Its project consortium is working on an automated end-to-end security management framework that allows not only protection but also trustworthiness in managing 5G cross-domains scenarios. In a similar vein, MonB5G [16], another EU's Horizon 2020 research and innovation project, centers on zero-touch slice management and orchestration to ensure end-to-end cross-domain Service Level Agreements (SLAs). In addition, it also empowers both Artificial Intelligent (AI)-assisted policy driven security monitoring and trust mechanisms for trustworthy and secure cross-domain operations. These are just some of the more recent research projects focused on modeling security and trust in 5G networks, but they are the drivers that intend to start the long road ahead in this area. Nevertheless, not only EU research projects are interested in building trust for 5G networks, the National Science Foundation via Secure and Trustworthy Cyberspace (SaTC) proposal is encouraging the generation of future projects that investigate frameworks and models for trust in computing environments, considering zero trust architectures and interpreting trust as a transparency and accountability mechanism [17].

One of the paramount rules in trust models is to guarantee that user data is trustworthy, and consequently, they are not biased since could be an indication that a trust model is receiving unrealistic recommendations, or in other words, is suffering from a collision attack. In [18], Jayasinghe et al. designed a hybrid trust framework that enabled them to assess user trust and data trust separately. This approach arose from existing literature models, that do not necessarily guarantee the trustworthiness of data. The main trust sources used to evaluate user trust and data trust are direct trust, from previous knowledge, and indirect trust, from experience and reputation. To discover those trust relationships, the authors utilized a data schema based on collaborative filtering, which allowed identifying misbehaving entities' data. Even though the authors proposed multiple IoT implementation scenarios, they did not carry out any experiments to check framework performance.

Regarding IoT scenarios, other authors also contributed to the improvement of trust models and/or trust management frameworks such as [19–21]. First, Fernández-Gago et al. introduced in [19] a dynamic trust model which helped to overcome the lack of certainty in IoT scenarios by means of trust, privacy, and security requirements. In order to develop their framework, the authors presented a 4-layer architecture that covered paramount phases of conventional trust models. At the bottom, the scenario layer identified enforcement IoT contexts. Then, the requirement layer detected crucial functional and non-functional requirements related to the context, following the service layer included services such as interoperability, dynamicity, and evolution of trust model. And finally, the trust layer included services packaged

Table 1 Security and trust model approaches comparison

Proposal	Year	Application scenario	Zero-touch based	Algorithms	Features	Implementation
[18]	2017	IoT	No	Collaborative filtering	Data properties	No
[19]	2017	IoT	No	–	Trust, privacy, identity, and functional requirements	No
[20]	2018	IoT	No	–	Verifiable belief-driven trust, statistical evidence-based trust, complex system-wide cognitive trust	No
[21]	2019	IoT	No	Own algorithm	Compatibility, honesty, and competence	No
[22]	2017	Cloud computing	No	RBAC and own equations	User's behavior, security policies	Yes, two cloud environments
[24]	2018	Cloud computing	No	Fuzzy based approach	Detecting attacks on user's feedbacks	Simulation
[25]	2020	SDNs	No	Own algorithm	Reputation, operational risk, information risk, and privacy level	Simulation
[26]	2020	SDNs	No	Own algorithm	Network performance	Yes, Mininet
[27]	2017	Blockchain	No	IFT	Data credibility, node stability	Simulation
[14, 28]	2018	5G network slices	No	MDS, *k*-means, and bisecting-*k*-means	Security properties from data flows	Yes, 5GENSURE
[15]	2019	5G and beyond 5G networks	Yes	Anomaly detection	Security Service Level Agreements, network slice properties	Ongoing, in INSPIRE-5G Plus project
[16]	2019	Network slice beyond 5G	Yes	–	Network slice properties, SLAs	Ongoing, in MonB5G project
[13] Ours	2019	5G and beyond 5G networks	Yes	Bayesian networks, Markov network, Fuzzy theory	Smart Contracts and Service Level Agreements, resource and service monitoring data, security properties	Ongoing, in 5GZORRO project

into a workflow-oriented development framework. Nonetheless, this approach did not carry out experiments on the proposed scenarios, so it can be interpreted as a fully theoretical approach. Second, Liu and Loper provided in [20] certain guidelines to create a trust evaluation framework for distributed IoT system management. Like the previous proposal, this framework was composed of multiple parts, specifically six core components. The authors of [20] pointed out a threat model, which considered common trust attacks, a feedback rating component, which gathered and calculated feedback scores based on experiences, and a trust model, which contained algorithms to compute a final trust based on feedbacks. In addition, the authors incorporated a decentralized technology like blockchain which supplied not only security through transaction encryption but also integrity by means of immutable records. Nevertheless, this approach was only a vision of Trust as a Service (TaaS), and hence it is a methodical approach. Last, Awan et al. addressed in [21] an important research into cross-domain trust management for IoT ecosystems. Due to the low capacity of IoT devices, the authors split domains into multiple communities based on similarities and interests. Each community had an architecture based on three central authority servers: (i) the domain server to guarantee a security domain, (ii) the community server to ensure intra- and inter-domain communications and to reduce threats, and (iii) the trust server to manage trust values and to assess trust scores. Regarding trust, this article leveraged a reputation-based trust approach, which was composed of direct trust (from previous interactions) and indirect (from recommendations) trust parameters. Furthermore, trust management was interpreted as a continuous and dynamic process due to trust changes over time, and therefore, either nodes or server updated and shared trust values between the community or the domain, depending on node's interaction. Accordingly, the authors carried out a theoretical investigation, through these three-layer security servers plus trust scores of each node, to finally propose a secure and trustworthy system considering the performance of IoT resource-constrained devices.

Apart from IoT scenarios, where trust models are thoroughly applied, other conventional areas such as cloud environments and network scenarios are considering trust as a paramount mechanism. First, Uikey and Bhilare worked on an innovative role-based access control model based on trust management [22], which could be employed in cross-domain cloud environments. In this case, trust is calculated from direct experiences and recommendations, being features of both dimensions stemming from a set of security policies. Additionally, the framework introduced two trust evaluation mechanisms, depending on single or multi-domain establishment. Note that this approach computed two trust scores when an entity established a multi-domain relationship, one assessed from its own domain and another from the new domain. In the end, the authors contrasted the performance of access control model-based trust management against traditional Role-Based Access Control (RBAC) models [23], providing the former a higher success rate. In [24], the authors analyzed the trustworthiness of user's feedbacks to ensure accurate evaluations through identifying Sybil and collusive attacks. Thus, the main objective of this approach is to analyze the credibility of the feedback. The authors developed a Cloud Broker (CB) which helped the user to select the best Cloud Provider. CB is an intermediate entity between the user and the provider which receives user's feedback and contains a malicious filter, which analyses the feedback to discover previous attacks. In that sense, the authors established several own algorithms to find the attacks, where the conducted experiments depicted that the framework achieved an 89–95% success rate when malicious feedbacks were detected. Besides, the framework reduced high job failure rate as well as associated cost loss to the user in a cloud environment.

Second, Burikova et al. contemplated in [25] trust as a trust mechanism capable of improving certain absences in network environments. The authors aimed at covering the lack of trust between the Software Defined Network (SDN) controller and the network management applications, since this absence may provoke key security concerns in SDNs such as malicious traffic or an infected asset. Thus, they proposed a framework to establish and manage trust between the OpenFlow controller and the applications. The framework was composed of five crucial components: identity management modules, trust module, trust database, access control decision module, and dynamic monitoring and evaluating module. Regarding the trust module, they only considered direct trust, what was generated from reputation, operational and information risks, and privacy level. Besides, they proposed three zones (critical, surveillance, and trusted) where the tasks would be executed regarding their trust scores and the decision from the access control module. To this end, the authors developed a dummy controller, but they didn't produce any performance or accuracy results in their framework. Like [25], Yao and Yan also considered in [26] trust as a key element to be applied on SDNs. The authors leveraged trust to design a management framework that allowed evaluating applications' trust values. The main objective of this trust framework was to mitigate conflicts with utilization policies as well as discover attacks. The framework was mainly divided into two modules: Network Performance Monitor (NPM) and Trust Evaluation module (TE). The NPM module monitored network performance through flow rules issued by different applications, and then, monitoring data were labeled and sent to the TE module. This latter module calculated a final trust score from previous evaluations, current monitoring data, and controller's feedback. After weighing these values, the TE sent a final score to the control and data plane. Lastly, the simulated experiments (Mininet and OpenFlow) showed that the trust framework was effective, because trust evaluations needed less than 10 ms, and was accurate, since it can assess positively an application trust through adjusting parameter weighting based on each scenario.

Another enforcement of trust was contemplated by Li et al. in [27], who determined trust degrees of blockchain nodes to select a set of nodes with powerful communication skills and high trust scores. Thus, the trust value was defined by the credibility of the data held by a node and the stability of the node when regarding the data provided by other nodes. In order to carry out the node selection, they leveraged an integrated factor communication tree (IFT) algorithm. First, this algorithm sorted nodes from the largest to the smallest communication link values, and then, the nodes were again sorted by the trust degree value. After that, the authors defined three thresholds that allowed classifying nodes such as honest, free-ride, and malicious. Finally, they simulated multiple experiments that depicted this approach as reproducible and effective, as long as blockchain-based communication contained well-equipped nodes to cover the power capacity. In the same way, trust can be employed for end-to-end connectivity management and orchestration.

In the same research area, Suomalainen et al. proposed in [28] an adaptable and expandable framework for trust measuring and security control in 5G networks. This framework was based on a Trust Level Agreement (TLA) mechanism for sharing near real-time security awareness in multi-domain scenarios. The TLA mechanism was implemented by a trust metric enabler that allowed establishing trust communication following four easy phases. First and foremost, the trust metric enabler monitors the network for significant security events and measurements. In the case of security events, the trust metric enabler defines a set of services running on network slice, and for each one, it establishes a maximum and minimum level to measure its events associated (i.e., traffic statistics and authentication events). Second, a client requests a slice from the enabler, which will determine whether such the slice fulfills the client's trust demands. After that, the client and the service provider agree on using a given trust slice, and they establish a secure tunnel for communication. Finally, the trust metric enabler continues to acquire network information in order to notify the client about possible risks. This approach was covered by the 5G-ENSURE project [14], where a testbed composed of IoT devices and a video streaming application was used as the enforcement scenario.

In the light of the state-of-the-art proposals, no solution has been identified that allows not only to establish an end-to-end trustworthiness relationship in multi-tenant and multi-domain scenarios but also to contemplate security aspects, for instance, detecting operational and cyber-security threats from monitoring networks communications and guaranteeing privacy and integrity of cross-domain communications. In this vein, the security and trust framework design proposed in Sect. 4 endeavors to fill the above gaps identified in the literature solutions. Table 1 is summarizing the different research papers previously introduced and discussed, together with relevant indicators that define each proposal, thereby allowing a comparison between the diverse security and trust model approaches analyzed.

3 Multi-domain Threat Model

In modern multi-domain network scenarios, such as the one enabled by 5G, new security threats arise associated with the distributed nature of these environments, in addition to the already existing in earlier networking paradigms. Besides, modern technologies developed to deploy 5G networks (new SDN/NFV capabilities, cloud RAN, etc.) also bring new security threats to deal with. In addition, the interaction process between entities also carries a series of trust threats, threats that are more abstract than those related to security issues, but which can make entities interactions unfruitful for them.

The set of threats described in this section comes from two different perspectives, a first one related to multi-tenant trust relationships where each side has its own interests, and a second one aligned with the current security problems associated with distributed environments and their technologies. Despite the fact that the trust and security threats described below may mostly be associated with intra- and inter-domain scenarios, we want to contextualize them in a multi-tenant and multi-domain environment since this is the basis for 5G scenarios [29]. It should be noted that the multi-domain threat model described in this section has been considered as a motivation to design the security and trust framework proposed in Sect. 4, and consequently, it does not endeavor to cover all of them.

3.1 Threats in Multi-tenant Trust Relationships

When two or more entities interact in a network scenario under a business relationship, mutual trust is one of key factors in making a satisfactory relationship for all parties. Therefore, the trust level can influence such critical aspects as to whether a service is consumed or not, enabled actions, its price, etc. Therefore, malicious entities can try to jeopardize this trust for their own benefit, affecting the revenue of legitimate entities.

Traditionally, trust relationships have been ordinarily derived from the use of trust models. Even though such models have been continuously evolving, they are not exempt from being affected by multiple threats. In this regard, a security and trust framework ought to consider and address the potential threats to trust in these multi-tenant environments, ensuring their proper functioning. Despite the set of conventional trust threats is very widespread and even dependent on the context and design decisions of each trustworthiness framework, we have gathered a subset of threats related to multi-tenant scenarios. Thus, the most well-known threats related to trust are identified in these scenarios together with possible mechanism to be addressed:

- *Trust privacy and secrecy*. Normally, the trust value that an entity gives to another one is not published since the revelation of that value to the other parties can affect the trust relationship between the entities, as it can be asymmetrical (entities give different trust values to each other).
- *Subjectivity*. Trust is a subjective concept by nature, different entities might give different trust values to the same relationship based on their different criteria. This aspect is greatly influenced by indirect trust, coming from non-deterministic aspects such as reputation. In order to tackle the subjectivity issue, a solution might be to derive personalized trust values based on a comparison of users' trust attitudes [30], another one might be not to consider an absolute score but a standard score (z-score), or as a percentile [31].
- *Credibility*. The believability of data content or recommendations by trustees is another conventional risk linked to trust models. Usually, credibility involves veracity, objectivity, observational sensitivity, and self-confidence [32], and it is regularly measured by the level of uncertainty [33].
- *Bad-mouthing attack*. It is often associated with trust models that contemplate recommendations or feedback. This attack intends to dwindle the trustworthiness of honest entities and/or increase the trustworthiness of untruthful entities by means of deceptive recommendations, feedback, or votes [34].
- *On–off attack*. In this case, a misleading entity has a split personality. First, when an attacker has a low trust level, it behaves honestly to grow its trust score over

a period. Then, once the attacker gets into a certain trust level, it adopts a deceptive behavior until the trust score returns to a low level [35].

- *Conflict behavior attack.* This attack occurs when the attacker is capable of providing different trust recommendations in different domains or times. In this sense, attackers cause conflicts with usual entities since they damage the confidence in recommendations of honest users [36].
- *Collusion attack.* It is a joint attack where a group of attackers selects a target on which to focus their dishonest recommendations [37]. Consequently, they control the trust value for the target through a set of negative recommendations, in an organized and orchestrated manner, so that an honest entity would see its trust score dwindled.
- *Sybil attack.* This attack is performed by malicious entities which intend to control the reputation of other honest entities involved in trust model in order to influence their trust estimations. By means of this attack, an attacker may take multiple bogus identities to steer certain actions from an honest entity, for instance, the redirection of network traffic toward a spiteful entity for performing exploitations [38].

As it can be appreciated from the previous list, there are many type threats that might affect trust from different perspectives. For that reason, solving or mitigating the existing threats is a critical issue when it comes to creating a properly functioning network environment, so that the potential malicious elements are clearly differentiated from the legitimate ones. Moreover, in the 5G-enabled distributed environments, these threats suppose an even higher risk to the environment, as the multiple network elements deployed are controlled by different decentralized entities, which prevent their unified management when trying to mitigate the threats. In this context, it is essential to develop new trust frameworks that take into account the trust threats in modern networks, and to make use of state-of-the-art technologies, such as Machine Learning (ML) and Deep Learning (DL), to mitigate and address these threats. In particular, this paper intends to address the collusion attack and the Sybil attack in spite of the fact that we do not currently have a definitive approach to tackle them. Furthermore, the other threats described above are intended to be covered in future iterations to introduce a robust and secure framework to the community.

3.2 Threats in Multi-tenant Network Environments

In 5G networks, it is usually necessary to combine network infrastructures located at different domains to reach the required Quality of Service (QoS) targets, thus creating multi-tenant network environments. These environments are mostly enabled by network slicing solutions. Nevertheless, network slicing carries its own security threats, as slices are formed by leveraging different parts of the 5G infrastructure. Each network part is subject to specific Tactics, Techniques and Procedures (TTPs) for interrupting its normal behavior. We hereby detail the TTPs that are relevant for each 5G network part:

- *Core*: SDN and NFV mechanisms (e.g., controllers), together with the Management and Orchestration (MANO) and Virtualized Infrastructure Manager (VIM), are exposed to remote access threats [39]. These threats normally are manifested when malicious users exploit a given vulnerability that provides remote access for maintenance and troubleshooting. This remote management is especially useful for components that are situated in distant and harsh locations. Additionally, an adversary can alter the settings of MANO or compromise the isolation between network functions. Sometimes, network slicing implementation or the absence of proper isolation mechanisms can lead to malicious infiltration in tenant slices. Malicious users may cause resource exhaustion as well as sensitive data disclosure [40].
- *Access network*: The insecure nature of 5G radio access systems may lead to frequent Address Resolution Protocol (ARP) poisoning attacks [41]. In such attacks, the adversary tries to associate its MAC address with the IP address of a legitimate 5G component, causing any traffic meant for that IP address to be sent to the attacker instead. Another significant threat to the 5G access network is radio flooding [42], occurring when transmission of data requests is sent to exhaust resources. This can subsequently lead to a reduction or even a complete shutdown of the radio resources provided by the component.
- *Transport network*: The transport part of 5G networks is where the main data exchange occurs, and it is supported by backhaul solutions. These solutions include satellite, fiber optics, micro-waves, Ethernet, and wireless communication. Usually, TLS is used to encrypt the exchanged data, however, recently discovered vulnerabilities (i.e., CVE-2020–1596) in the TLS hash algorithms can be leveraged to decrypt the original TLS traffic and eavesdrop on the enclosed information [6].
- *Multi-access edge computing (MEC)*: The use of MEC platforms can offload part of the processing to improve latency and performance as they are deployed closer to the User Equipment (UE), in base stations. However, adversaries often use MEC platforms as a further attack vector that can be flooded with a request or directed traffic. Furthermore, MEC platforms usually employ APIs to interface resources and services, such as gateways, sensors, or actuators [43]. Since these APIs are open, they may be exploited by adversaries to gain access to the MEC platform.

Mitigating each of the above threats is vital for a proper 5G infrastructure operation, and hence no prioritization among them is considered. For successful detection and prevention, the system should consider a sequence of actions that

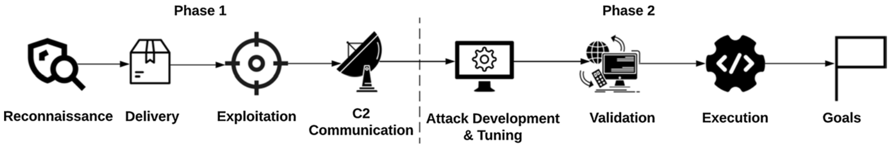


Fig. 1 Multi-tenant environment attack phases and associated steps

are followed by adversaries when performing their attack. These actions are illustrated in Fig. 1.

Specifically, attack actions are divided into two distinct phases. The first one concerns the cyber intrusion preparation for initial access to the 5G network, and the second phase refers to the attack development as well as its execution on the multi-tenant environment. The first step has the purpose of eavesdropping information [44] about the system, learning its behavior (*Reconnaissance* in Fig. 1) and developing methods to evade internal perimeter protections or security mechanisms, in order to gain access to the 5G infrastructure (*Delivery*). This usually involves potential inefficiencies that are leveraged as entry points to the 5G infrastructure (*Exploitation*) as well as communicating to external servers the information about the victim, and also download from them attack data (*C2 Communication*). As an example, an adversary can penetrate the enterprise network, eavesdrop on 5G connections, and use potential inefficiencies as entry points to the 5G infrastructure. Inefficiencies are often exposed by architectural complexity.

The second phase in Fig. 1 seeks to cause interruption of the multi-tenant environment normal operation. As each 5G infrastructure uses its own communication protocols and commands for controlling the system operation, an adversary requires this phase to cause a meaningful impact on the system. Such impact is caused by developing the attack (*Attack Development & Tu*ning in Fig. 1) and validating it on similar or identically configured systems (*Validation*). This is usually a long-lasting period and during its course, the adversary maintains access to the system. When the attack is fully developed and validated, it still has to be executed in the multi-tenant environment (*Execution*). Upon effective execution, the attack is considered as successful.

If an adversary manages to successfully execute the above sequence of attack actions, a direct impact on the creation of the multi-domain network slices can be caused. Therefore, a resilient security architecture should cover all the 5G infrastructure as well as the multi-tenant and multi-domain scenarios. In addition, the detection and protection mechanisms against sophisticated and zero-day threats [45] need the combination of new security solutions at various levels, both within an administrative (i.e., resource owner) domain as well as cross-domains (i.e., the interconnection with other domains).

4 Multi-domain Security and Trust Framework Design

As seen in the previous section, multiple security and trust threats may appear in a multi-domain network scenario. Thus, it is essential to produce a security and trust management framework capable of addressing these threats, leveraging prevalent state-of-the-art technologies and following a holistic approach.

Even though security aspects covered by multi-domain networks involve a wide variety of mechanisms and techniques that might be introduced in a generic framework, such as AAA (Authentication, Authorization, and Accounting), firewalling, detection and mitigation attacks, these are already well studied and addressed by other good practice approaches, as [46, 47]. Hence, it is not considered within the scope of this paper. In the paper, the focus will be on addressing the issues related to the lack of security and trust models in the 5G ecosystem, as well as some ways for mitigating the effect of some threats mentioned above if they realize. Additionally, a real deployment scenario from the 5GZORRO ecosystem will be presented, and there the security and trust framework will be instantiated to showcase trustworthiness and a protected landscape.

4.1 End-to-End Security and Trust Framework

The security and trust framework, which will be used by the 5GZORRO platform, provides an innovative mechanism to orchestrate end-to-end trust establishment and secure communications, in multi-tenant and multi-stakeholder scenarios. The requirements dictate the way in which 5GZORRO platform will be conducting security and trust across domains, both at business level and at system level. The former entails identity and permissions management (IdM), security and trust policy definition, etc., while the latter brings secure connectivity with third party resource using Generic Routing Encapsulation (GRE) or Virtual Private Network (VPN), Virtual Trust Domain establishment based on Trusted Execution Environments, among others. These requirements are the ones that will determine the selection of defensive mechanisms. This section will also look into methods to assess and respond to potential vulnerabilities that intend to undermine the trusted execution of workloads, offloaded across multiple domains. In addition, this section also brings a transversal concept like zero-touch, which plays a key role in allowing the integration of the security and trust framework with existing solutions in 5G networks. The process automation leads in a certain way to guarantee a higher security and trust level in the processes and environments which is precisely covered by a crucial concept considered in our framework, the zero trust principle [11].

From a high-level point of view, the security and trust framework can be perceived as the composition of three distinctive modules: trust management, intra-domain security, and inter-domain security (see Fig. 2). They intend to cover trustworthiness and ensure a protected environment where the 5GZORRO platform resides. Specifically, the *Trust Management* module increases the trust level of multi-domain environments, the Intra-*domain Security* provides a detection and protection layer inside each domain, and finally, the *Inter-domain Security* focuses on protecting communication channels between domains. Even though these modules are instantiated and deployed as separate entities, these modules may require

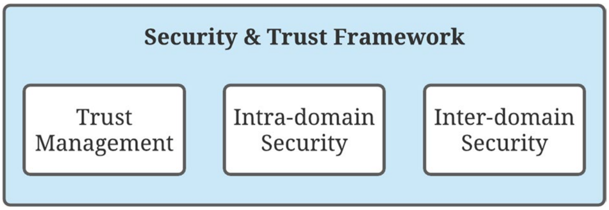


Fig. 2 Overview of the security and trust modules

information from other to carry out their activities. In this vein, the proposed framework leverages a back-end database (Data Lake) to share non-sensitive information that other modules can use through a publish and subscriber mechanism (Kafka). Next, the three modules are described thoroughly below.

4.1.1 Trust Management

The Trust Management module is responsible for establishing end-to-end trustworthiness across distributed environments belonging to different stakeholders, such as the ones proposed by the 5GZORRO project, service or resource providers and service or resource consumers. Trust is a key element when defining and establishing commercial relationships between two or more partners. The fact of trusting (or not) other parties influences which partners are chosen for business relations and under which conditions. Factors that can influence trust or the lack of trust are, for example, the presence of trust-based resources in the infrastructure, service access control, or sensitive information execution. Therefore, this is a paramount element when trading resources and services allocated at a third-party infrastructure, one of the main environments in which 5GZORRO operates.

The essential functionality of the 5GZORRO Trust Management module is to control the entire life cycle of trust establishment for relationships among different entities: from the selection of the information sources to be used to the algorithms for calculating and updating the trust values, and finally, the improvement of the current calculation models and mechanisms. Additionally, this module also gathers indirect trust information derived from the relationships between two external stakeholders and the one doing trust calculation, generating a trust link between stakeholders based on their shared commercial relationships and interactions. Another characteristic of the 5GZORRO Trust Management module is its commitment to a zero trust approach driven by the NIST [11]. Zero trust means that there is no implicit confidence granted to stakeholders, regardless of whether they are located under their own domain. Due to the fact that the proposed Trust Management module enables both intra- and inter-domain connections, zero trust plays a pivotal role to cope with probable entities within our organization that were attacked and are behaving inappropriately. In this regard, the zero trust principle is one of the utmost relevant in the trust area since trust by default may be one of the attack vectors. Considering the zero trust principle, the proposed Trust Management will not consider previous trust scores calculated as valid for establishing a new relationship between entities and will require a trust score to be calculated for any internal or external relationship establishment.

In this vein, the Trust Management module operates following four generic phases with a logical order, which will be described below. It is worth mentioning that Fig. 3 describes the interrelationships of how calculations are performed. Hence, the Trust Management life cycle will start in the *Trust information source module* that will begin a continuous trust information collection process from multiple available sources (see the left side of Fig. 4). Then, such information will be sent toward the *Trust calculation module* in which a trust score will be determined, taking into account the information gathered in the previous module

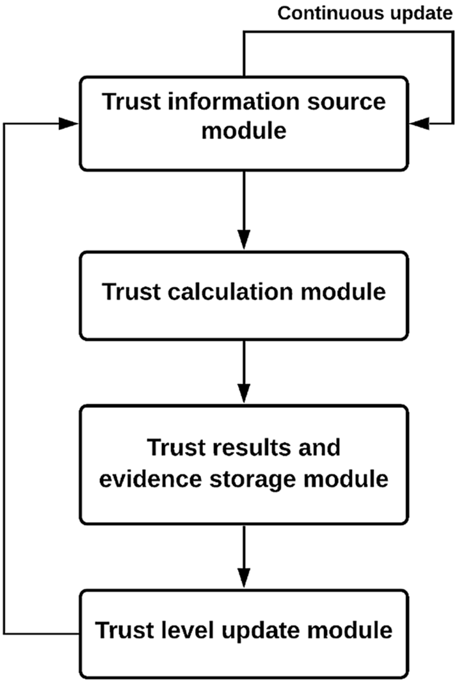
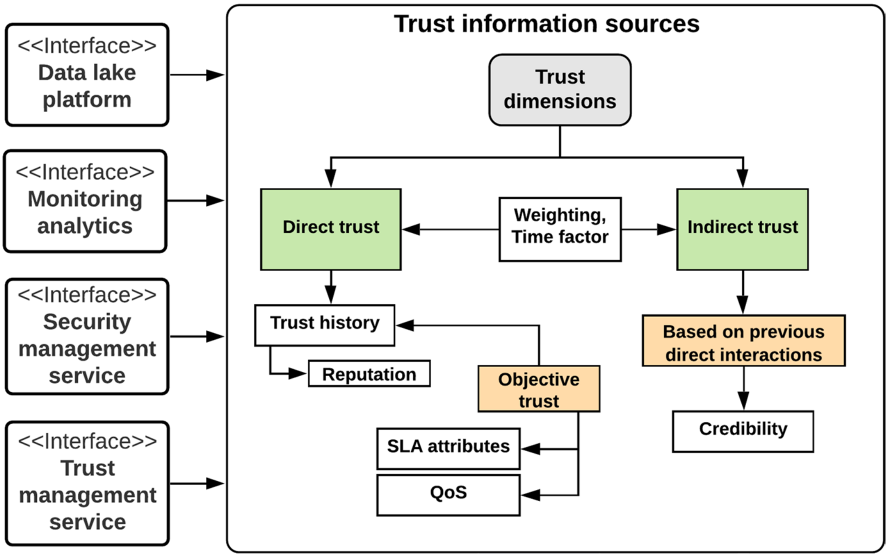

Continuous update
Trust information source module
Trust calculation module
Trust results and evidence storage module
Trust level update module

Fig. 3 Principal Trust Management modules

as well as ML/DL algorithms. After that, the information collected in the *Trust information source module* and the information inferred from the *Trust calculation module* will be stored via the *Trust results and evidence storage module* so as to keep track. Finally, the *Trust level update module* will be triggered to detect certain events which imply a trust score recalculation.

4.1.1.1 Trust Information Source Module The initial phase concerns information gathering from trusted sources. This is a fundamental step that will have a direct impact on the next trust model phases, and on the produced output. In that sense, the Trust Management module ought first to find what are the available information sources. For the 5GZORRO ecosystem, there are multi-tenants and multi-stakeholders that make use of Smart Contracts (SCs) and SLAs, which are based on Distributed Ledger Technologies (DLT). Moreover, the SLAs are used to track breaches based on the initial SC agreements. These smart contracts are in turn stored in a secure and immutable network (DLT) that can be consulted by any 5GZORRO stakeholder. In this ecosystem, there are three main sources for trust calculation, depicted at the left side in Fig. 4, as input to the Trust Management module, from which to derive and infer features: the shared Data lake platform, the Monitoring analytics, and the Security management service. Once information sources have been determined, the Trust Management module will generate a set of trust features from that information.



<<Interface>> Data lake platform
<<Interface>> Monitoring analytics
<<Interface>> Security management service
<<Interface>> Trust management service
Trust information sources
Trust dimensions
Direct trust
Weighting, Time factor
Indirect trust
Trust history
Reputation
Objective trust
Based on previous direct interactions
Credibility
SLA attributes
QoS

Fig. 4 Trust information sources module

As shown in Fig. 4, trust models are mainly composed of direct trust and indirect trust, components located at the *Trust information sources* in the figure. On the one hand, direct trust is the information that has been gathered from direct interactions (trust history) with the entity from which it is intended to calculate its trust level. Through time, a stakeholder builds reputation information about other stakeholders, i.e., collects different trust assessments with the same entities to have an estimation, or a reference, on how future trust relationships could be. This way the Trust Management module considers objective properties to compute direct trust, such as SLA attributes or QoS properties, in order to avoid subjectivity problems. On the other hand, indirect trust is computed when an external entity, not directly involved in the current trust establishment event, provides information about one of the actors (trustee) involved in the relationship to be established. However, the trustor must have previous relationships with the intermediate entity. Since this information source involves feedback from other entities, it is necessary to determine how trustworthy the reply is, also known as, recommendation's credibility. Therefore, credibility will also be a factor directly linked to indirect trust.

4.1.1.2 Trust Calculation Module Once all parameters have been gathered, from direct and indirect trust sources, the *Trust calculation* comes into play. It makes use of common algorithms from literature. On top of those, a set of ML-based algorithms are applied, though the selection of the ML/DL algorithm is based on the scenario characteristics and features. Nonetheless, Fig. 5 introduces some of the most conventional intelligent techniques such as Fuzzy theory, Bayesian networks, Markov networks, and so on. Note that the final trust score should withstand, at

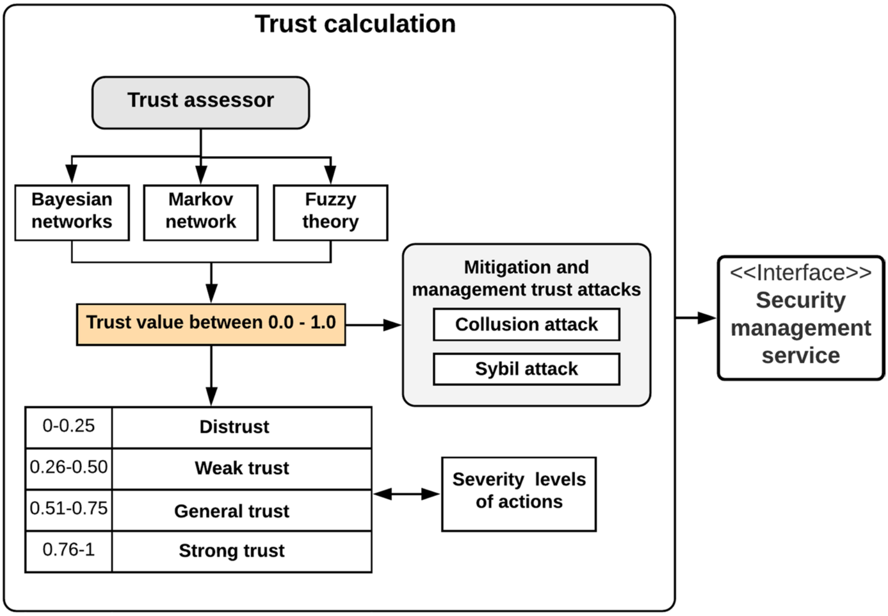


Fig. 5 Trust calculation module

least, two of the main attacks that trust models often suffer, such as collusion attack (unrealistic or biased recommendations) and Sybil attack (multiple identities, associated with the same entity, increase/diminish reputation). Due to the fact that the proposed Trust Management is in an early development stage, more testing is needed, nevertheless, we are contemplating credibility as possible technique to distinguish deluding trust (collusion attack) [48] and fuzzy-based mechanisms to prevent Sybil attacks [49]. To avoid problematic subjectivities from indirect trust (known as recommendations), the 5GZORRO Trust Management module utilizes percentiles as a metric by which a trustee provides recommendations to a trustor. Thus, a relative quantity is used instead of absolute values, when estimating recommended trust. A percentile value indicates trustee's perception of another entity in relation to the other recommendations that the recommender has rated in the past. Lastly, the trust calculation phase also considers both sensitive information and which actions will the stakeholders be able to perform once the trust relationship is established. This consideration provides a final trust score according to the properties of each situation.

4.1.1.3 Trust Results and Evidence Storage Next, when trust has been calculated, it is time for the *Trust results and evidence storage* module (see Fig. 6). To keep a time-based tracking, either data lakes or SQL/No-SQL databases will be used to store the output of the trust calculation model. They will maintain both a trust history and some of the information, considered public, to have recommendations available for future stakeholders. The selection of the storage source will be decided based on the type of information. For the case of sensitive information, it will be stored in a local

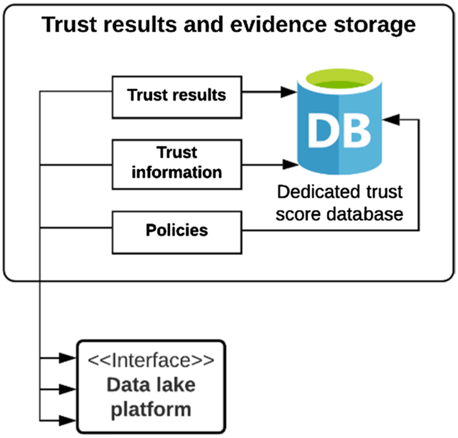


Fig. 6 Trust results and evidence storage module

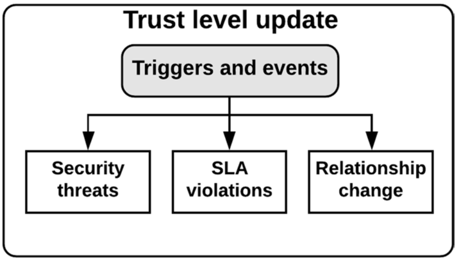
repository where only stakeholders of its domain can access the information. For the non-sensitive, more options are available. Besides the functionality described previously, note that local repositories (SQL/No-SQL databases) will also host intra- and inter-domain policies, which enable large-scale adaptive systems that dynamically change their behavior in response to changing environments or requirements. Otherwise, in case the information can be shared with other stakeholders participating in the 5GZORRO platform, such information will be stored in a shared data lake.

4.1.1.4 Trust Level Update As a last remark, note that the *Trust level update* module is a process that will run constantly since trust is a dynamic concept, which changes over time. It is paramount to identify a set of events that can be used as triggers for updating the current trust value. Security threats, SLA breaches, and relationship changes are considered as a set of candidates to trigger trust re-calculation of an active relationship (see Fig. 7).

4.1.2 Intra-domain Security

This module aims to offer security services in charge of detecting possible vulnerabilities and attacks, and apply the required countermeasures to mitigate the adverse events. The scope of this module covers an intra-domain perspective, where

Fig. 7 Trust level update module



each stakeholder deploys the services enabled by this module to enhance internal resource and service security. Besides, the deployment of this module in the internal organization infrastructure also improves the external trust from other stakeholders, as these services can be seen as an additional security guarantee for possible delegated resources or services.

The Intra-domain Security module allows the detection of operational and cyber-security threats based on evidence that originates from monitoring network communications. To this end, operational threats relate to failures or malfunctions, whereas cyber-security threats relate to malicious activity, abuse of the 5GZORRO platform components or disrupt network communications [50, 51]. Moreover, network communication monitoring is applied in (i) the modules, resources, and services inside each domain, and (ii) the 5G network infrastructure, i.e., mobile core with NFV MANO, RAN, or mobile edge. For the former, intra-domain communications occur through a network bus, which implements all the protocols and APIs to allow module interconnectivity. This bus is called intra-domain network fabric and allows different communication types, such as synchronous, asynchronous (event-based), point-to-point, or brokered communications. Furthermore, the latter requires access to the network packets that are exchanged into different layers of the 5G infrastructure. The high-level architecture of this module is shown in Fig. 8.

The first component of Fig. 8 is the *Packet Analyzer*, which is using a virtual SPAN (i.e., port mirroring) configuration or network probes on network elements as switches, gateways, and routers to collect network traffic data and control commands for each domain. Since traffic data and control commands can be sent either in standardized or proprietary formats, it also includes dissector modules for interpreting them. These network protocols are the ones used in (i) the *5G Network infrastructure* (e.g., Core, RAN, and Edge) as well as (ii) the *Intra-domain communication fabric*.

For the detection part, it focuses on both known and unknown (zero-day) threats, by employing three main threat detection mechanisms, depending on the type of threat:

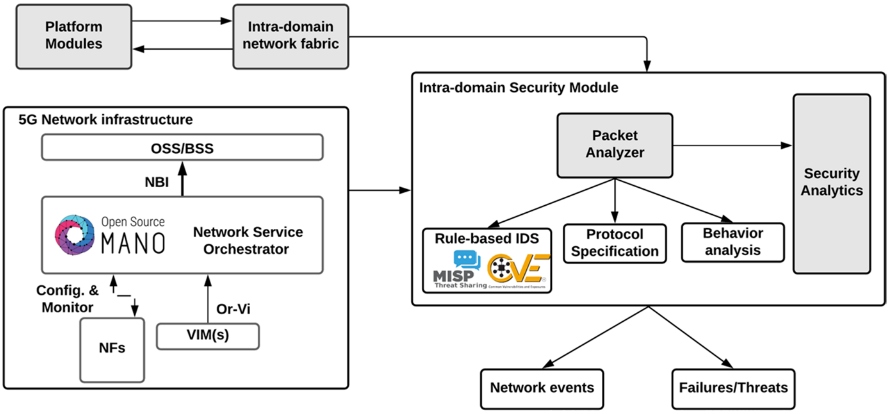


Fig. 8 The Intra-domain Security module architecture

- Rule-based: following a set of predefined rules and signatures for detecting known threats. The required inputs for this mechanism are obtained by Threat Intelligence platforms, as the Malware Information Sharing Platform (MISP) [52] or vulnerability databases as MITRE CVE [53].
- State-based: following the specifications of the network protocols that are used to communicate between the intra-domain modules and to detect anomalies when unusual message sequences, unsupported commands/codes, and error or unsupported messages are spotted. Since many protocols lack a dedicated specification or their specification is only proprietary, this module may require reverse engineering actions for interpreting commands that are inside the exchanged packets.
- Behavior-based: using ML techniques to learn the intra-domain behavior by analyzing network data and forming a baseline upon which the detection of anomalies (including zero-day threats [45]) is feasible.

The *Security Analytics* module uses the collected data from the *Packet Analyzer* to produce data for analytics and visualizations, as well as to retrieve Indicators of Compromise (IoC) that are useful for the investigation of failures or threats. Moreover, since the Intra-domain Security module includes zero-touch automation capabilities, that facilitates management of complex systems in which operators may resort to utilize resources from other domains and allows operational processes and tasks to run automatically, the *Security Analytics* module allows integrating prevention and mitigation plugins (i.e., mechanisms and procedures). Such plugins enable the 5G infrastructure and multi-tenant environment to adapt, with the aim of applying countermeasures to potential attacks, for instance, brute force, privilege abuse, flooding, malicious logic insertion, bypassing physical security, etc. Prevention and mitigation plugins can be linked to the integration of firewall policies, blocking unauthorized entities and compromised assets from accessing the 5G network, or also isolating affected resources in a separate VLAN. Overall, these plugins define a closed loop architecture according to the ETSI Zero-touch network and Service Management (ZSM) [12] and since they perform active modifications on the 5G infrastructure, they also require stakeholder (e.g., MNOs, tenants, or CSPs) permissions.

4.1.3 Inter-domain Security

This module is tasked with establishing secure and trusted connections between different domains in the 5GZORRO environment, guaranteeing privacy and integrity without sacrificing performance. The Inter-domain Security module has a significant importance when it comes to performing network slicing and when integrating into domain networks, the resources leased from the marketplace and located in a third-party infrastructure. Thence, the Inter-domain Security module plays a pivotal role to avoid communication risks, which is the key objective. But before describing the process of establishing secure communication channels, it is important to introduce two key elements which play a significant role in the Inter-domain Security module, the Decentralized Identifier (DID) and the Verifiable Credential (VC).

A DID [54] is a new type of identifier, globally unique, resolvable with high availability, and cryptographically verifiable. DIDs are typically associated with cryptographic material, such as public keys and service endpoints, and they are used for establishing secure communication channels. The DID infrastructure can be thought of as a global key-value database in which the database is all DID-compatible blockchains, distributed ledgers, or decentralized networks. In this virtual database, the key is a DID and the value is a DID document. The purpose of the DID document is to describe the public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically verifiable interactions with the identified entity. In this regard, DID documents often leverage VCs to demonstrate claims. Thus, a VC [54] describes a privacy-preserving and tamper-evident credential (sort of claims) that can be demonstrated through a cryptographic process. The addition of technologies, such as digital signatures and distributed ledgers, makes VCs more tamper-evident and more trustworthy than their physical counterparts.

After introducing these technologies, it is time to explain how the Inter-domain Security module makes use of them, when setting up an innovative and reliable VPN between domains. The Inter-domain Security module uses the cryptographic material present in the DIDs, to derive shared keys between the elements located in different domains, and to establish a VPN-type connection that integrates these resources and services in the purchasing domain.

Figure 9 depicts all the steps involved in establishing secure cross-domain communication channels where 5G Operator A realizes that it is not able to fulfill the performance levels indicated in its SLA, and therefore, checks the marketplace for available resources/services to expand its current capabilities. If it finds the needed

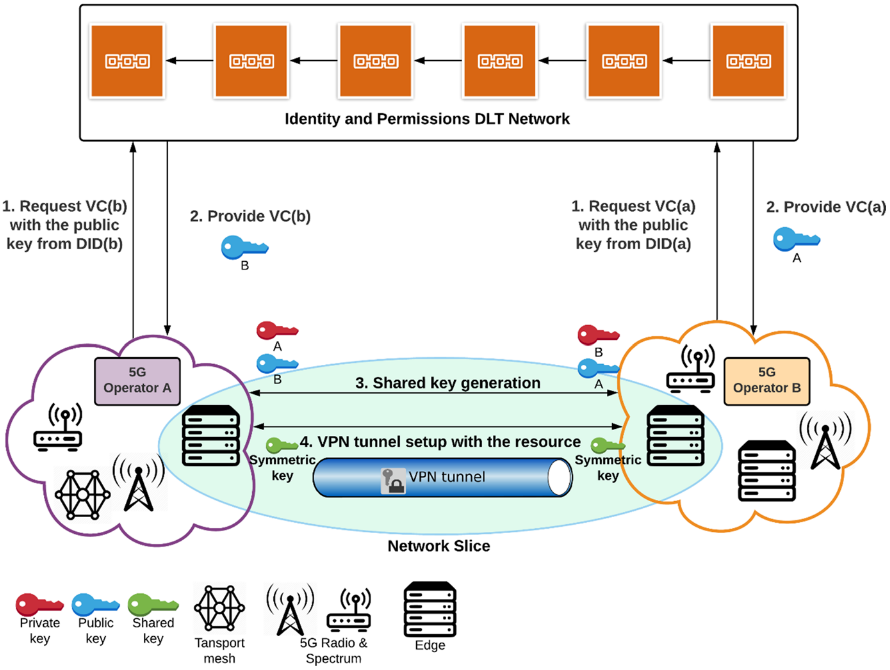


Fig. 9 5GZORRO inter-domain secure establishment

resources, it selects one of them and a Smart Contract is produced to reflect the transaction with 5G Operator B. After that, both operators request each other's public key to start the establishment of a secure and private communication channel. Since 5GZORRO leverages the DIDs and VCs when identifying, authenticating, and authorizing stakeholders, services, or resources, these may also be utilized as the asymmetric keys to derivate symmetric key pairs for a VPN tunnel (steps 1 and 2). Therefore, 5G Operator A is starting the VPN configuration process, by initiating a process called the shared key generation. By using 5G Operator B's public key, which was acquired from its VC (IdM DLT network), 5G Operator A forwards an authenticity proof to 5G Operator B (step 3). If the answer is satisfactory, 5G Operator A will generate and send a symmetric key to 5G Operator B, which will be subsequently utilized to securely and confidentially share information. Finally, the VPN configuration process will be finished, and the VPN will be set up with the purchased resources (step 4).

4.2 A Real Enforcement Use Case by 5GZORRO

After proposing and describing the components for a security and trust framework, this section describes how that framework will be a good fit for a real deployment scenario.

The 5GZORRO project aims to provide a framework for automated network management and cross-domain services. In this regard, security and trust are keys to succeeding in the goal. 5GZORRO often operates in multi-stakeholder environments and the project leverages on NFV, SDN, and service-based architecture to implement 5G networks, offering seamless end-to-end 5G service management. The project provides a Marketplace in which stakeholders can trade resources and services, in order to keep with the demanding dynamic requirements associated with 5G networks. The novelty here is the fact that an operator can lease on-demand resources and services located on third-party premises/infrastructures combining zero-touch automatization solutions and ensuring zero trust principles in distributed multi-stakeholder environments. Hence, these resources can be deployed and managed as their own, using zero-touch resource and service orchestration, for automated slice provisioning. Furthermore, another novelty here is the concept of *security intents* [55] that enable an operator to finally select, through intelligent resource and service discovery applications, a third-party that fulfills its security requirements.

The focus of this section will be on presenting how the proposed security and trust framework, which is composed of three different modules, integrates into an automated process of slice management and resource orchestration, involving resources belonging to different network domains.

Figures 10, 11, and 12 illustrate the proposed 5GZORRO business flow for trustworthiness and secure end-to-end slice establishment, from the moment the entity uses the marketplace to search for the resources offered in other domains, all the way until the moment in which the slicing process with the acquired resources has been completed. But to understand Figs. 10, 11, and 12, we first provide a brief explanation of the entities involved in the end-to-end slicing process:

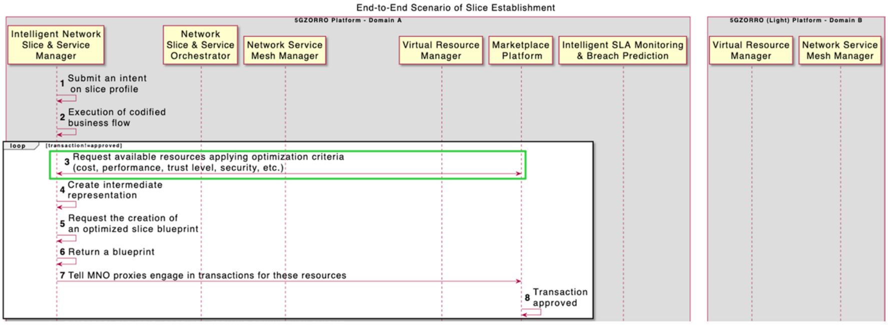

End-to-End Scenario of Slice Establishment
5GZORRO Platform - Domain A
5GZORRO (Light) Platform - Domain B
Intelligent Network Slice & Service Manager
Network Slice & Service Orchestrator
Network Service Mesh Manager
Virtual Resource Manager
Marketplace Platform
Intelligent SLA Monitoring & Breach Prediction
Virtual Resource Manager
Network Service Mesh Manager
1 Submit an intent on slice profile
2 Execution of codified business flow
loop [transaction!=approved]
3 Request available resources applying optimization criteria (cost, performance, trust level, security, etc.)
4 Create intermediate representation
5 Request the creation of an optimized slice blueprint
6 Return a blueprint
7 Tell MNO proxies engage in transactions for these resources
8 Transaction approved

Fig. 10 Trust Management module enforcement in 5GZORRO simple end-to-end scenario of slice establishment (Color figure online)

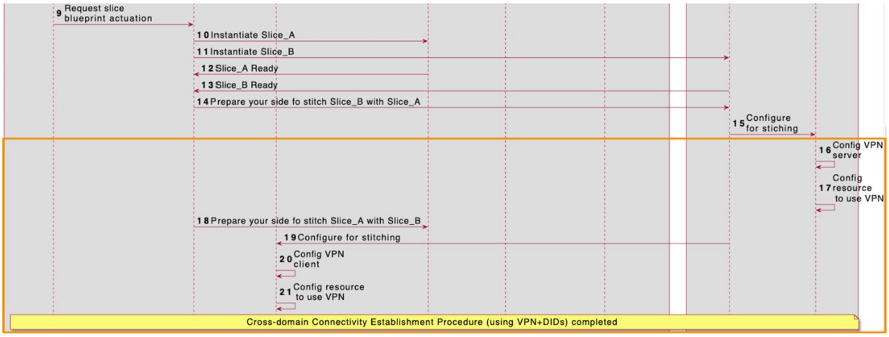

9 Request slice blueprint actuation
10 Instantiate Slice_A
11 Instantiate Slice_B
12 Slice_A Ready
13 Slice_B Ready
14 Prepare your side fo stitch Slice_B with Slice_A
15 Configure for stiching
16 Config VPN server
17 Config resource to use VPN
18 Prepare your side fo stitch Slice_A with Slice_B
19 Configure for stitching
20 Config VPN client
21 Config resource to use VPN
Cross-domain Connectivity Establishment Procedure (using VPN+DIDs) completed

Fig. 11 Inter-domain Security module enforcement in 5GZORRO simple end-to-end scenario of slice establishment

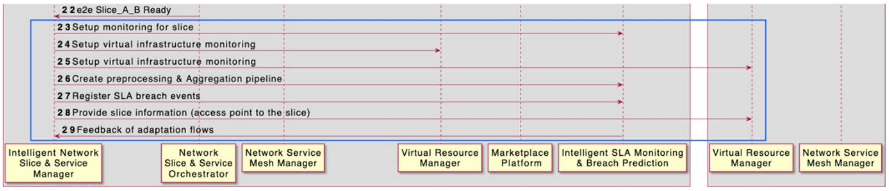

22 e2e Slice_A_B Ready
23 Setup monitoring for slice
24 Setup virtual infrastructure monitoring
25 Setup virtual infrastructure monitoring
26 Create preprocessing & Aggregation pipeline
27 Register SLA breach events
28 Provide slice information (access point to the slice)
29 Feedback of adaptation flows
Intelligent Network Slice & Service Manager
Network Slice & Service Orchestrator
Network Service Mesh Manager
Virtual Resource Manager
Marketplace Platform
Intelligent SLA Monitoring & Breach Prediction
Virtual Resource Manager
Network Service Mesh Manager

Fig. 12 Intra-domain security module enforcement in 5GZORRO simple end-to-end scenario of slice establishment

- *Intelligent Network Slice & Service Manager* This functional entity is tasked with the automatic management of network slices into its own domain, or when the operator needs to extend its reach into other domains. This entity gathers monitoring data to produce intelligent analytics with the aim of proactively adapting the system due to constantly changing contexts.
- *Network Slice & Service Orchestrator* Functional entity responsible for the deployment of network slices. This same entity orchestrates network services which can be provisioned on the intra- or inter-domain network slices.

- *Network Service Mesh Manager* It handles the service meshes to provide connectivity for network services (service discovery, service routing, and service connection management).
- *Virtual Resource Manager* Its main goal is to monitor the status of the managed entities and push monitoring data to the Intelligent Network Slice & Service Manager. Furthermore, this component is divided into three elements: service and resource monitoring, virtual resource management and control, and radio resource management and control.
- *Marketplace Platform* It is an instance of the marketplace, anchored to one Marketplace DLT node. This component allows trading 5G resources and services through a decentralized catalog, taking advantage of the DLT technology. Each resource and service offered by the marketplace has a unique and global identifier, to be quickly and easily identified. These identifiers (DIDs) are then used to perform other actions such as establishing a secure end-to-end connection.
- *Intelligent SLA Monitoring & Breach Prediction* This functional entity is made up of two key services. Its main objectives are to gather and examine aggregated monitoring data to identify SLA breaches by using AI techniques. Then, the Marketplace and the appropriated Smart Contract (SC) are notified, and the SC recalculates SLA status.

The proposed security and trust framework (highlighted in a green box in Fig. 10) will interact with the 5GZORRO platform at various stages and performing its operations in a holistic way, in few steps, and in parallel benefiting from its modular design. Initially, the Trust Management module is triggered when the client stakeholder asks for the available resources in the marketplace. During the resource selection process, trust level is a critical characteristic, since it can mislead the customer into selecting a slightly higher priced resource from a stakeholder who knows its ways to appear reliable to the system. Besides, the Trust Management module oversees the entire process, monitoring service incidents, or SLA breaches that may require trust level recalculation.

Second, the Intra-domain Security module (highlighted in the blue box in Fig. 11) is responsible for the continuous monitoring of the complete infrastructure. It gets triggered during the secure slicing process and makes sure that platforms on both ends are secure against threats. When slice monitoring is set up, decrypted network traffic from the slice is received and then forwarded to the Intra-domain Security module using a virtual SPAN port configuration. In the current implementation, the Intra-domain Security module is extending the functionality and protocol support of the Zeek network security monitor [56] as well as is integrated with a 5GZORRO-tailored Kibana [57] dashboard for the Security Analytics module. The complete integration is illustrated in Fig. 13. The choice of Zeek was based on its ability to perform knowledge- and behavior-based intrusion detection, instead of a rule-based detection that Suricata and Snort perform [56].

Finally, the Inter-domain Security module (highlighted in the orange box in Fig. 12) is critical in the slice setup process, as it oversees the end-to-end security for the established communications. In that sense, the Inter-domain Security module

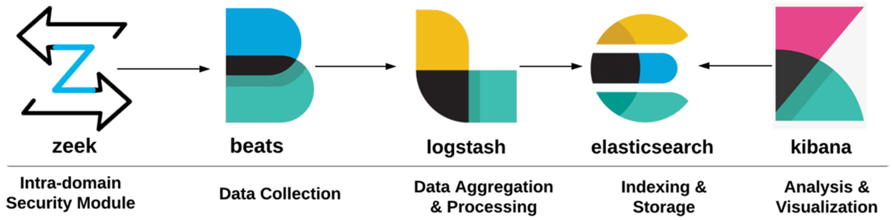


Fig. 13 5GZORRO Intra-domain security module implementation

is triggered by the Network Service Mesh Manager when stitching slices are created in both domains. Here, both the Network Service Mesh Manager's DID and the leased resource's DID are utilized to configure a VPN connection using their public and private keys, and in consequence, a secure end-to-end communication is guaranteed across domains by means of the Inter-domain Security module. In the current 5GZORRO implementation, WireGuard VPN [58] has been selected based on its performance when comparing to other VPN solutions. This solution has been already used in 5G slicing solutions [59], outperforming other VPN solutions. Another of the strong points for WireGuard is that it supports, by design, asymmetrical key authentication based on Curve25519. This key protocol is also compatible with the W3C DID specification [54]. Then, DID public/private key adaptation with WireGuard would be straightforward if this protocol is used in the key generation process associated with the DIDs.

The described use case highlights how the security and trust framework proposed in this article can be integrated with the logic of slicing in a real environment. This way, the security of the process is improved against possible threats. Note that this framework could be applied in other use cases in the same way; for example, the trust module could be used once the slicing process is completed to manage resources or cancel their use.

5 Discussion, Trends, and Challenges

Once the design of the proposed security and trust framework has been detailed, it is essential to discuss its similarities and differences with related state-of-the-art frameworks. This discussion differentiates our work from other proposals and shows possible gaps in the current solutions of the literature. Besides, it is critical to detail the trends and challenges in the area, guiding future iterations of the 5GZORRO security and trust framework as well as setting the stage for new designs and framework implementations.

First, we compare the main characteristics of the most relevant frameworks presented in Sect. 2 with the framework presented in this manuscript and such characteristics are summarized in Table 2 to provide an overview of each framework. In that sense, most of the analyzed frameworks focus on IoT scenarios, and only Suomalainen et al. in [28] apply the framework to 5G and network slicing

Table 2 Features comparison between the upmost relevant projects

Proposal	Framework	Centralized approach	Zero-touch based	Zero trust	Privacy-preserving	Cross-domain connectivity
[14, 28]	5GENSURE	Yes	No	No	Yes	Yes
[15]	INSPIRE-5G Plus	No	Yes	No	Yes	Yes
[16]	MonB5G	No	Yes	Yes	Yes	Yes
[13] Ours	5GZORRO	No	Yes	Yes	Yes	Yes

environments. Nevertheless, they also do not consider a zero-touch automated approach as the rest of frameworks presented in Sect. 2. Given that automation is clearly the path for future frameworks [60], the one presented in this article considers the automation of security and trust frameworks for 5G and beyond 5G, just as other under development frameworks in INSPIRE-5G Plus [15] and MonB5G [16] projects. Furthermore, this path involves many technical improvements regarding AI and network orchestration, such as the integration of AI and orchestration softwares, model optimization for real-time data processing, or the application and development of new algorithms.

Besides automation, the application of AI to security and trust processes brings numerous benefits. A very important one of these benefits is the ability to detect previously unseen threats by applying anomaly detection algorithms, something that is much more complex, if not impossible, using rule-based processing. In addition, the AI models can be adapted to new threats by simply changing the data they receive, reducing the need for expert knowledge to create them. Finally, these AI algorithms usually perform better at detecting complex patterns related to advanced security and trust threats, improving the results of traditional approaches.

Considering the implementation of the frameworks analyzed in Sect. 2, only a few of them have been accomplished, and a couple of solutions rely on simulations or no actual implementations. In this sense, our framework is being developed in a real scenario, very similar to the use case of Sect. 4.2, within the 5GZORRO project. In addition, INSPIRE-5G Plus and MonB5G are following similar paths in terms of implementation.

Finally, so far, only the MonB5G project and the framework designed for 5GZORRO project take into account a zero trust approach, where trust is not assumed depending on where the assets are located, improving trust management and further avoiding internal attacks. This is a paramount point that other frameworks have not already developed nor considered, and that is of utmost importance in modern network environments where intra- and inter-connections are more and more frequent, and with it the exploitation of trust assigned by default. In the case of intra-domain scenarios, the trust by default may have negative consequences if an internal entity has been attacked and consequently, its behavior tampered. In contrast, the trust assigned by default in an inter-domain scenario may skip a new trust computation process on a previously known entity, which would violate trust principles as trust varies over time and must be continuously updated (internal domains) or previously calculated (external domains).

Through the state-of-the-art research and the design of our security and trust framework, numerous trends and challenges have been identified in that research area. These trends guide the current implementation, while the encountered challenges are to be addressed by future framework iterations, in order to improve its capabilities and offered functionalities.

Regarding current trends, the main approaches and ideas expected for future security and trust frameworks are:

- *ML and DL application as trust computation algorithms* Traditionally, trust value computation has been achieved by using rules, statistical functions, or proprietary algorithms developed for a particular platform. However, the rapid expansion of ML and DL techniques has led the current solutions, as well as those under development, to opt for these solutions when calculating confidence values [61]. The main advantage of these is their adaptability to different tasks, as they only require tweaking the training data and hyperparameters to generate different models, while traditional methods require manual changes and adaptations. Besides, these techniques achieve better performance than traditional algorithms because they can extract correlations and infer complex information between different network metrics that traditional algorithms cannot.
- *Virtualization* Currently, many network components in the infrastructure are offered as a virtualized service (SaaS, PaaS, IaaS), and accessed through cloud services. In this extensively cloud-based network landscape, security and trust services are not an exception. Current frameworks are tending toward modularization or fragmentation, making that services can be offered independently through the network. In this sense, Security as a Service (SECaaS) [62] and TaaS [63] cloud applications are emerging, so that the requirements of each entity can be covered independently and in a personalized way.
- *From centralized architectures to decentralized ones* Together with the virtualization of services, also comes its decentralization. Different security and trust functionalities can be enforced from different network elements and even different entities. This trend drastically enables the security and trust service scalability, indispensable in the new massive device 5G scenarios. Besides, this trend is also enabled by the integration of modern blockchain-based technologies in the security and trust life cycle [64], such as the DID integration [65] proposed in our architecture for the Inter-domain Security module.

Due to the fast evolution in the security and trust threats, but also in the frameworks dealing with them, there are many challenges to be considered when developing future security and trust solutions:

- *Standardization* Several standardization organizations are working on security and trust frameworks and documents to boost common approaches for modern network management, however, there is not yet a common framework in this perspective. Currently, the most active group in this area is ETSI ISG ZSM [12], investigating automated network and service management and its application to future networks such as 5G. Regarding security and trust, the ZSM 010 group is studying the threat identification and mitigation options to ensure automated secure processes. Other organizations are also working on different proposals in this paradigm, such as the ITU-T Y.3053 [66] recommendation that introduces a framework for trustworthy networking with trust-centric network domains, or the IETF RFC 8485 [67], proposing a standard for determining the amount of trust to be placed in a digital identity transaction.

- *Zero-touch perspective* Motivated by the explosion of ML and DL, the integration of these methods with network management has become one of the current challenges for modern network solutions. Thus, the automation of security and trust frameworks is not an exception and is receiving a lot of attention in the current designs under development. Nevertheless, there is still a lot of work to be done before fully automated solutions can adapt themselves to changing threats without external intervention. In this sense, and similarly to the previous challenge, the ETSI ZSM is the main group working toward a zero-touch perspective for security and trust management, together with the rest of the network aspects.
- *Optimal countermeasures and countermeasure fairness* Once the different threats to security and trust can be detected, it is essential to properly define what to do to mitigate them. Here, despite the work done so far [68], there is no standardized set of countermeasures applicable to each threat. Instead, each framework defines its own countermeasure actions. Therefore, it is critical that these measures have a compromise between mitigating threats and maintaining high QoS without impairing network performance. In addition, countermeasures to trust threats also need to consider equity with other entities, as aggressive measures could be too damaging to them.
- *Transparency in security and trust management* Transparency is one of the outstanding issues in the trust management of multi-stakeholder environments, since there is a tendency toward models in which security is provided by the obfuscation or confidentiality of the implemented security measures. However, the management of security and trust based on this approach has proven to be inefficient [69], leading to weak trust relationships.
- *Zero trust* The application of zero trust approaches [11] for trust chain management is a novel paradigm that still requires to be implemented in frameworks and architectures of the future. This solution can greatly assist in managing trust in 5G environments where the number of devices is massive, highly dynamic, and heterogeneous. Thus, the security and trust threat landscape might be enclosed through a zero trust approach since it not only guarantees data and services intra- and inter-domain protection, but also all enterprise assets and subjects.

From the trends and challenges described above, it is possible to extract the research lines that should guide the development of the security and trust frameworks of the future. As a conclusion of the future of the research, it can be stated that the main direction is toward the application of ML and DL techniques for the automation of security and trust frameworks, which will be deployed in a distributed and modular way and offered as virtualized services.

6 Conclusions and Future Work

Despite the benefits of 5G networks mass rollouts (higher dynamicity and multi-tenancy), it also brings a mighty threat landscape for adversaries. Owing to the fact that existing security and trust models are not suitable for dealing with the dynamicity of 5G infrastructure threats, the security risks due to the multi-tenancy, nor contemplating new approaches such as zero-touch and zero trust, a pivotal gap was identified in the literature. To address the aforementioned issues, this article has presented a security and trust framework designed for 5G multi-domain network scenarios. The framework has a modular architecture designed to cover threats originated by the new networking paradigms enabled by 5G, where resources from different stakeholders are leveraged to create network slices. Thus, the framework has three main components: a Trust Management module, in charge of managing end-to-end trustworthiness relationships between different entities and elements in the network; the Intra-domain Security module, able to identify attacks and vulnerabilities within the 5G infrastructure as well as in a multi-tenant/multi-domain environment through dynamic traffic analysis; and the Inter-domain Security module, in charge of providing security when creating slices using resources located cross-domains. The framework has been deployed in a realistic use case to demonstrate its usefulness and how it can be applied in a multi-domain network scenario associated with the EU H2020 5GZORRO project. In addition, a series of trends and challenges have been identified during the design phase, which will be addressed during the development stage.

As future work, we plan to provide concrete implementation and deployment details of the security and trust framework following the advances within the 5GZORRO project. Such details will also be in-line with the trends and challenges that were identified in this article. Another feasible objective for future work is to assess the chance of generating a taxonomy for trust models, so that recommendations can be shared with other entities and problems as subjectivity can be avoided. Similarly, well-known trust algorithms such as PeerTrust or PowerTrust will be analyzed to adapt its general functionalities to the requirements presented by the 5GZORRO project. Moreover, there is also a lack of standardizations or guidelines with practical recommendations to be used when generating trust models in 5G networks. Finally, we are also planning to conduct experiments validating the framework according to attacks that are based on the identified threats in 5G multi-tenant and multi-domain scenarios.

Acknowledgements This work was funded by the European Commission through 5GZORRO project (Grant No. 871533) part of the 5G PPP in Horizon 2020. The paper solely reflects the views of the authors. EC is not responsible for the contents of this paper or any use made thereof. Authors thank the 5GZORRO Consortium for useful insights to this work.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. This work has been supported by the European Commission through 5GZORRO project (Grant No. 871533) part of the 5G PPP in Horizon 2020.

Declarations

Conflict of interest All authors declare that they have no conflict of interest.

References

1. Bangerter, B., Talwar, S., Arefi, R., Stewart, K.: Networks and devices for the 5G era. IEEE Commun. Mag. **52**(2), 90–96 (2014)
2. Foukas, X., Patounas, G., Elmokashfi, A., Marina, M.K.: Network slicing in 5G: Survey and challenges. IEEE Commun. Mag. **55**(5), 94–100 (2017)
3. Gündoğran, C., Kietzmann, P., Lenders, M., Petersen, H., Schmidt, T.C., Wählisch, M.: NDN, CoAP, and MQTT: A comparative measurement study in the IoT. In 5th ACM Conference on Information-Centric Networking. pp. 159–171 (2018)
4. Barros, M.: Threat landscape for 5G networks: Updated threat assessment for the fifth generation of mobile telecommunications networks (5G). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks (2020). Accessed 14 July 2021
5. Reynaud, F., Aguessy, F.X., Bettan, O., Bouet, M., Conan, V.: Attacks against network functions virtualization and software-defined networking: State-of-the-art. In 2016 IEEE NetSoft Conference and Workshops. pp. 471–476 (2016)
6. Merget, R., Brinkmann, M., Aviram, N., Somorovsky, J., Mittmann, J., Schwenk, J.: Raccoon attack: Finding and exploiting most-significant-bit-oracles in TLS-DH(E). In 30th USENIX Security Symposium. USENIX Association (2020)
7. Mazurczak, W., Bisson, P., Jover, R.P., Nakao, K., Cabaj, K.: Challenges and novel Solutions for 5G network security, privacy and trust. IEEE Wirel. Commun. **27**(4), 6–7 (2020)
8. Alemany, P., Vilalta, R., Muñoz, R., Casellas, R., Martínez, R. Peer-to-peer blockchain-based NFV service platform for end-to-end network slice orchestration across multiple NFVI domains. IEEE 3rd 5G World Forum (5GWF). pp. 151–156 (2020)
9. Suomalainen, J., Ahola, K., Majanen, M., Mämmelä, O., Ruuska, P.: Security Awareness in Software-Defined Multi-Domain 5G Networks. Future Internet. **10**, 27 (2018)
10. 5GZORRO. https://www.5gzorro.eu/. Accessed 14 July 2021
11. Stafford, V.A.: Zero trust architecture. NIST Spec. Publ. **800**, 207 (2020)
12. ETSI: Zero-touch network and service management (ZSM); Requirements based on documented scenarios. https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/001/01.01.01_60/gs_ZSM001v010101p.pdf (2020). Accessed 14 July 2021
13. Carrozzo, G., Siddiqui, M.S., Betzler, A., Bonnet, J., Martínez Pérez, G., Ramos, A., Subramanya, T.: AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture. In 2020 European Conference on Networks and Communications. pp. 254–258 (2020)
14. Surridge, M., Correndo, G., Meacham, K., Papay, J., Phillips, S.C., Wiegand, S., Wilkinson, T.: Trust modelling in 5G mobile networks. In Workshop on Security in Softwarized Networks: Prospects and Challenges. pp. 14–19 (2018)
15. Ortiz, J., Sanchez-Iborra, R., Bernal Bernabe, J., Skarmeta, A., Benzaid, C., Taleb, T., Alemany, P., Muñoz, R., Vilalta, R., Gaber, C., Wary, J.P., Ayed, D., Bisson, P., Christopoulou, M., Xilouris, G., Montes de Oca, E., Gür, G., Santinelli, G., Lefebvre, V., Pastor, A., Lopez, D. INSPIRE-5Gplus:

Intelligent security and pervasive trust for 5G and beyond networks. In 15th International Conference on Availability, Reliability and Security. 105, 1–10 (2020)

16. Esteves, J.J.A., Boubendir, A., Guillemin, F., Sens, P.: Edge-enabled optimized network slicing in large scale networks. In 11th International Conference on Network of the Future. pp. 129–131 (2020)
17. National Science Foundation: Secure and Trustworthy Cyberspace (SaTC). https://www.nsf.gov/pubs/2021/nsf21500/nsf21500.htm (2020). Accessed 14 July 2021
18. Jayasinghe, U., Otebolaku, A., Um, T.-W., Lee, G.M.: Data centric trust evaluation and prediction framework for IOT. In 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE (2017)
19. Fernández-Gago, C., Moyano, F., Lopez, J.: Modelling trust dynamics in the Internet of Things. Inf. Sci. **396**, 72–78 (2017)
20. Liu, L., Loper, M.: Trust as a Service: Building and managing trust in the Internet of Things. In 2018 IEEE International Symposium on Technologies for Homeland Security. pp. 1–6 (2018)
21. Awan, K.A., Din, I.U., Zareei, M., Talha, M., Guizani, M., Jadoon, S.U.: Holitrust-A holistic cross-domain trust management mechanism for service-centric Internet of Things. IEEE Access. **7**, 52191–52201 (2019)
22. Uikey, C., Bhilare, D.S.: TrustRBAC: Trust role based access control model in multi-domain cloud environments. In International Conference on Information, Communication, Instrumentation and Control. pp. 1–7 (2017)
23. Ravidas, S., Lekidis, A., Paci, F., Zannone, N.: Access control in Internet-of-Things: A survey. J. Netw. Comput. Appl. **144**, 79–101 (2019)
24. Varalakshmi, P., Judgi, T., Balaji, D.: Trust management model based on malicious filtered feedback in cloud. In International Conference on Data Science Analytics and Applications. pp. 178–187 (2018)
25. Burikova, S., Lee, J., Hussain, R., Sharafitdinova, l., Dzheriev, R., Hussain, F., Sharieh, S., Ferworn, A.: A trust management framework for Software Defined Networks-based Internet of Things. In 10th Annual Information Technology, Electronics and Mobile Communication Conference. 0325–0331 (2019)
26. Yao, Z., Yan, Z.: A trust management framework for software-defined network applications. Concurr. Comput. **32**(16), e4518 (2020)
27. Li, J., Liang, G., Liu, T.: A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication. KSII Trans. Internet Inf. Syst. **11**(8), 1 (2017)
28. Suomalainen, J., Ahola, K., Majanen, M., Mämmelä, O., Ruuska, P.: Security awareness in software-defined multi-domain 5G networks. Future Internet. **10**(3), 27 (2018)
29. Wang, Q., Alcaraz-Calero, J., Weiss, M.B., Gavras, A., Neves, P.M., Cale, R., Bernini, G., Carrozzo, G., Ciulli, N., Celozzi, G., Ciriaco, A., Levin, A., Lorenz, D., Barabash, K., Nikaein, N., Spadaro, S., Morris, D., Chochliouros, J., Agapiou, Y., Patachia, C., Iordache, M., Oproiu, E., Lomba, C., Aleixo, A.C., Ro-Drigues, A., Hallissey, G., Bozakov, Z., Koutsopoulos, K., Walsh, P.: SliceNet: End-to-end cognitive network slicing and slice management framework in virtualised multi-domain, multi-tenant 5G networks. In IEEE international symposium on broadband multimedia systems and broadcasting (BMSB). pp. 1–5 (2018)
30. Zupancic, E., Juric, M.B.: TACO: a novel method for trust rating subjectivity elimination based on Trust Attitudes COmparison. Electron. Commer. Res. **15**(2), 207–241 (2015)
31. Hasan, O., Brunie, L., Pierson, J. M., Bertino, E.: Elimination of subjectivity from trust recommendation. In IFIP International Conference on Trust Management. pp. 65–80 (2009)
32. Blasch, E., Laskey, K.B., Jousselme, A.L., Dragos, V., Costa, P.C., Dezert, J.: URREF reliability versus credibility in information fusion (STANAG 2511). In 16th International Conference on Information Fusion. pp. 1600–1607 (2013)
33. Cho, J.H., Chan, K., Adali, S.: A survey on trust modeling. ACM Comput. Surv. **48**(2), 1–40 (2015)
34. Gilbert, E.P.K., Kaliaperumal, B., Rajsingh, E.B., Lydia, M.: Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. Comput. Electr. Eng. **72**, 894–909 (2018)
35. Mendoza, C.V.L., Kleinschmidt, J.H.: A distributed trust management mechanism for the Internet of things using a multi-service approach. Wirel. Pers. Commun. **103**(3), 2501–2513 (2018)
36. Mahmud, K., Usman, M.: Trust establishment and estimation in cloud services: a systematic literature review. J. Netw. Syst. Manage. **27**(2), 489–540 (2019)

37. Fung, C., Zhang, J., Aib, I., Boutaba, R.: Trust management and admission control for host-based collaborative intrusion detection. J. Netw. Syst. Manage. **19**, 257–277 (2011)
38. Cai, L., Rojas-Cessa, R.: Containing sybil attacks on trust management schemes for peer-to-peer networks. In 2014 IEEE International Conference on Communications. pp. 841–846 (2014)
39. Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., Ylianttila, M.: Security for 5G and beyond. IEEE Commun. Surv. Tutor. **21**(4), 3682–3722 (2019)
40. Zhang, X., Kunz, A., Schröder, S.: Overview of 5G security in 3GPP. In 2017 IEEE conference on standards for communications and networking (CSCN). pp. 181–186 (2017)
41. Aggarwal, R. K.: A survey on comparative analysis of tools for the detection of ARP poisoning. In 2017 2nd International Conference on Telecommunication and Networks (TEL-NET). pp. 1–6 (2017)
42. Mamolar, A.S., Salva-Garcia, P., Chirivella-Perez, E., Pervez, Z., Calero, J.M.A., Wang, Q.: Autonomic protection of multi-tenant 5G mobile networks against UDP flooding DDoS attacks. J. Netw. Comput. Appl. **145**, 102416 (2019)
43. Kekki, S., Featherstone, W., Fang, Y., Kuure, P., Li, A., Ranjan, A., Purkayastha, D., Jiangping, F., Frydman, D., Verin, G., Wen, K.W.: MEC in 5G networks. ETSI White Paper. **28**, 1–28 (2018)
44. Xiao, K., Zhao, J., Jiang, M., Wang, F.: An anti-eavesdropping scheme for hybrid multicast services with massive MIMO in 5G. J. Comput. Methods Sci. Eng. **19**(1), 71–81 (2019)
45. Parrend, P., Navarro, J., Guigou, F., Deruyver, A., Collet, P.: Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. EURASIP J. Inf. Secur. **2018**(1), 1–21 (2018)
46. Molina Zarca, A., Garcia-Carrillo, D., Bernal Bernabe, J., Ortiz, J., Marin-Perez, R., Skarmeta, A.: Enabling virtual AAA management in SDN-based IoT networks. Sensors **19**(2), 295 (2019)
47. Chang, V., Kuo, Y.H., Ramachandran, M.: Cloud computing adoption framework: A security framework for business clouds. Futur. Gener. Comput. Syst. **57**, 24–41 (2016)
48. Noor, T.H., Sheng, Q.Z., Yao, L., Dustdar, S., Ngu, A.H.: CloudArmor: Supporting reputation-based trust management for cloud services. IEEE Trans. Parallel Distrib. Syst. **27**(2), 367–380 (2015)
49. Almogren, A., Mohiuddin, I., Din, I.U., Al Majed, H., Guizani, N.: Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. IEEE Internet Things J. **8**(6), 4485–4497 (2020)
50. Radford, B. J., Apolonio, L. M., Trias, A. J., Simpson, J. A.: Network traffic anomaly detection using recurrent neural networks. (2018)
51. Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., Narayan, D.G.: Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Comput. Sci. **167**, 2297–2307 (2020)
52. Wagner, C., Dulaunoy, A., Wagener, G., Iklody, A.: MISP: The design and implementation of a collaborative threat intelligence sharing platform. In ACM on Workshop on Information Sharing and Collaborative Security. pp. 49–56 (2016)
53. Common Vulnerabilities and Exposures. https://cve.mitre.org. Accessed 14 July 2021
54. Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., Holt, J.: Decentralized identifiers (DIDs) v1. 0. Draft Community Group Report. https://www.w3.org/TR/did-core/ (2020). Accessed 14 July 2021
55. Olariu, A., Martinez-Julia, P., Nobre, J., Lopez, D.: Draft IRTF NMRG IBN Intent Classification 03. Network Working Group, Internet Draft (2021) https://tools.ietf.org/html/draft-irtf-nmrg-ibn-intent-classification-03. Accessed 14 July 2021
56. Ghafir, I., Prenosil, V., Svoboda, J., Hammoudeh, M.: A survey on network security monitoring systems. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops. pp. 77–82 (2016)
57. Shah, N., Willick, D., Mago, V.: A framework for social media data analytics using Elasticsearch and Kibana. Wireless Networks. pp. 1–9 (2018)
58. Dowling, B., Paterson, K.G. A cryptographic analysis of the WireGuard protocol. In International Conference on Applied Cryptography and Network Security. pp. 3–21 (2018)
59. Haga, S., Esmaeily, A., Kralevska, K., Gligoroski, D.: 5G Network Slice Isolation with WireGuard and Open Source MANO: A VPNaaS Proof-of-Concept. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). pp. 181–187 (2020)
60. Samdanis, K., Taleb, T.: The road beyond 5G: A vision and insight of the key technologies. IEEE Netw. **34**(2), 135–141 (2020)

61. Deng, S., Huang, L., Xu, G., Wu, X., Wu, Z.: On deep learning for trust-aware recommendations in social networks. IEEE Trans. Neural Netw. Learn. Syst. **28**(5), 1164–1177 (2016)
62. Khettab, Y., Bagaa, M., Dutra, D.L.C., Taleb, T., Toumi, N.: Virtual security as a service for 5G verticals. In 2018 IEEE Wireless Communications and Networking Conference. pp. 1–6 (2018)
63. Xiang, M., Liu, W., Bai, Q., Al-Anbuky, A., Wu, J., Sathiaseelan, A.: NTaaS: Network trustworthiness as a service. In 2017 27th International Telecommunication Networks and Applications Conference. pp. 1–6 (2017)
64. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.: Blockchain-based decentralized trust management in vehicular networks. IEEE Internet Things J. **6**(2), 1495–1505 (2018)
65. Jung, E.: A decentralized access control model for IoT with DID. In IT Convergence and Security. pp. 141–148 (2020)
66. ITU-T. Y.3053: Framework of trustworthy networking with trust-centric network domains. https://www.itu.int/rec/T-REC-Y.3053 (2018). Accessed 14 July 2021
67. Richer, J., Johansson, L.: Vectors of trust. IETF RFC 8485. https://tools.ietf.org/html/rfc8485 (2018). Accessed 14 July 2021
68. Nespoli, P., Gómez Mármol, F., Maestre Vidal, J.: Battling against cyberattacks: Towards pre-standardization of countermeasures. Clust. Comput. (2020)
69. Ismail, U.M., Islam, S., Ouedraogo, M., Weippl, E.: A framework for security transparency in cloud computing. Future Internet **8**(1), 5 (2016)

José María Jorquera Valero is a Ph.D. student in Computer Science at Murcia University. Jorquera Valero received the M.Sc. degree in Computer Science from the University of Murcia, Spain. His scientific interests include cybersecurity, data privacy, continuous authentication, computer networks, trust models, and 5G.

Pedro Miguel Sánchez Sánchez received the M.Sc. degree in computer science from the University of Murcia. He is currently pursuing his PhD in computer science at University of Murcia. His research interests are focused on continuous authentication, networks, 5G, cybersecurity and the application of machine learning and deep learning to the previous fields.

Alexios Lekidis is currently working as a Senior Researcher for projects related to the design and development of telecom solutions for 5G, focusing on NFV and SDN technologies. He is also a Research Assistant at the Aristotle University of Thessaloniki (Department of Informatics), where I work on energy consumption analysis for the Internet of Things (IoT). He has a PhD in Theoretical Computer Science from the University of Grenoble.

Javier Fernandez Hidalgo is a Computer Science engineer with more than 17 years of experience. During the last 12 years he has managed projects in Spain and Finland with teams distributed across multiple countries. Working with different technologies in challenging environments has taught me a variety of skills and how to adapt to constant change. Currently, my projects focus on Virtualization, Containers and Virtual Machines, SDN, NFV and Orchestration.

Manuel Gil Pérez is Assistant Professor in the Department of Information and Communication Engineering of the University of Murcia, Murcia, Spain. His scientific activity is mainly devoted to cyber security, including intrusion detection systems, trust management, privacy-preserving data sharing, and security operations in highly dynamic scenarios. Gil Pérez received M.Sc. and Ph.D. degrees (latter with distinction) in Computer Science from the University of Murcia. He is co-author of 70 + scientific publications in journals and conference papers, as well as an active member on different national and international research projects.

M. Shuaib Siddiqui holds a Ph.D. in Computer Science from Technical University of Catalonia (UPC) (Spain), M.Sc. in Communication Systems (2007) from École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, and B.Sc. in Computer Engineering (2004) from King Fahd University of Petroleum & Minerals (KFUPM), Saudi Arabia. He has 10 + years of experience working in the academic, research and industry of ICT sector. At present, he is a senior researcher at i2CAT Foundation where he is also the Area Manager for Software Networks research lab. He has also given several talks at Mobile

World Congress, Smart City Expo World Congress, SDN/NFV World Congress and other events.

Alberto Huertas Celdrán received the M.Sc. and Ph.D. degrees in computer science from the University of Murcia, Spain. He is currently a postdoctoral fellow associated with the Communication Systems Group (CSG) at the University of Zurich UZH. His scientific interests include medical cyber-physical systems (MCPS), brain–computer interfaces (BCI), cybersecurity, data privacy, continuous authentication, semantic technology, context-aware systems, and computer networks.

Gregorio Martínez Pérez received a Ph.D. degree in Computer Science at the University of Murcia, where he is Full Professor since 2014. His scientific activity is mainly devoted to cybersecurity and data science. He is working on different national (14 in the last decade) and European IST research projects (11 in the last decade) related to these topics, being Principal Investigator for UMU in most of them. He has published + 200 papers and guest edit + 40 special issues in different journals and magazines. He is member of the editorial board of + 15 journals and has already supervised 10 PhD students, several of them recognized with honors.

Authors and Affiliations

José María Jorquera Valero[1] · Pedro Miguel Sánchez Sánchez[1] · Alexios Lekidis[2] · Javier Fernandez Hidalgo[3] · Manuel Gil Pérez[1] · M. Shuaib Siddiqui[3] · Alberto Huertas Celdrán[1] · Gregorio Martínez Pérez[1]

Pedro Miguel Sánchez Sánchez
pedromiguel.sanchez@um.es

Alexios Lekidis
alekidis@intracom-telecom.com

Javier Fernandez Hidalgo
javier.fernandez@i2cat.net

Manuel Gil Pérez
mgilperez@um.es

M. Shuaib Siddiqui
shuaib.siddiqui@i2cat.net

Alberto Huertas Celdrán
alberto.huertas@um.es

Gregorio Martínez Pérez
gregorio@um.es

[1] University of Murcia, Murcia, Spain

[2] Intracom Telecom, Athens, Greece

[3] i2CAT Foundation, Barcelona, Spain