UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Cross-domain Reputation-based Trust Management for Beyond 5G Scenarios

Gestión de la Confianza Basada en la Reputación para Escenarios más allá de 5G

D. José María Jorquera Valero

2023

UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Cross-domain Reputation-based Trust Management for Beyond 5G Scenarios

Gestión de la Confianza Basada en la Reputación para Escenarios más allá de 5G

Autor: D. José María Jorquera Valero

Director/es: D. Manuel Gil Pérez y D. Gregorio Martínez Pérez

UNIVERSIDAD DE MURCIA

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA EN MODALIDAD DE COMPENDIO O ARTÍCULOS PARA OBTENER EL TÍTULO DE DOCTOR

Aprobado por la Comisión General de Doctorado el 19-10-2022

D./Dña. José María Jorquera Valero

doctorando del Programa de Doctorado en

Informática

de la Escuela Internacional de Doctorado de la Universidad Murcia, como autor/a de la tesis presentada para la obtención del título de Doctor y titulada:

Cross-domain Reputation-based Trust Management for Beyond 5G Scenarios / Gestión de la Confianza Basada en la Reputación para Escenarios más allá de 5G

y dirigida por,

D./Dña. Manuel Gil Pérez

D./Dña. Gregorio Martínez Pérez

D./Dña.

DECLARO QUE:

La tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la Ley de Propiedad Intelectual (R.D. legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, modificado por la Ley 2/2019, de 1 de marzo, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita, cuando se han utilizado sus resultados o publicaciones.

Además, al haber sido autorizada como compendio de publicaciones o, tal y como prevé el artículo 29.8 del reglamento, cuenta con:

- *La aceptación por escrito de los coautores de las publicaciones de que el doctorando las presente como parte de la tesis.*
- *En su caso, la renuncia por escrito de los coautores no doctores de dichos trabajos a presentarlos como parte de otras tesis doctorales en la Universidad de Murcia o en cualquier otra universidad.*

Del mismo modo, asumo ante la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad del contenido de la tesis presentada, en caso de plagio, de conformidad con el ordenamiento jurídico vigente.

En Murcia, a 21 de agosto de 2023

Fdo.: José María Jorquera Valero

Esta DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD debe ser insertada en la primera página de la tesis presentada para la obtención del título de Doctor.

Información básica sobre protección de sus datos personales aportados	
Responsable:	Universidad de Murcia. Avenida teniente Flomesta, 5. Edificio de la Convalecencia. 30003; Murcia. Delegado de Protección de Datos: dpd@um.es
Legitimación:	La Universidad de Murcia se encuentra legitimada para el tratamiento de sus datos por ser necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. art. 6.1.c) del Reglamento General de Protección de Datos
Finalidad:	Gestionar su declaración de autoría y originalidad
Destinatarios:	No se prevén comunicaciones de datos
Derechos:	Los interesados pueden ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento, olvido y portabilidad a través del procedimiento establecido a tal efecto en el Registro Electrónico o mediante la presentación de la correspondiente solicitud en las Oficinas de Asistencia en Materia de Registro de la Universidad de Murcia

The following PhD Thesis is a compilation of the next published articles, being the PhD candidate the main author in all of them:

- José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Manuel Gil Pérez, Alberto Huertas Celdrán, Gregorio Martínez Pérez. "**Cutting-edge assets for trust in 5G and beyond: requirements, state of the art, trends, and challenges**", *ACM Computing Surveys*, vol. 55, no. 11, art. no. 222, pp. 1-36, 2023.
  DOI: 10.1145/3572717
  JIF 2022: 16.6 (Q1-D1)

- José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Manuel Gil Pérez, Alberto Huertas Celdrán, Gregorio Martínez Pérez. "**Toward pre-standardization of reputation-based trust models beyond 5G**", *Elsevier Computer Standards & Interfaces*, vol. 81, art. no. 103596, pp. 1-18, 2022.
  DOI: 10.1016/j.csi.2021.103596
  JIF 2022: 5.0 (Q1)

- José María Jorquera Valero, Vasileios Theodorou, Manuel Gil Pérez, Gregorio Martínez Pérez. "**SLA-driven trust and reputation management framework for 5G distributed service marketplaces**", *IEEE Transactions on Dependable and Secure Computing*, In Press, pp. 1-13, 2023.
  DOI: 10.1109/TDSC.2023.3292589
  JIF 2022: 7.3 (Q1-D1)

Contents

Acknowledgements

As it could not be otherwise, I want to begin these words by thanking my parents for everything they have done for me. Thank you for the love, support, and principles you have always given me to allow me to be who I am today.

To my father, Jose, and my mother, Maria de la Cruz, for being there each time I have needed them. Your unwavering support and positive energy are the principal reasons I am writing these words to you today. You have taught me that effort, dedication, and respect are the keys to grow and move forward. Thank you for the time you have devoted, as well as every single effort and sacrifice.

To my brother, Leandro, for transmitting to me his perseverance as an essential foundation to confront difficult moments. Your non-conformist and ambitious character has taught me to get out of my comfort zone and go a step further in whatever challenge life throws at you. *"No human is limited"*.

To my girlfriend, Paula, for supporting me and encouraging me in uncertain moments. Your patience and listening have helped me in an incommensurable way in the hardest moments during the last seven years. Thank you for being always there, I will be eternally grateful to you.

To my colleagues, Pedro and Antonio, for all experiences we lived. Thank you, Pedro, for all advice and support you have given me in the last eight years. Each moment experienced, inside and outside the university, has forged an unimaginable friendship. Thank you, Antonio, for propagating your happiness and positivity through your jolly personality every working day.

To each and every one of my close friends, from all of you, I have learned new things. Especially to Jose Antonio for showing me your indefatigable devotion and continuous wish to learn and grow in defiance of every limit. To Pedro, for teaching me that science is not an abstract set of facts and equations but a way to see the world. To Jose Miguel, for all moments lived and light my path so that I appreciate every step of this journey.

Last but not least, I would like to extend my heartfelt thanks to my thesis directors, Manuel and Gregorio, for everything you have done for me since the first minute I knocked on your doors to ask for advice and help. You trusted my work and this research line from the very beginning. You have been, are, and will be a reference not only for your tireless work and vocation to teach but also for your nearness and transparency. You have taught me many skills that I never thought I could learn.

To all of you, thank you. A part of this thesis belongs to each of you.

Agradecimientos

Como no podría ser de otra forma, quiero comenzar estas palabras agradeciendo a mis padres todo lo que han hecho por mí. Gracias por el cariño, apoyo y valores que siempre habéis transmitido para permitirme ser quien a día de hoy soy.

A mi padre, José, y a mi madre, María de la Cruz, por estar ahí cada vez que los he necesitado. Vuestra dedicación incondicional y energía positiva son la principal razón de que hoy os pueda dedicar estas palabras. Me habéis enseñado que el esfuerzo, la dedicación y el respeto son las claves para crecer y avanzar. Gracias por todo el tiempo que habéis invertido en mí, así como todos y cada uno de los esfuerzos y sacrifícios.

A mi hermano, Leandro, por transmitirme su perseverancia como un pilar esencial para afrontar situaciones complicadas. Tu carácter inconformista y ambicioso me ha enseñado a salir de la zona de confort e ir un paso más allá en cualquier reto que se presente en la vida. *"No human is limited"*.

A mi novia, Paula, por apoyarme y darme ánimos en los momentos de incertidumbre. Tu paciencia y saber escuchar me han ayudado de forma incomesurable en los momentos más difíciles en estos 7 años. Gracias por estar siempre ahí, te estaré eternamente agradecido.

A mis compañeros, Pedro y Antonio, por todas las experiencias vividas. Gracias a Pedro, por todos los consejos y ayuda que me ha brindado en los últimos 8 años. Cada uno de los momentos vividos, dentro y fuera de la universidad, han forjado una amistad inimaginable. Gracias, Antonio, por transmitir tu alegría y positivimos todos los días de trabajo a través de tu personalidad jacarandosa.

A todos y cada uno de mis amigos cercanos, de todos vosotros he aprendido cosas nuevas. En espcial, a José Antonio por mostrarme su pasión incansable y deseo constante de aprender y crecer desafiando cualquier límite. A Pedro, por enseñarme que la ciencia no es un conjunto abstracto de hechos y fórmulas, sino una forma de ver el mundo. A José Miguel, por los momentos vividos e iluminar mi camino para que aprecie cada paso de este viaje.

Finalmente, y no por ello menos importante, quiero agradecer de corazón a mis directores de tesis, Manuel y Gregorio, todo lo que habéis hecho por mí desde el primer minuto que toqué en vuestras puertas para pedir consejo y ayuda. Apostasteis por mi trabajo y por esta línea de investigación desde el primer momento. Habéis sido, sois y seréis referentes, no sólo por vuestro trabajo incansable y vocación a enseñar, sino también por vuestra cercanía y transparencia. Me habéis enseñado multitud de habilidades que nunca pensé que podría aprender.

A todos vosotros, gracias. Una parte de esta tesis es de cada uno de vosotros.

Abstract

1 Introduction and motivation

The introduction of fourth-generation (4G) brought significant advancements in mobile communication, enabling faster data speed and improved connectivity. Yet, as our digital lifestyles continue to evolve, 4G's capabilities have started to show some limitations. In particular, 4G networks have been partially overwhelmed by the massive growth of connected devices and performance features that they require, such as greater data processing and transmission rate, lower end-to-end latency, or higher cell density, to name a few [1]. In this regard, the fifth-generation (5G) telecommunication networks, mostly edge-oriented approaches, aim at overcoming the shortcomings of 4G, usually cloud-oriented, and unlocking new possibilities for the digital era by achieving substantial improvement in Quality-of-Service (QoS) and Quality-of-Experience (QoE) [2]. In order to address some of the 4G limitations, 5G recognizes the need for enhanced computation, processing, and storage capabilities to meet the growing demand for data-intensive applications like Artificial Intelligence (AI), Virtual Reality (VR), and the Internet of Things (IoT). By distributing computing resources closer to the network edge, 5G envisions faster processing, reduced latency, and enhanced scalability, ultimately empowering a new wave of innovative services. Therefore, 5G networks have been designed with the intention of integrating both edge computing and cloud services.

Nevertheless, 5G is also conceived as a highly dynamic environment where asset heterogeneity entails the data and network requirements may rapidly vary [3], for instance, the number of users communicating with each other and the necessary resource capability to guarantee high QoS and QoE. Hence, *verticals* should be capable of dealing with possible peak loads they may suffer whilst coping with capital expenditures (CAPEX) and operational expenditures (OPEX). Due to the fact that it is challenging to foresee the peak loads, on-demand service and resource provisioning solutions [4] have gained prominence in 5G scenarios. Concretely, on-demand provisioning solutions refer to the ability to dynamically allocate and manage network resources and services in real-time based on user demand and specific system requirements. These solutions play a crucial role in 5G networks by enabling flexible and efficient delivery of services, thereby enhancing the overall user experience. Normally, such solutions are principally supported by telcos that have the infrastructure and computation capabilities to assist *verticals*, which are interested in consuming them to ensure statements declared in the Service Level Agreement (SLA) [5].

In the last few years, cutting-edge marketplace approaches have emerged as a solu-

tion for supporting on-demand service, resource, and infrastructure provisioning [6] and enabling their consumers to fulfill the agreed QoS and QoE. Marketplaces also allow consumers to discover and access available resources in real time, as well as resource providers to publish offers about their resources and services, including capacity, capabilities, pricing, localization, etc. When it comes to resource and service aggregation, marketplaces boost both the creation of single offers, coming from only one provider, and composed offers, which aggregate services or resources coming from multiple providers. Marketplaces help to simplify this process through a unified interface, making it easier for consumers to compare options, select the most suitable offer, and initiate provisioning requests. Some examples of such offers, centered on 5G enforcement scenarios, could be cloud, edge, radio access network (RAN), spectrum, virtual network function (VNF), network service, or slice. On the other hand, marketplace-based solutions may pursue a centralized [7] or decentralized approach. However, there is a current trend toward decentralized marketplace solutions [8] since they offer enhanced scalability, fault tolerance (avoiding a single point of failure), and lower latency. Therefore, marketplaces create a cross-domain ecosystem in which both consumers and providers may trade their heterogeneous resources in dynamic 5G environments through a distributed platform that promotes interoperability among resource providers.

Regardless of whether a marketplace has been designed through a centralized or decentralized approach, consumers need assurance that both providers and their resources are trustworthy and secure. In this vein, the lack of trust between a consumer and a provider has a direct impact on the business relationship as consumers may have uncertainty about which provider to choose and how they might behave in the near future [9]. Trust is understood as a belief or confidence in the reliability, integrity, and credibility of another entity or person. It normally involves a willingness to depend on and have positive expectations about the actions, intentions, and behaviors of the other party. Conventionally, when two or more entities want to establish a relationship but have no prior knowledge or experience with each other, trust becomes crucial. Trust helps bridge the gap of uncertainty and allows the entities to engage in a mutually beneficial relationship. In addition, trust may aid in multiple situations such as the risk mitigation [10], by assuring with a certain level of likelihood that an entity will fulfill its commitments and obligations; confidence building [11], by moving forward, cooperating, and collaborating effectively, knowing that the other entity is expected to behave with certain level of reliability and trustworthy; transparent communication [12], by sharing information, clarifying expectations, and maintaining consistent communications; or evidence gathering [13], by providing a possible resolution when appearing conflicts and disputes between multiple stakeholders; among others.

When it comes to trust, several articles have addressed the ways in which can be defined [14, 15, 16] by means of well-known methods such as rule-based [17], blockchain-based [18], game theory-based [19], reputation-based [20], etc. As previously stated, marketplaces are ecosystems in which multi-domain stakeholders are involved, therefore, the awareness of historical incidents and facts is pivotal to predict the forthcoming ones. Likewise, the possibility of profiling stakeholders' behaviors based on previous interactions is another characteristic which can be inferred from marketplaces. Besides, marketplaces may also be visualized as a community where stakeholders can help each other through recommendations on third parties so as to enlarge and aid the community in this cross-domain scenario, where many consumers may have no information about providers and vice versa. Bearing in mind the aforementioned statements and the utmost important trust models [21], reputation-based trust models are one of the best fits for marketplace-based solutions because they fulfill the previous assumptions by enabling the prediction of future stakeholder

behaviors based on historical data and trustworthy recommendations provided by third parties. Furthermore, such models promote transparent evaluations of trustworthiness, which enables consumers and providers from diverse domains to engage with confidence, building a robust and trustworthy decentralized marketplace environment. Additionally, reputation-based trust models foster collaboration and innovation within the marketplace ecosystem due to the fact that they may include new features previously not considered. Usually, consumers can apply various filters through the Graphical User Interface (GUI) to filter available providers' services and resources, e.g., category, price, geographic location, and hardware capacities. By contemplating trust as a new feature or intent, consumers could set new business relationships with lower risk because they may have an estimation of providers' behaviors as well as feedback that supports or does not support such an intuition based on previous evidence.

Yet, just as technologies have been advancing in recent years to adapt them to the new features and requirements of telecommunications networks, so too should trust models. Prior trust models have mostly analyzed the behavior of an end-user to find out a trust level, however, 5G envisions the establishment of end-to-end communications [22]. In this sense, trust models should extend their scopes beyond end-users in order to additionally encompass the analysis of intermediate entities, e.g., network service providers, network resource providers, or software suppliers, among others. Linked to end-to-end communications, it is pivotal to study novel 5G enablers and enforcement scenarios on which trust may be relevant since up-to-date network and business requirements can be discovered. For example, 5G marketplaces bring the flexibility of generating multi-party offers [23] in which multiple resources or services are combined as a whole for consumers. In this regard, prior trust models need to evolve towards approaches analyzing each service and resource of composed offers so as to discover potential weak points or mistrust entities.

On the other hand, 5G networks promote other requirements, such as zero-touch orchestration and zero trust, which add additional value to trust models. Concerning zero-touch orchestration, trust models should not be designed as stand-alone services but should enable seamless integrations with other critical services of 5G and beyond 5G networks (B5G) [24]. Particularly, trust models need to assess their possible impact on the orchestration lifecycle trying to be part of it without compromising performance. With respect to zero trust, it entails one of the most relevant requirements for novel reputation-based trust models. Zero trust principle was defined by the National Institute of Standards and Technology (NIST) [25] and it implies no inherent trust in any user, device, or network, regardless of its location. Thus, trust models should prevent implicit trust granted to any asset, regardless of whether it belongs to our same domain (intra-domain) or an external one (inter-domain), or whether we established reliable relationships long ago. Therefore, zero trust requirement intends to diminish the potential attack surface by emphasizing strict access controls, continuous monitoring, and supporting a least privilege strategy.

Based on the above, there is an opportunity for future works delving into the realm of trust applying to 5G scenarios. These efforts may probably be preceded by a prior analysis of possible enforcement scenarios, entities, or network architectures for which cutting-edge trust-driven solutions are going to be planned. Likewise, novel particular network and business requirements may arise with respect to previous designs centered on 4G-oriented solutions, so new research opportunities appear on the roadmap. In this regard, there is also an opportunity to design and develop innovative trust solutions that can not only enhance the performance of existing solutions but also elevate the user experience. Additionally, trust models present ongoing challenges, with a scarcity of literature addressing the development of innovative solutions applicable in dynamic environments where users

can establish cross-domain relationships on demand to ensure QoS and QoE.

2 Objectives

The main objective of this PhD Thesis consists of studying, analyzing, and addressing the principal limitations of reputation-based trust models in 5G and B5G scenarios, identifying novel business and network requirements to evolve prior models. Furthermore, this work aims to develop a scalable reputation-based trust management framework for an on-demand service provisioning scenario in which several cutting-edge business and network requirements are fulfilled. More specifically, several specific sub-objectives are inferred from this objective and are listed below:

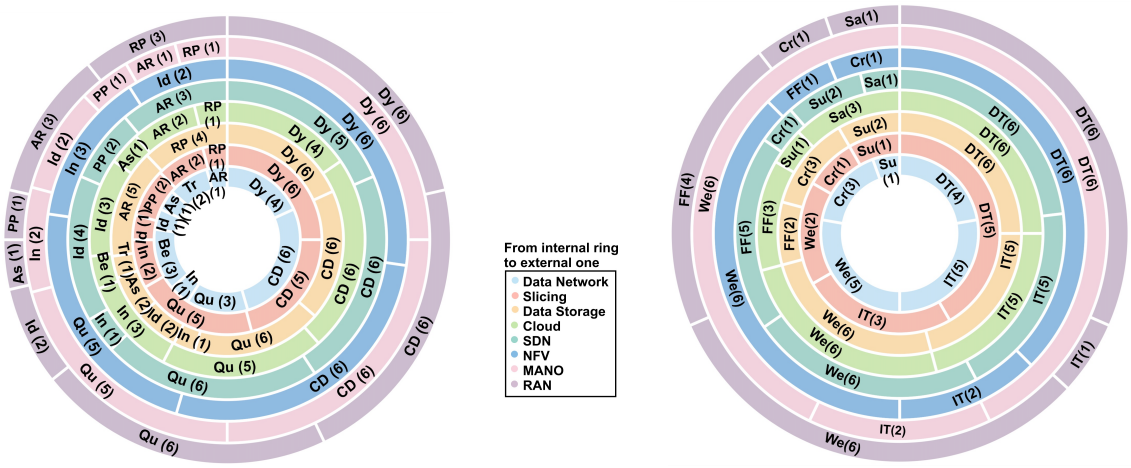
1. Analyze the current state-of-the-art proposals regarding trust and reputation models in several 5G and B5G scenarios, studying the properties and features of trust models.
2. Identify a set of pivotal trust enablers in 5G and beyond networks as well as similarities among their application scenarios in terms of properties and features.
3. Highlight the current trends of trust models and describe future research challenges.
4. Gather pre-5G and 5G/B5G requirements and Key Performance Indicators (KPI) for cutting-edge trust models.
5. Propose a pre-standardization approach for reputation-based trust models beyond 5G.
6. Design and development of a reputation-based trust management framework in a decentralized 5G marketplace platform.
7. Analyze the impact that the reputation-based trust model could cause on the network resource provisioning discovery and orchestration processes through exhaustive experiments.
8. Implement a set of attacks impacting trust concepts in a real testbed, using multiple waves of malicious behaviors, to test the framework resilience and their impact on trust scores.

3 Methodology

This PhD Thesis was conducted as a publication compendium following a scientific approach. In particular, this PhD Thesis is composed of a set of three research papers published in reputable journals indexed in the Journal Citation Report (JCR). Therefore, all work performed through these three papers was directed towards fulfilling the PhD Thesis objectives introduced in the above section.

The first milestone of this PhD Thesis was the in-depth analysis of the utmost important concepts of trust models. Prior to laying the foundations of trust models, understanding their intrinsic characteristics is an essential step. In this sense, the first publication (Survey of Trust Models and Enablers for 5G and Beyond Scenarios (Article 1–ACM_CSUR)) involved the study of multiple trust models in order to gather and identify the principal properties and features that made them up. By means of this study, a dual objective was carried out. To begin with, it tried to find out what properties could be applied to trust

models regardless they belong to a reputation-based approach and what features could be only considered by reputation-based models. On the other hand, the study described the meaning of each and what actions should be performed to cover them without leveraging specific application scenarios. Some of the identified properties could be dynamism, context-dependence, or reward and punishment, whilst credibility, satisfaction, or forgetting factors were presented as features related to reputation. Note that these properties and features were later taken into account in the design and development phases. Once both properties and features were investigated, we performed a review of 5G assets or enablers in which trust enforcement could help to deal with their weaknesses or current challenges, available in Article 1–ACM_CSUR. Among the most relevant assets found in the literature, we may point out *data network, slicing, cloud, Management and Orchestration (MANO), or data storage,* to name a few. Furthermore, the first publication also evaluated what similarities and differences had trust models across 5G assets in order to figure out whether properties and features were equally considered in the current solutions of the state-of-the-art. To this end, we assessed more than 45 publications collecting information about properties and features contemplated, main information sources to compute trust values, algorithms, and key results.



(a) Properties (b) Features

Figure 1: Properties and Features across 5G and B5G assets

A graphical synopsis of the surveyed works with references to the assets and their principal properties and features is displayed in Figure 1. More specifically, such a figure revealed valuable insights, inferred from the literature review process, about the properties and features that shape the landscape of trust models in 5G and B5G assets. The distribution of these properties illustrated how dynamism, context-dependence, and quantification are the most prominent, reflecting the emphasis on on-demand service and resource provisioning in these enablers' application scenarios. However, identity is also a prevalent property across all enablers, albeit to a lesser extent. Regarding features, we observed how direct and indirect trust, weighting factor, and forgetting factor played a vital role in forecasting trust. Nevertheless, there were other features that appeared to be underrepresented, such as subjectivity and credibility but hold the potential for improving trust models. By analyzing and understanding the aspects highlighted in Figure 1, researchers may focus on designing and developing solutions that address the evolving needs of trust and reputation models and enable more robust and reliable communication systems in the future.

Based on the thorough analysis carried out in Article 1–ACM_CSUR, several current trends (top three from the following list) and research challenges (last three) were recognized which are relevant to design and develop upcoming reputation-based trust models:

- *Trustworthy end-to-end connections*: analyze not only end-users but also intermediary entities of trustworthy chains such as network service providers, network resource providers, or software suppliers services.
- *Automation and zero-touch service management*: seamless trust integration with other 5G orchestration services without compromising performance.
- *Zero Trust*: recent studies started to address it due to the exponential growth of threat landscapes though only one reviewed approach took it into account.
- *Reputation-based trust model standardization*: efforts to standardize trust models in research and industry have been made, but there are currently no universal guidelines or standards that can be widely adopted by researchers in any enforcement scenario.
- *Trust as distributed service*: pervasive and scalable resource-sharing solutions in 5G and B5G networks are driving the adoption of distributed solutions and multi-party collaboration for on-demand service provisioning, posing new challenges for trust models in terms of design and development.
- *Trust-related attacks*: the huge growth of interconnected devices and services comes with an increased attack surface, so trust model should analyze trust-based attacks to be resilient.

In order to address the challenges outlined in the previous statements, another meaningful achievement of this PhD Thesis was the proposal of a pre-standardization approach for reputation-based trust models beyond 5G (Guidelines for reputation-based trust models (Article 2–Elsevier_CSI)). After reviewing the literature concerning trust models for 5G and beyond scenarios and discovering properties and features conventionally presented in trust enabler solutions, we planned to design our trust and reputation model to face all aforementioned challenges in a single solution. Nevertheless, we did not find widely-known guidelines or standards to be pursued so as to build novel 5G and B5G trust and reputation models, so we decided to go deep into such a challenge. In this vein, Article 2–Elsevier_CSI attempted to support the scientific community that intends to tackle a similar challenge in the near future. Firstly, we conducted an in-depth analysis of solutions working on pre-standardization, standardization, guideline, or long-term trust model. Such an effort had a dual objective because it allowed us to determine whether there were proposals dealing with the challenge in the context of 5G and B5G networks and to comprehend the principal actions and ideas to be transmitted in a pre-standardization proposal. Therefore, we analyzed (pre-)standardization publications, significant European and non-European research projects, and regulatory bodies that had been working on or were still working on reputation-based trust model standardization or beyond 5G. Through such an analysis, we were able to validate that the previous properties and features had also been considered in standardization proposals as well as adjust some of them to be well aligned. Among the most significant solutions, we can stand out the research papers by Gómez Mármol and Martínez Pérez [26] and Ylianttila et al. [27], the INSPIRE5G-Plus research project [28], and the International Telecommunication Union-T Y.3052 regulatory organization [29] because they shared the vast majority of our properties, features, and

components we had in mind for designing a reputation-based trust model in beyond 5G networks.

Once we finished the review of the literature, we concluded that not only properties and features had been partaken of the analyzed trust and reputation models, but also requirements and KPIs. At this point, we gathered requirements of pre-5G trust model standardizations and requirements for 5G and beyond 5G trust models. Besides, we also observed that some requirements had been proposed for pre-5G models but were still considered today in current proposals. In this sense, 27 requirements and 8 KPIs were collected together with their information source and how reputation-based trust model proposals should cover them. It is true that several methodologies can be leveraged to deploy requirements and KPIs, but we tried to be as generic as possible to help at least the reader understand the key ideas to ensure these requirements and KPIs. Lastly, after identifying the present requirements and KPIs of both 5G and beyond networks, we presented a collection of suggestions aimed at crafting a trust model based on reputation. These suggestions served as guiding principles for developing advanced trust and reputation models. Furthermore, we put forth state-of-the-art technologies and approaches that can be considered to fulfill requirements and establish all-encompassing trust models.

At this time, we had already settled the guidelines to design a trust and reputation model for 5G and B5G scenarios, so the next step was to establish a specific environment for designing and developing it. Thus, the third publication of this PhD Thesis, presented in the third chapter (Trust for on-demand service provisioning (Article 3–IEEE_TDSC)), contextualized a 5G network resource provisioning as the enforcement scenario for the reputation-enabled trust model to be designed. It is worth mentioning that such an application scenario is aligned with the 5GZORRO H2020 European project [30], where we all have been actively involved, and a brief description of 5GZORRO project together with some additional publications can be found in Section 4.1. When it comes to Article 3–IEEE_TDSC, we presented through it four major achievements. On the one hand, we designed our reputation-based trust framework, which was mainly composed of four modules: (i) the *Information gathering and sharing*, (ii) the *Trust computation*, (iii) the *Trust storage*, and (iv) the *Continuous update* (see Figure 2). Bearing in mind the properties, features, and requirements, we thoroughly described the significant actions to be carried out under each module and how such a module could be developed for the suggested network service provisioning scenario.

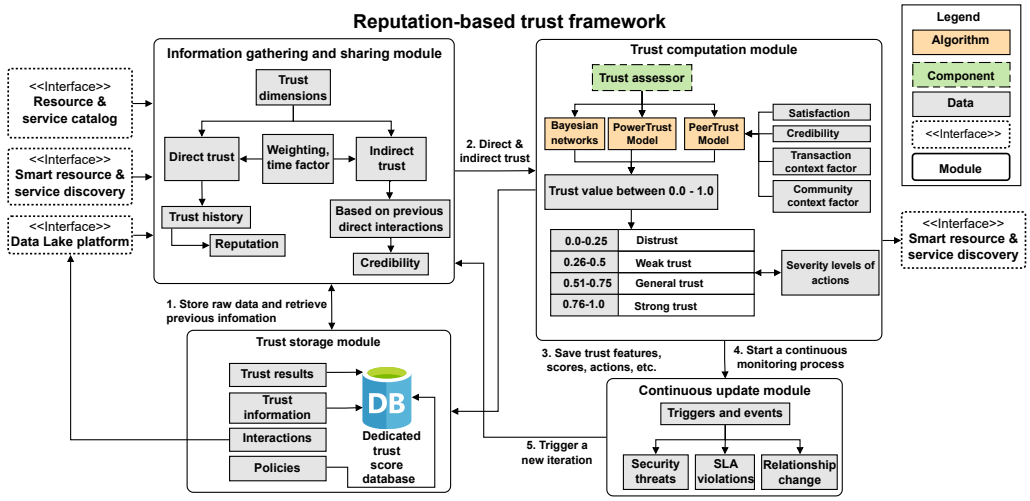


Figure 2: Overview of trust and reputation framework design

Concerning the *Information gathering and sharing* module, it collected raw data and statistics from several information sources, e.g., the *Resource & service catalog*, the *Smart resource & service discovery*, or the *Data Lake*, among others. In addition, such a module introduced what specific information could be used for each information source. For example, the *Resource & service catalog* may provide information related to Product Offers such as geolocation of services and resources, current life-cycle status, service specification, etc. or the *Data Lake* may support the monitoring of Service Level Agreements (SLA) between consumers and providers. Afterwards, all information was categorized as direct trust, which means the information coming from previous personal experiences, or indirect trust, which refers to information provided by recommenders. At this point, all information is forwarded to the *Trust computation* module to evaluate it and provide a trust score. To this end, we inspected different statistical algorithms dealing with distributed scenarios where peer-to-peer connections could be established. Among the different candidates, we observed that Bayesian networks, the PowerTrust model, and the PeerTrust model could satisfy our previous statements. Yet, we finally elected PeerTrust model because it brought significant versatility to researchers as they should freely formulate the four principal dimensions: satisfaction (S), credibility (Cr), transaction context factor (TF), and community context factor (CF) (see Equation 1). Therefore, we followed the PeerTrust's principles but we needed to formulate how each pillar was going to be calculated. In this sense, we set up an adapted PeerTrust model. Furthermore, the PeerTrust model also contemplated the main properties and features, previously indicated in Article 1–ACM_CSUR and Article 2–Elsevier_CSI, therefore best suited our principles. It should be pointed out that the thorough description of dimensions is itemized across several publications, where [31] addressed the community context factor, and [32] tackled both satisfaction (S) and transaction context factor (TF).

$$T(u) = \alpha \cdot \left(\sum_{i=1}^{I(u)} S(u,i) \cdot Cr(p(u,i)) \cdot TF(u,i) \right) + \beta \cdot CF(u) \tag{1}$$

Due to the fact that trust is not a one-time process, our reputation-enabled trust framework also contemplated one module for storing evidence and another to update trust scores continuously. The former, named *Trust Storage* module, aimed primarily at ensuring data security as there were two types of storage sources. To begin with, the Data Lake was leveraged as a shared platform across stakeholders to disseminate awareness regarding reliable engagements among the participants comprising the 5GZORRO ecosystem. In this context, newcomers can identify viable advisors to consult with. In addition, our framework contemplated a private database per domain whose main goal was to diminish the time necessary to process information in real time, which is required each time we requested information from the Data Lake, and maintain personal data, inferred information from raw data, which should not be shared with the community. The latter, called *Continuous update* module, was in charge of monitoring real-time events to trigger a reassessment of a trust relationship. In particular, the reputation-based trust framework defined two reward and punishment mechanisms to adjust trust scores. For example, we declared a reward and punishment mechanism based on security events inferred from network monitoring [31]. Such a mechanism enabled the identification of threats and misbehaviors in the network traffic and, in consequence, applied the proper punishment in the case of discovering unusual actions.

Another example was proposed in the third chapter of this document (Article 3–IEEE_TDSC) so as to analyze the behavior of our reputation-enabled trust framework when multiple types of trust-related attacks intended to tamper a reliable flow. More specifically,

it presented a solution for 5G distributed service marketplaces whose goal is to support on-demand resource and service provisioning. This last article reported an edge-based use case (UC) in the context of a virtual Content Delivery Network (vCDN) paradigm. It highlighted the application of trust for optimizing orchestration and ensuring the selection of a reliable slice. Such a real use case implicated a stakeholder seeking slice expansion to handle the increased load on their vCDN server at the Content Service Provider (CSP) Edge. Therefore, the stakeholder needed to acquire compute resources, specifically a slice instance, at the Edge to bypass network core traffic routing. Since the UC was instantiated under the scope of the 5GZORRO project, we also detailed in Article 3–IEEE_TDSC the integration of a trust and reputation framework into a 5G distributed service marketplace.

Another significant milestone of Article 3–IEEE_TDSC was the description of a new reward and punishment mechanism under the *Continuous update* module. As we briefly introduced above, an SLA-driven reward and punishment mechanism was created so as to find out when a stakeholder should be able to participate in a relationship or finish its current relationship due to subsequent misbehaviors. In particular, the SLA-driven mechanism was designed to be flexible and adaptable, compatible with various trust and reputation models. Furthermore, it followed an event-driven approach, dynamically adjusting relationships in real time based on breach prediction rate (BPRate), impact of trust (ITrust), and historical SLA violation rate (SLAVRate) (see Equation 2). Additionally, we leveraged two fuzzy models to assess the membership degree of trust scores within the defined trust levels (untrustworthy, little trustworthy, moderately trustworthy, trustworthy, and fully trustworthy) and to evaluate the occurrence level of SLA violations in the last time window (momentary, recurrent, and persistent).

$$Pu(v,u) = \sum_{m=1}^{n} \frac{BPRate(u,m) + ITrust(v,u) \cdot SLAVRate(u,m)}{2} \tag{2}$$

As a final milestone, we needed to check whether the reputation-enabled trust framework, its nineteen equations, and its mechanisms had the expected behavior and were resistant to some known attacks. To demonstrate it, we performed three principal experiments. Nonetheless, prior to the experiments, we also carried out a fine tuning process to understand how essential parameters, such as forgetting factor ξ and the increase or decrease percentage of our punishment and reward mechanism n, may have an impact on trust scores. After analyzing the results, we obtained two main conclusions. On one side, as the value of n increases, the extent of punishment imposed on trust scores will be constrained in contrast to a lower value of n. This is reflected in likely drastic changes in trust values. Conversely, by utilizing a forgetting factor ξ closer to 0.2 (up to 1), it would require an increased number of interactions to equate $SLAVRate^{(t)}(u,m)$ to a recurring increment of SLA violations over time. Therefore, the recovery rate of the reward mechanism should be slower compared to its punishment one, as trust and reputation models typically prioritize identifying stakeholders' misbehaviors rather than their positive actions.

When it comes to experiments, our reputation-based trust framework was capable of handling on-off attacks providing two main lessons. Firstly, the reward mechanism prevented stakeholders from surpassing a series of successive misbehaviors (2, 4, or 8 waves) within a brief timeframe. Thus, our earlier assertion that negative events have a more significant influence on trust scores than positive events is being substantiated. Secondly, the punishment mechanism allowed for a gradual decrease in a high trust score rather than immediately setting it to 0, provided that the setback was an isolated incident and the stakeholder had successfully recovered. Lastly, the framework was also resilient to collusive bad-mouthing attacks when there were different numbers of malicious entities between the

recommenders' populations. Outcomes revealed that the framework can ensure an accuracy of 0.93 when 30% of recommenders behaved spitefully and a 0.67 accuracy when 50% of recommenders had malicious behaviors. Besides, we observed that a trust score decreased by 8.6% when our trust and reputation framework achieved a 33% accuracy in identifying misbehaviors, with a malicious population of 90% and 100/150 recommenders. In contrast, when only 30% of recommenders exhibited malicious behavior, the trust score decreased by only 2.1%. In this way, our solution was capable of fairly distinguishing collusive bad-mouthing attacks as well as coping with continuous misbehavior waves.

4 Other relevant publications

Furthermore, during this PhD Thesis, the PhD candidate also participated in a research project related to security and trust aspects, leading significant publications that enhanced his expertise, both in terms of research capabilities and collaborative teamwork. Next, the principal publications related to the involved research project and thesis topic are listed.

4.1 5GZORRO: Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks

The 5GZORRO project aimed to create solutions for seamless management of services, networks, and security in multi-stakeholder environments, as well as settle a trustworthy ecosystem where stakeholders can interact across different administrative domains. A key goal of the 5GZORRO project was to design and develop a security and trust framework that is seamlessly integrated with 5G service management platforms. This framework aimed to showcase the implementation of Zero Trust principles within distributed environments involving multiple stakeholders. Additionally, it facilitated automated security management to ensure the trusted and secure execution of offloaded workloads across various domains in 5G networks.

This project was funded by the European Commission through grant no. 871533 part of the 5G PPP in Horizon 2020, being the University of Murcia one of the main collaborator partners and leader of a work package centered on zero-touch automation with trust, security, and AI. The related publications are listed as follows:

- Adriana Fernández-Fernández, Michael De Angelis, Pietro G Giardina, James Taylor, Paulo Chainho, José María Jorquera Valero, Leonardo Ochoa-Aday, Diego R López, Gino Carrozzo, M Shuaib Siddiqui, "**Multi-party collaboration in 5G networks via DLT-enabled marketplaces: A pragmatic approach**", *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 550-555.
  DOI: 10.1109/EuCNC/6GSummit51104.2021.9482487

- José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Alexios Lekidis, Javier Fernandez Hidalgo, Manuel Gil Pérez, Muhammad Shuaib Siddiqui, Alberto Huertas Celdrán, Gregorio Martínez Pérez, "**Design of a security and trust framework for 5G multi-domain scenarios**", *Journal of Network System Management*, vol. 30, art. no. 7, pp. 1-35, 2022.
  DOI: 10.1007/s10922-021-09623-7
  JIF 2022: 3.6 (Q3)

- José María Jorquera Valero, Manuel Gil Pérez, Gregorio Martínez Pérez, "**A security and trust framework for decentralized 5G marketplaces**", Seventh National Conference on Cybersecurity (JNIC), 2022, pp. 237-240, Bilbao, Spain.

5 Conclusions and future work

The abrupt growth of interconnected services and devices has, in turn, entailed an increase in the number and type of relations between entities. Due to the nature of 5G networks, it is becoming more and more common to settle relationships with entities belonging to different administrative domains. In fact, one of the challenges faced by end-users on a daily basis is the high demand for resources to cover workloads while maintaining QoS, which is certainly caused by the boost of interconnected services and devices. Thereby, end-users frequently rely on services, resources, and infrastructure offered by network infrastructure providers or network service/resource providers, willing to ameliorate their current capabilities.

Yet, the wide variety of opportunities and useful solutions to support the deployment of services, resources, or infrastructures that allow end-users to cover certain peak loads introduces a default trust in some cases. Depending on end-users' requirements, they may be interested in hiring solutions to broaden their capabilities, such as Infrastructure-as-a-Services approaches, when they want to configure virtualized computing resources based on their requirements and specific services, or marketplaces, when on the contrary they are only interested in using third party resources without the need to configure from scratch and maintain them. Nonetheless, marketplaces are gaining prominence as they allow resources or services to be requested on demand, allowing them to be used in highly dynamic scenarios where flexible and extensible solutions are sought.

In both scenarios, trust is a pivotal pillar to consider before establishing a business relationship or selecting an available service or resource, as trust may help to forecast how an entity will behave in a forthcoming time window by looking at its previous interactions. Nevertheless, marketplaces do not generally enable filtering options or characteristics based on trust, but they usually provide end-users with advanced options to filter available resources based on performance, hardware, or location characteristics. On the other hand, prior trust models should not be directly leveraged in cutting-edge 5G network scenarios as new trends and challenges are constantly appearing. Thereby, trust models require progressing toward new approaches which analyze and contemplate novel network and business requirements, properties, features, and KPIs.

Attempting to contribute to the previous concerns and limitations, this PhD Thesis centered on analyzing the challenges and gaps of reputation-based trust models in 5G scenarios and proposing a reliable solution for on-demand service and resource provisioning solutions, especially multi-party service marketplaces. Having in mind the principal objective and sub-objectives listed in Section 2, the next outstanding contributions have been accomplished:

- firstly, a thorough review of the literature concerning trust and reputation models in 5G scenarios. By means of this analysis, Article 1–ACM_CSUR reported an in-depth analysis of utmost importance properties and features for trust models. Besides, eight significant enablers were identified, together with reviewing and comparing the most recent trust-related papers. Additionally, Article 1–ACM_CSUR described a set of trends and challenges that subsequently set the course for this thesis.

- secondly, a pre-standardization approach for reputation-based trust model beyond 5G. A comprehensive collection of requirements and essential KPIs was derived by

reviewing and comparing (pre-)standardization papers, research projects, and regulatory organizations. Furthermore, a set of preliminary recommendations was suggested for addressing crucial aspects of upcoming networks and addressing the absence of standardized trust and reputation models beyond the 5G era, as described in Article 2–Elsevier_CSI.

- thirdly, an analysis of our reputation-enabled trust framework when suffering different trust-related attack bursts. The proposed framework was made up of four modules that enabled a dynamic, context-aware, automated, and flexible solution. An adapted PeerTrust model was created to compute trust scores based on statistical information inferred from product offers, network providers, and recommenders. Additionally, an SLA-driven reward and punishment mechanism was designed to continuously adapt trust scores of an ongoing trust relationship when SLA violation, breach prediction, or breach detection appeared in real time. Article 3–IEEE_TDSC also detailed an edge-based use case in which the proposed framework was integrated with other marketplace-linked services, developed under the 5GZORRO European project, in a seamless way. Experiments demonstrated that our reputation framework was resilient to bad-mouthing and on-off attacks.

These research findings have been published in high-impact JCR-indexed journals to share the outcomes and potentially influence the wider research community as the primary objective. Moreover, the results have been closely monitored and shared with the 5GZORRO consortium and the European Commission. Nevertheless, there is still a considerable distance to cover in the enforcement of trust models for 5G and B5G scenarios. Undoubtedly, certain challenges remain unresolved and will demand substantial contributions in the times ahead.

More specifically, the official standardization of reputation-based trust models is a cornerstone to homogenizing solutions and rowing in the same direction. To date, there have been individual initiatives as well as regulatory organizations (ITU-T Y.3053) aiming to establish trust models in the research and industry domains, respectively. However, there is currently no comprehensive guideline or universally adopted standard applicable to the majority of individuals, regardless of the specific implementation scenario. In this vein, organizations like the TM Forum and ITU-T X.5Gsec-t have made efforts to address the lack of standardization in trust models, but unfortunately, public versions of these drafts are not yet available. In line with the standardization endeavors, there are also other prerequisites, such as a common vocabulary, information models, business process models, APIs, and assessment metrics, that need to be addressed before achieving a final standardization approach.

As a future work, this PhD Thesis first identifies the necessity of extending the resilience of our reputation-enabled trust framework as not only on-off and bad-mouthing are attacks that may tamper the appropriate behavior of trust models. Attacks such as shilling, collusion, or ballot stuffing should also be tackled. Another forthcoming milestone is the application of AI-driven models instead of purely statistical algorithms based on customized equations. Based on our personal experiences during this PhD Thesis, statistics models like PeerTrust or similar are capable of providing accurate results without penalizing the performance of the whole lifecycle of trust management models. Yet, when the comparison between statistical models has to be performed, this is a complicated process because it usually entails the (re)design or (re)definition of a new set of equations for each purely statistical model. Therefore, such a process involves a huge time consumption in contrast to what happens when several AI models are compared more easily in terms of precision,

recall, or F1 score. Likewise, an AI-driven trust model could benefit from the large amount of monitoring data that exists in addition to the predictive capacity that some of these models may provide.

Additionally, this research also detects the need of incorporating security features as another crucial pillar of the trust models for beyond 5G solutions. Trust and security, together with privacy, are the foundations to assemble the future sixth generation (6G) of mobile telecommunications. Thence, security is one of the main concerns when designing future 6G networks. This is shown by some of 6G's research lines focusing on designing future 6G networks by assessing the security of a network service in a particular application environment. In this regard, our trust model may evolve towards a trust assessment function, AI-driven, capable of ensuring security aspects from a set of applicable technologies to 6G domain experts. Therefore, our expanded trust model could support the discovery of an intent-based and neutral solution to determine the trustworthiness of infrastructure and network providers by analyzing their security and privacy properties, technologies, and threat patterns, as well as considering user requirements throughout its AI-enabled information processing.

Resumen

1 Introducción y motivación

La introducción de la cuarta generación (4G) trajo avances significativos en la comunicación móvil, permitiendo una mayor velocidad de datos y una mejor conectividad. Sin embargo, a medida que nuestros estilos de vida digitales continúan evolucionando, las capacidades del 4G han comenzado a mostrar algunas limitaciones. En particular, las redes 4G han sido parcialmente sobrepasadas por el enorme crecimiento de dispositivos conectados y las nuevas características de rendimiento que requieren, como un mayor procesamiento y velocidad de transmisión de datos, una menor latencia de extremo a extremo o una mayor densidad celular, por mencionar algunas [1]. En este sentido, las redes de telecomunicaciones de quinta generación (5G), mayormente orientadas a enfoques basados en el borde de la red, tienen como objetivo superar los hándicaps del 4G, normalmente orientado a la nube, y desbloquear nuevas posibilidades para la era digital al lograr una mejora sustancial en la calidad de servicio (del inglés Quality of Service, QoS) y calidad de experiencia (del inglés Quality of Experience, QoE) [2]. Para abordar algunas de las limitaciones del 4G, 5G reconoce la necesidad de capacidades mejoradas de cálculo, procesamiento y almacenamiento para satisfacer la creciente demanda de aplicaciones intensivas en datos como la inteligencia artificial (del inglés Artificial Intelligence, AI), la realidad virtual (del inglés Virtual Reality, VR) y el Internet de las cosas (del inglés Internet of Things, IoT). Al distribuir los recursos de computación más cerca del borde de la red, el 5G visualiza un procesamiento más rápido, una menor latencia y una mayor escalabilidad, lo que finalmente potencia una nueva ola de servicios innovadores. Por lo tanto, las redes 5G han sido diseñadas con la intención de integrar tanto la computación y los servicios en el borde como en la nube.

No obstante, el 5G también se concibe como un entorno altamente dinámico donde la heterogeneidad de los activos implica que los requisitos de datos y red pueden variar rápidamente [3], por ejemplo, el número de usuarios que se comunican entre sí y la capacidad de recursos necesaria para garantizar una alta QoS y QoE. Por lo tanto, los *verticals* deben ser capaces de hacer frente a posibles picos de carga de trabajo que puedan sufrir, al mismo tiempo que manejan los gastos de capital (del inglés capital expenditures, CAPEX) y los gastos operativos (del inglés operational expenditures, OPEX). Debido a que es difícil prever las picos de carga, las soluciones de provisión de servicios y recursos bajo demanda [4] han ganado protagonismo en los escenarios 5G y más allá. Concretamente, las soluciones de provisión bajo demanda se refieren a la capacidad de asignar y gestionar de

manera dinámica los recursos y servicios de red en tiempo real en función de la demanda del usuario y los requisitos específicos del sistema. Estas soluciones desempeñan un papel crucial en las redes 5G al permitir la entrega flexible y eficiente de servicios, mejorando así la experiencia general del usuario. Normalmente, dichas soluciones son principalmente respaldadas por empresas de telecomunicaciones que cuentan con la infraestructura y las capacidades de computación para asistir a los sectores verticales, que están interesados en consumirlas para garantizar las declaraciones establecidas en el acuerdo de nivel de servicio (del inglés Service Level Agreement, SLA) [5].

En los últimos años, han surgido enfoques basados en mercados como una solución para respaldar la provisión de servicios, recursos e infraestructura bajo demanda [6] y habilitar a sus consumidores a cumplir con los QoS y QoE acordados. Los mercados permiten a los consumidores descubrir y acceder a los recursos disponibles en tiempo real, así como a los proveedores de recursos publicar ofertas sobre sus recursos y servicios, que incluyen capacidad, precio, ubicación, etc. En lo que respecta a la agregación de recursos y servicios, los mercados fomentan tanto la creación de ofertas individuales, provenientes de un único proveedor, como las ofertas compuestas, que agregan servicios o recursos provenientes de múltiples proveedores. Los mercados ayudan a simplificar este proceso a través de una interfaz unificada, facilitando a los consumidores comparar opciones, seleccionar la oferta más adecuada e iniciar solicitudes de provisión. Algunos ejemplos de tales ofertas, centradas en escenarios de implementación del 5G, podrían ser la nube, el borde de la red, la red de acceso por radio (del ingés radio access network, RAN), el espectro, la función de red virtual (del inglés virtual network function, VNF), el servicio de red o el *corte de red* (del inglés slice). Por otro lado, las soluciones basadas en mercados pueden seguir un enfoque centralizado [7] o descentralizado. Sin embargo, existe una tendencia actual hacia soluciones de mercado descentralizadas [8] debido a que ofrecen una mayor escalabilidad, tolerancia a fallos (evitando un único punto de fallo) y menor latencia. Por lo tanto, los mercados crean un ecosistema interdominio en el cual tanto los consumidores como los proveedores pueden intercambiar sus recursos heterogéneos en entornos 5G dinámicos a través de una plataforma distribuida que promueve la interoperabilidad entre los proveedores de recursos.

Independientemente de si un mercado ha sido diseñado mediante un enfoque centralizado o descentralizado, los consumidores necesitan asegurarse de que tanto los proveedores de recursos como sus recursos per se sean confiables y seguros. En este sentido, la falta de confianza entre un consumidor y un proveedor tiene un impacto directo en la relación comercial, ya que el consumidor puede tener incertidumbre sobre qué proveedor elegir y cómo se comportará en un futuro cercano [9]. La confianza se entiende como la creencia en la fiabilidad, integridad y credibilidad en otra entidad o persona. Normalmente implica una voluntad de depender y tener expectativas positivas sobre las acciones, intenciones y comportamientos de la otra parte. Convencionalmente, cuando dos o más entidades desean establecer una relación pero no tienen conocimiento o experiencia previa entre sí, la confianza se vuelve crucial. La confianza ayuda a cerrar la brecha de la incertidumbre y permite que las entidades se involucren en una relación mutuamente beneficiosa. Además, la confianza puede ayudar en múltiples situaciones, como la mitigación del riesgo [10], al garantizar con cierto nivel de probabilidad que una entidad cumplirá con sus compromisos y obligaciones; la construcción de la fiabilidad [11], al avanzar, cooperar y colaborar de manera efectiva, sabiendo que la otra entidad espera comportarse con un cierto nivel de fiabilidad; la comunicación transparente [12], al compartir información, aclarar expectativas y mantener una comunicación coherente; o la recopilación de pruebas [13], proporcionando una posible resolución cuando aparezcan conflictos y disputas entre múltiples usuarios;

entre otros.

Cuando se trata de confianza, varios artículos han abordado las formas en que se puede definir [14, 15, 16] mediante métodos conocidos como basados en reglas [17], basados en *blockchain* [18], basados en teoría de juegos [19], basados en reputación [20], etc. Como se mencionó anteriormente, los mercados son ecosistemas en los que participan partes interesadas de múltiples dominios, por lo tanto, el conocimiento de incidentes y hechos históricos es fundamental para poder predecir los próximos. Del mismo modo, la posibilidad de perfilar los comportamientos de las partes interesadas basándose en interacciones previas es otra característica que se puede inferir de los mercados. Además, los mercados también se pueden visualizar como una comunidad donde las partes interesadas pueden ayudarse mutuamente a través de recomendaciones sobre terceros para ampliar y ayudar a la comunidad en este escenario interdominio, donde muchos consumidores pueden no tener información sobre los proveedores y viceversa. Teniendo en cuenta las declaraciones anteriores y los modelos basados en la confianza más importantes [21], los modelos de confianza basados en reputación son uno de los enfoques que mejor encajarían en los mercados de provisión de recursos y servicios bajo demanda, ya que cumplen con las suposiciones anteriores al permitir la predicción de los comportamientos futuros de las partes interesadas basándose en datos históricos y recomendaciones confiables proporcionadas por terceros. Además, tales modelos promueven evaluaciones transparentes de la confiabilidad, lo que permite que los consumidores y proveedores de diversos dominios se involucren con confianza, creando así un entorno de mercado descentralizado sólido y confiable. Además, los modelos de confianza basados en reputación fomentan la colaboración y la innovación dentro del ecosistema del mercado debido a que pueden incluir nuevas características que antes no se consideraban. Normalmente, los consumidores pueden establecer diversas combinaciones de características de todo tipo, a través de las Interfaces Gráficas de Usuario (del inglés Graphical User Interface, GUI), para filtrar los servicios y recursos disponibles de los proveedores, por ejemplo, por categoría, precio, ubicación geográfica y capacidades de *hardware*. Al contemplar la confianza como una nueva característica o *intent*, los consumidores podrían establecer nuevas relaciones comerciales con menor riesgo porque podrían tener una estimación de los comportamientos de los proveedores, así como comentarios que respalden o no respalden dicha intuición basada en evidencias previas.

Sin embargo, al igual que las tecnologías han ido avanzando en los últimos años para adaptarlas a las nuevas características y requisitos de las redes de telecomunicaciones, también deberían hacerlo los modelos de confianza. Los modelos de confianza anteriores analizaron principalmente el comportamiento de un usuario final para averiguar un nivel de confianza, sin embargo, 5G prevé el establecimiento de comunicaciones de extremo a extremo [22]. En este sentido, los modelos de confianza deben ampliar su alcance más allá de los usuarios finales para abarcar adicionalmente el análisis de entidades intermedias, por ejemplo, proveedores de servicios de red, proveedores de recursos de red o proveedores de software, entre otros. Vinculado a las comunicaciones de extremo a extremo, es fundamental estudiar nuevos habilitadores 5G y escenarios de aplicación en los que la confianza pueda ser relevante, ya que pueden descubrirse nuevos requisitos empresariales y de red. Por ejemplo, los mercados 5G aportan la flexibilidad de generar ofertas de múltiples partes [23] en las que múltiples recursos o servicios se combinan como un todo para los consumidores. En este sentido, los modelos de confianza anteriores deben evolucionar hacia enfoques que analicen cada servicio y recurso de las ofertas compuestas para descubrir posibles puntos débiles o entidades de desconfianza.

Por otro lado, las redes 5G promueven otros requisitos, como la orquestación sin contacto y la confianza cero, que añaden valores adicionales a los modelos de confianza. En

cuanto a la orquestación sin contacto, los modelos de confianza no deben diseñarse como servicios independientes, sino que deben permitir integraciones sin interrupciones con otros servicios críticos de las redes 5G y más allá de las redes 5G (B5G) [24]. En particular, los modelos de confianza deben evaluar su posible impacto en el ciclo de vida de la orquestación y tratar de formar parte de él sin comprometer el rendimiento. En cuanto a la confianza cero, implica uno de los requisitos más relevantes para los nuevos modelos de confianza basados en reputación. El principio de confianza cero fue definido por el Instituto Nacional de Estándares y Tecnología (del inglés National Institute of Standards and Technology, NIST) [25] e implica la ausencia de confianza inherente en cualquier usuario, dispositivo o red, independientemente de su ubicación. Por lo tanto, los modelos de confianza deben evitar la confianza implícita otorgada a cualquier activo, ya sea porque pertenezca a nuestro mismo dominio (*intra-dominio*) o a uno externo (*inter-dominio*), o si hemos establecido relaciones confiables en el pasado que finalizaron. El requisito de confianza cero pretende disminuir la superficie de ataque potencial haciendo hincapié en los controles de acceso estrictos, la monitorización continua y el apoyo a una estrategia de privilegios mínimos.

Basándose en lo anterior, existe una oportunidad para futuros trabajos que profundicen en el ámbito de la confianza aplicable a escenarios 5G. Estos esfuerzos es probable que estén precedidos por un análisis previo de posibles escenarios de cumplimiento, entidades o arquitecturas de red para las cuales se planearán las soluciones de vanguardia basadas en la confianza. Asimismo, pueden surgir requisitos novedosos de red y de negocio particulares con respecto a diseños anteriores centrados en soluciones orientadas a 4G, por lo que aparecen nuevas oportunidades de investigación en la hoja de ruta. En este sentido, también existe la oportunidad de diseñar y desarrollar soluciones de confianza innovadoras que no sólo puedan mejorar el rendimiento de las soluciones existentes sino también mejorar la experiencia del usuario. Además, los modelos de confianza presentan desafíos continuos, con una escasez de literatura que aborde el desarrollo de soluciones innovadoras aplicables en entornos dinámicos donde los usuarios pueden establecer relaciones entre dominios bajo demanda para garantizar QoS y QoE.

2 Objetivos

El objetivo principal de esta Tesis de Doctoral consiste en estudiar, analizar y abordar las principales limitaciones de los modelos de confianza basados en reputación en escenarios 5G y B5G, identificando nuevos requisitos de negocio y de red para evolucionar los modelos previos. Además, este trabajo tiene como objetivo desarrollar un marco escalable de gestión de confianza basado en reputación para un escenario de provisión de servicios bajo demanda en el que se cumplan múltiples requisitos de red y negocio. Más específicamente, se derivan varios subobjetivos específicos de este objetivo y se enumeran a continuación:

1. Analizar las propuestas actuales más destacadas en cuanto a modelos de confianza y reputación en varios escenarios 5G, estudiando las propiedades y características de los modelos de confianza.

2. Identificar un conjunto de habilitadores de confianza en las redes 5G y más allá, así como las similitudes entre sus escenarios de apliación en términos de propiedades y características.

3. Destacar las tendencias actuales de los modelos de confianza y describir los desafíos de investigación futuros.

4. Recopilar requisitos previos a 5G y 5G/B5G y los Indicadores Clave de Rendimiento (del inglés Key Performance Indicators, KPI) para los modelos de confianza de vanguardia.

5. Proponer un enfoque de pre-estandarización para los modelos de confianza basados en reputación más allá de 5G.

6. Diseñar y desarrollar un marco de gestión de confianza basado en reputación en una plataforma de mercado 5G descentralizada.

7. Analizar el impacto que el modelo de confianza basado en reputación podría causar en los procesos de descubrimiento y orquestación de provisión de recursos de red a través de experimentos exhaustivos.

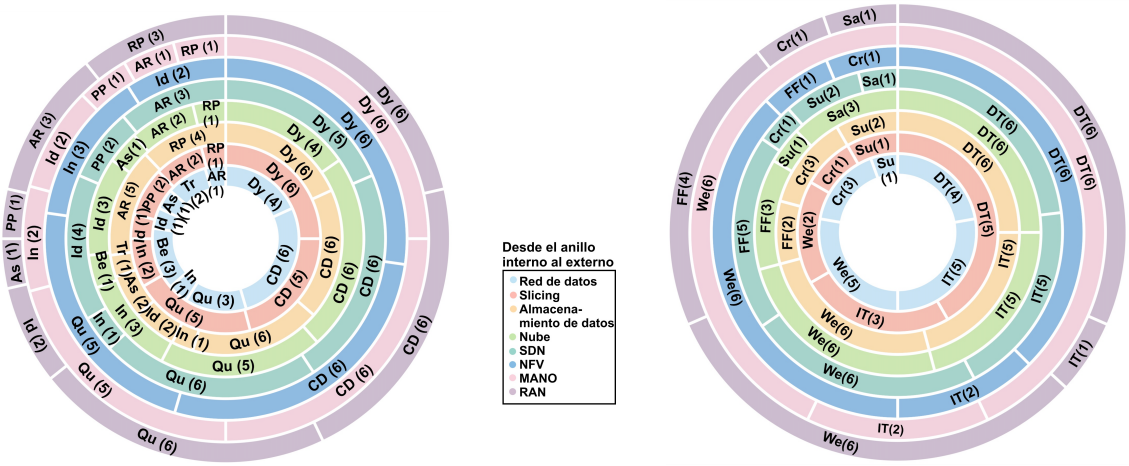
8. Implementar un conjunto de ataques de confianza en un entorno real de prueba, utilizando múltiples oleadas de comportamientos maliciosos, para probar la resistencia del marco y su impacto en las puntuaciones de confianza.

3 Metodología

Esta Tesis Doctoral se llevó a cabo como un compendio de publicaciones siguiendo un enfoque científico. En particular, esta Tesis Doctoral está compuesta por un conjunto de tres artículos de investigación publicados en revistas de prestigio indexadas en el *Journal Citation Report* (JCR). Por lo tanto, todo el trabajo realizado a través de estos tres artículos se dirigió a cumplir los objetivos de la Tesis Doctoral presentados en la sección anterior.

El primer hito de esta Tesis Doctoral fue el análisis en profundidad de los conceptos más importantes de los modelos de confianza. Antes de sentar las bases de los modelos de confianza, es un paso esencial comprender sus características intrínsecas. En este sentido, la primera publicación (Article 1–ACM_CSUR) consistió en el estudio de múltiples modelos de confianza con el fin de recopilar e identificar las principales propiedades y características que los conforman. A través de este estudio, se llevó a cabo un objetivo dual. En primer lugar, se intentó descubrir qué propiedades podrían aplicarse a los modelos de confianza independientemente de si pertenecen o no a un enfoque basado en reputación, y qué características solo podrían ser consideradas por los modelos basados en reputación. Por otro lado, el estudio describió el significado de cada una de ellas y qué acciones se deben realizar para cubrirlas sin tener en cuenta escenarios de aplicación específicos. Algunas de las propiedades identificadas podrían ser la dinamicidad, la dependencia del contexto o la recompensa y el castigo, mientras que la credibilidad, la satisfacción o los factores de olvido se presentaron como características relacionadas con la reputación. Es importante destacar que estas propiedades y características se tuvieron en cuenta posteriormente en las fases de diseño y desarrollo. Una vez investigadas tanto las propiedades como las características, realizamos una revisión de los activos o habilitadores 5G en los que la aplicación de la confianza podría ayudar a abordar sus debilidades o desafíos actuales, disponible en Article 1–ACM_CSUR. Entre los activos más relevantes encontrados en la literatura, podemos mencionar *red de datos, segmentación, nube, gestión y orquestación* (del inglés Management and Orchestration, MANO) o *almacenamiento de datos*, por mencionar algunos. Además, la primera publicación también evaluó qué similitudes y diferencias tenían los modelos de confianza en los activos 5G para determinar si las propiedades y características se consideraban de manera equitativa en las soluciones actuales del estado del arte. Con este fin,

evaluamos más de 45 publicaciones recopilando información sobre las propiedades y características contempladas, las principales fuentes de información para calcular los valores de confianza, los algoritmos y los resultados clave.



(a) Propiedades (b) Características

Figura 3: Propiedades y Características de los activos 5G y B5G

Una sinopsis gráfica de los trabajos analizados con referencias a los activos y sus principales propiedades y características se muestra en la Figura 3. Más específicamente, dicha figura reveló información valiosa, inferida del proceso de revisión bibliográfica, sobre las propiedades y características que dan forma al panorama de los modelos de confianza en los activos 5G y B5G. La distribución de estas propiedades ilustró cómo el dinamismo, la dependencia del contexto y la cuantificación son los más destacados, reflejando la importancia del aprovisionamiento de servicios y recursos bajo demanda en los escenarios de aplicación de estos habilitadores. Sin embargo, la identidad también es una propiedad predominante en todos los habilitadores, aunque en menor medida. En cuanto a las características, observamos cómo la confianza directa e indirecta, el factor de ponderación y el factor de olvido desempeñan un papel vital en la predicción de la confianza. No obstante, también se identificaron otras características que parecen estar poco representadas, como la subjetividad y la credibilidad, pero que tienen un gran potencial para mejorar los modelos de confianza y la fiabilidad de los mismos. Mediante el análisis y comprensión de los aspectos destacados en la Figura 3, futuros investigadores pueden centrarse en el diseño y desarrollo de soluciones que aborden las necesidades cambiantes de los modelos de confianza y reputación, y que permitan sistemas de comunicación más sólidos y confiables en el futuro.

Basándonos en el exhaustivo análisis realizado en Article 1–ACM_CSUR, se reconocieron varias tendencias actuales (las tres primeras de la siguiente lista) y desafíos de investigación (las tres últimas) relevantes para diseñar y desarrollar futuros modelos de confianza basados en reputación:

- *Conexiones extremo a extremo confiables*: no solo analizar a los usuarios finales, sino también a entidades intermediarias de cadenas confiables, como proveedores de servicios de red, proveedores de recursos de red o proveedores de software.
- *Automatización y gestión de servicios sin intervención humana*: integración transparente de la confianza con otros servicios de orquestación 5G sin comprometer el rendimiento.

- *Confianza Cero*: estudios recientes comenzaron a abordarlo debido al crecimiento exponencial de los paisajes de amenazas, aunque solo se tuvo en cuenta un enfoque revisado.
- *Estandarización de modelos de confianza basados en reputación*: se han realizado esfuerzos para estandarizar los modelos de confianza en la investigación y la industria, pero actualmente no existen pautas o estándares universales que puedan ser ampliamente adoptados por los investigadores en cualquier escenario de aplicación.
- *Confianza como servicio distribuido*: las soluciones de intercambio de recursos omnipresentes y escalables en redes 5G y B5G están impulsando la adopción de soluciones distribuidas y colaboración entre múltiples partes para el aprovisionamiento de servicios bajo demanda, los cuales plantean nuevos desafíos para los modelos de confianza en términos de diseño y desarrollo.
- *Ataques relacionados con la confianza*: el enorme crecimiento de dispositivos y servicios interconectados conlleva un aumento de la superficie de ataque, por lo que los modelos de confianza deben analizar los ataques basados en la confianza para ser resilientes.

Para abordar los desafíos mencionados en las declaraciones anteriores, otro logro significativo de esta Tesis Doctoral fue la propuesta de un enfoque de pre-estan-darización para modelos de confianza basados en reputación más allá de 5G (Article 2–Elsevier_CSI). Después de revisar la literatura sobre modelos de confianza para escenarios 5G y más allá, y descubrir las propiedades y características presentadas convencionalmente en soluciones de habilitación de confianza, planeamos diseñar nuestro modelo de confianza y reputación para afrontar todos los retos anteriores en una única solución. Sin embargo, no encontramos directrices o estándares ampliamente conocidos que pudieran ser seguidos para construir nuevos modelos de confianza y reputación en redes 5G y B5G, por lo que decidimos adentrarnos en este desafío. En este sentido, Article 2–Elsevier_CSI intentó apoyar a la comunidad científica que pretende abordar un desafío similar en un futuro cercano. En primer lugar, realizamos un análisis en profundidad de soluciones relacionadas con la pre-estandarización, estandarización, directrices o modelos de confianza a largo plazo. Este esfuerzo tuvo un doble objetivo, ya que nos permitió determinar si había propuestas que abordaran el desafío en el contexto de las redes 5G y B5G, y comprender las principales acciones e ideas a transmitir en una propuesta de pre-estandarización. Por lo tanto, analizamos publicaciones de (pre-)estandarización, proyectos de investigación relevantes europeos y no europeos, y organismos reguladores que habían estado trabajando o aún estaban trabajando en la estandarización de modelos de confianza basados en reputación o más allá de 5G. A través de este análisis, pudimos validar que las propiedades y características mencionadas anteriormente también se habían considerado en las propuestas de estandarización, así como ajustar algunas de ellas para que estuvieran bien alineadas. Entre las soluciones más significativas, destacamos los artículos de investigación de Gómez Mármol y Martínez Pérez [26] y Ylianttila et al. [27], el proyecto de investigación INSPIRE5G-Plus [28] y la organización reguladora Unión Internacional de Telecomunicaciones-T Y.3052 [29], ya que comparten la gran mayoría de nuestras propiedades, características y componentes que teníamos en mente para diseñar un modelo de confianza basado en reputación en redes más allá de 5G.

Una vez finalizada la revisión de la literatura, concluimos que no solo se habían tenido en cuenta propiedades y características en los modelos de confianza y reputación analizados, sino también requisitos e indicadores clave de rendimiento (KPI). En este punto,

recopilamos los requisitos de estandarización de modelos de confianza previos a 5G y los requisitos para los modelos de confianza en 5G y más allá de 5G. Además, observamos que algunos requisitos propuestos para modelos previos a 5G todavía se consideraban en las propuestas actuales. En este sentido, recopilamos 27 requisitos y 8 KPIs junto con su fuente de información y cómo las propuestas de modelos de confianza basadas en reputación deberían cubrirlos. Si bien es cierto que se pueden utilizar varias metodologías para implementar requisitos e indicadores clave de rendimiento, intentamos ser lo más genéricos posible para ayudar al lector a comprender las ideas clave para asegurar estos requisitos y KPIs. Por último, después de identificar los requisitos y KPIs presentes tanto en las redes 5G como en las redes más allá de 5G, presentamos una colección de sugerencias dirigidas a diseñar un modelo de confianza basado en reputación. Estas sugerencias sirvieron como principios orientadores para el desarrollo de modelos avanzados de confianza y reputación. Además, presentamos tecnologías y enfoques de vanguardia que se pueden considerar para cumplir con los requisitos y establecer modelos de confianza integrales.

En este momento, ya habíamos establecido las directrices para diseñar un modelo de confianza y reputación para los escenarios 5G y B5G, por lo que el siguiente paso era establecer un entorno específico para su diseño y desarrollo. Así, en la tercera publicación de esta Tesis Doctoral, presentada en el tercer capítulo (Article 3–IEEE_TDSC), se contextualizó el aprovisionamiento de recursos de una red 5G como escenario de aplicación del modelo de confianza basado en reputación a diseñar. Cabe mencionar que dicho escenario de aplicación está alineado con el proyecto europeo 5GZORRO del H2020 [30], donde hemos estado involucrado activamente, y una breve descripción del proyecto 5GZORRO junto con algunas publicaciones adicionales se pueden encontrar en la Sección 4.1. En cuanto al Article 3–IEEE_TDSC, presentamos a través de él cuatro grandes logros. Por un lado, diseñamos nuestro marco de confianza basado en la reputación, compuesto principalmente por cuatro módulos: (i) la *recopilación e intercambio de información*, (ii) el *cálculo de la confianza*, (iii) el *almacenamiento de la confianza*, y (iv) la *actualización continua* (véase la Figura 4). Teniendo en cuenta las propiedades, características y requisitos, describimos detalladamente las acciones significativas que deben llevarse a cabo en cada módulo y cómo podría desarrollarse dicho módulo para el escenario de prestación de servicios de red sugerido.

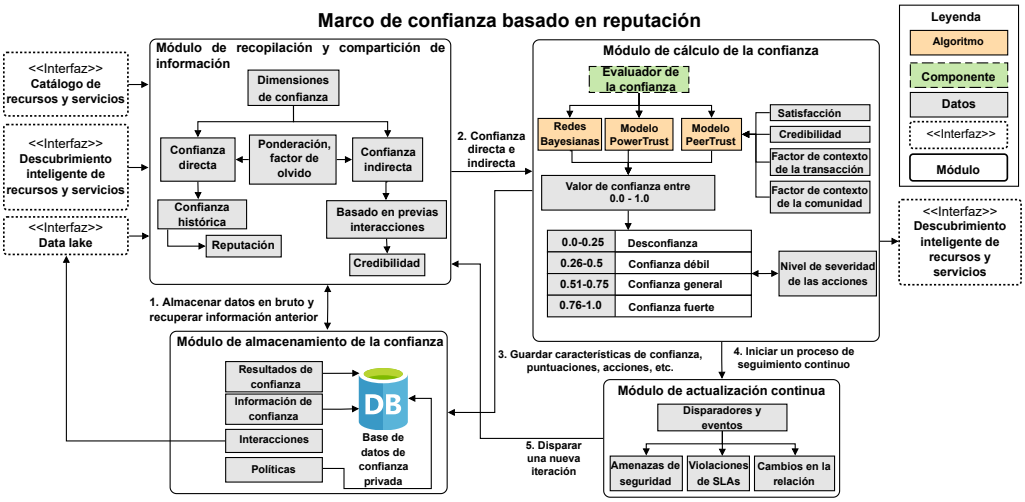


Figura 4: Visión general del diseño del marco de trabajo de confianza y reputación

En cuanto al módulo *recopilación e intercambio de información*, recoge datos en crudo

y estadísticas de varias fuentes de información, por ejemplo, el *Catálogo de recursos y servicios*, el *Descubrimiento inteligente de recursos y servicios* o el *Date lake*, entre otros. Además, dicho módulo introduce qué información específica puede utilizarse para cada fuente de información. Por ejemplo, el *Catálogo de recursos y servicios* puede proporcionar información relacionada con las ofertas de productos, como la geolocalización de servicios y recursos, el estado actual del ciclo de vida, la especificación del servicio, etc., o el *Data lake* puede dar soporte a la supervisión de los acuerdos de nivel de servicio (SLA) entre consumidores y proveedores. Después, toda la información se categoriza como confianza directa, es decir, la que procede de experiencias personales previas, o confianza indirecta, que se refiere a la información proporcionada por los recomendadores. En este punto, toda la información se envía al módulo de *cálculo de la confianza* para que la evalúe y proporcione una puntuación de confianza. Para ello, inspeccionamos diferentes algoritmos estadísticos que trataban escenarios distribuidos en los que se podían establecer conexiones entre pares. Entre los distintos candidatos, observamos que las redes bayesianas, el modelo PowerTrust y el modelo PeerTrust podían satisfacer nuestras afirmaciones anteriores. Sin embargo, finalmente elegimos el modelo PeerTrust porque aportaba una gran versatilidad a los investigadores, ya que se pueden formular libremente las cuatro dimensiones principales: satisfacción (del inglés satisfaction, S), credibilidad (del inglés credibility, Cr), factor de contexto de la transacción (del inglés transaction context factor, TF) y factor de contexto de la comunidad (del inglés community context factor, CF) (véase la Ecuación 3). Por tanto, seguimos los principios de PeerTrust, pero necesitábamos formular cómo se iba a calcular cada pilar. En este sentido, establecimos un modelo PeerTrust adaptado. Además, el modelo PeerTrust también contemplaba la principales de propiedades y características, indicadas previamente en Article 1–ACM_CSUR y Article 2–Elsevier_CSI, por lo que se adaptaba mejor a nuestros principios. Cabe señalar que la descripción exhaustiva de las dimensiones se detalla en varias publicaciones, donde [31] aborda el factor de contexto de la comunidad, y [32] aborda tanto la satisfacción (S) como el factor de contexto de la transacción (TF).

$$T(u) = \alpha \cdot \left(\sum_{i=1}^{I(u)} S(u,i) \cdot Cr(p(u,i)) \cdot TF(u,i) \right) + \beta \cdot CF(u) \tag{3}$$

Dado que la confianza no es un proceso puntual, nuestro marco de confianza basado en la reputación también contemplaba un módulo para almacenar pruebas y otro para actualizar continuamente las puntuaciones de confianza. El primero, denominado módulo de *almacenamiento de la confianza*, tenía como principal objetivo garantizar la seguridad de los datos, ya que existían dos tipos de fuentes de almacenamiento. Para empezar, el *Data lake* se aprovechó como plataforma compartida entre las partes interesadas para difundir la concienciación sobre los compromisos de confianza entre los participantes que conforman el ecosistema 5GZORRO. En este contexto, los recién llegados pueden identificar posibles asesores a los que consultar. Además, nuestro marco contemplaba una base de datos privada por dominio cuyo objetivo principal era disminuir el tiempo necesario para procesar la información en tiempo real, que se requiere cada vez que solicitamos información al *Data lake*, y mantener los datos personales, la información inferida de los datos en crudo, que no debe compartirse con la comunidad. Este último, denominado módulo de *actualización continua*, se encargaba de monitorizar los eventos en tiempo real para activar la reevaluación de una relación de confianza. En concreto, el marco de confianza basado en la reputación definía dos mecanismos de recompensa y castigo para ajustar las puntuaciones de confianza. Por ejemplo, declaramos un mecanismo de recompensa y castigo basado en eventos de seguridad inferidos de la monitorización de la red [31]. Dicho

mecanismo permitía identificar amenazas y comportamientos indebidos en el tráfico de la red y, en consecuencia, aplicar el castigo adecuado en caso de descubrir acciones inusuales.

En el tercer capítulo de este documento (Article 3–IEEE_TDSC) se propuso otro ejemplo para analizar el comportamiento de nuestro marco de confianza basado en la reputación cuando múltiples tipos de ataques relacionados con la confianza intentan alterar un flujo fiable. Más concretamente, presentaba una solución para mercados de servicios distribuidos 5G cuyo objetivo es apoyar el aprovisionamiento de recursos y servicios bajo demanda. Este último artículo presentaba un caso de uso (del inglés Use Case, UC) basado en el borde en el contexto de un paradigma de red virtual de entrega de contenidos (del inglés virtual Content Delivery Network, vCDN). En él se ponía de relieve la aplicación de la confianza para optimizar la orquestación y garantizar la selección de una porción fiable. Este caso de uso real implicaba a una parte interesada que buscaba la expansión de slice para gestionar el aumento de carga en su servidor vCDN en el borde del proveedor de servicios de contenidos (del inglés Content Service Provider, CSP). Por lo tanto, la parte interesada necesitaba adquirir recursos informáticos, concretamente una instancia de *slice*, en el *Edge* para evitar el enrutamiento del tráfico del núcleo de la red. Dado que el caso de uso se instanció en el marco del proyecto 5GZORRO, también detallamos en Article 3–IEEE_TDSC la integración de un marco de confianza y reputación en un mercado de servicios distribuidos 5G.

Otro hito significativo del Article 3–IEEE_TDSC fue la descripción de un nuevo mecanismo de recompensa y castigo bajo el módulo *continuous update*. Tal y como hemos presentado brevemente más arriba, se creó un mecanismo de recompensa y castigo basado en SLAs con el fin de averiguar cuándo una parte interesada debería poder participar en una relación o finalizar sus relaciones actuales debido a que ha tenido comportamientos incorrectos posteriores. En particular, el mecanismo basado en SLA se diseñó para ser flexible y adaptable, compatible con varios modelos de confianza y reputación. Además, siguió un enfoque basado en eventos, ajustando dinámicamente las relaciones en tiempo real en función de la tasa de predicción de incumplimiento (del inglés breach prediction rate, BPRate), el impacto de la confianza (del inglés impact of trust, ITrust) y la tasa histórica de violación de SLA (del inglés SLA violation rate, SLAVRate) (véase la ecuación 4). Además, utilizamos dos modelos difusos para evaluar el grado de pertenencia de las puntuaciones de confianza dentro de los niveles de confianza definidos (no confiable, poco confiable, moderadamente confiable, confiable y totalmente confiable) y para evaluar el nivel de ocurrencia de violaciones de SLA en la última ventana temporal (momentáneo, recurrente y persistente).

$$Pu(v,u) = \sum_{m=1}^{n} \frac{BPRate(u,m) + ITrust(v,u) \cdot SLAVRate(u,m)}{2} \tag{4}$$

Como último hito, necesitábamos comprobar si el marco de confianza basado en la reputación, sus diecinueve ecuaciones y sus mecanismos tenían el comportamiento esperado y eran resistentes a algunos ataques conocidos. Para demostrarlo, realizamos tres experimentos principales. No obstante, antes de los experimentos, también llevamos a cabo un proceso de ajuste de hiperparámetros para comprender cómo algunos parámetros esenciales, como el factor de olvido ξ y el porcentaje de aumento o disminución de nuestro mecanismo de castigo y recompensa n, pueden tener un impacto en las puntuaciones de confianza. Tras analizar los resultados, obtuvimos dos conclusiones principales. Por un lado, a medida que aumenta el valor de n, el alcance del castigo impuesto sobre las puntuaciones de confianza se verá limitado en contraste con un valor más bajo de n. Esto se refleja en probables cambios drásticos en los valores de confianza. Por el contrario, utilizando un factor de olvido ξ más cercano a 0.2 (hasta 1), se necesitaría un mayor número de interacciones

para equiparar $SLAVRate^{(t)}(u, m)$ a un incremento recurrente de las violaciones del SLA a lo largo del tiempo. Por lo tanto, la tasa de recuperación del mecanismo de recompensa debería ser más lenta en comparación con la del de castigo, ya que los modelos de confianza y reputación suelen dar prioridad a la identificación de los malos comportamientos de las partes interesadas en lugar de a sus acciones positivas.

En cuanto a los experimentos, nuestro marco de confianza basado en la reputación fue capaz de hacer frente a los ataques *on-off* aportando dos lecciones principales. En primer lugar, el mecanismo de recompensa impidió que los interesados superaran una serie de comportamientos erróneos sucesivos (2, 4 u 8 oleadas) en un breve plazo de tiempo. Así, se corrobora nuestra afirmación anterior de que los acontecimientos negativos influyen más en las puntuaciones de confianza que los positivos. En segundo lugar, el mecanismo de castigo permitió una disminución gradual de una puntuación de confianza alta en lugar de ponerla inmediatamente a 0, siempre que el contratiempo fuera un incidente aislado y la parte interesada se hubiera recuperado con éxito. Por último, el marco también era resistente a los ataques colusorios de mala reputación cuando había un número diferente de entidades maliciosas entre las poblaciones de recomendadores. Los resultados revelaron que el marco puede garantizar una precisión de 0,93 cuando el 30% de los recomendadores se comportaron de forma maliciosa y una precisión de 0,67 cuando el 50% de los recomendadores tuvieron comportamientos maliciosos. Además, observamos que la puntuación de confianza disminuía en un 8,6% cuando nuestro marco de confianza y reputación lograba una precisión del 33% en la identificación de comportamientos malintencionados, con una población maliciosa del 90% y 100/150 recomendadores. Por el contrario, cuando sólo el 30% de los recomendadores mostraban un comportamiento malicioso, la puntuación de confianza disminuía sólo un 2,1%. De este modo, nuestra solución fue capaz de distinguir con justicia los ataques colusorios de mala reputación, así como de hacer frente a oleadas continuas de mal comportamiento.

4 Otras publicaciones relevantes

Además, durante esta Tesis Doctoral, el candidato de doctorado también participó en un proyecto de investigación relacionado con aspectos de seguridad y confianza, liderando publicaciones significativas que mejoraron su experiencia, tanto en términos de capacidades de investigación como de trabajo en equipo colaborativo. A continuación, se enumeran las principales publicaciones relacionadas con el proyecto de investigación y el tema de la tesis.

4.1 5GZORRO: Seguridad y confianza sin intervención para la computación ubicua y conectividad en redes 5G

El proyecto 5GZORRO tenía como objetivo crear soluciones para la gestión de servicios, redes y seguridad en entornos multiparte, así como establecer un ecosistema confiable donde los interesados puedan interactuar en diferentes dominios administrativos. Un objetivo clave del proyecto 5GZORRO fue diseñar y desarrollar un marco de seguridad y confianza que esté integrado sin problemas con las plataformas de gestión de servicios 5G. Este marco tenía como objetivo mostrar la implementación de los principios de confianza cero dentro de entornos distribuidos que involucran a múltiples interesados. Además, facilitaba la gestión automatizada de la seguridad para garantizar la ejecución confiable y segura de cargas de trabajo desviadas en diversos dominios en redes 5G.

Este proyecto fue financiado por la Comisión Europea a través de la subvención n.º 871533, como parte de 5G PPP en Horizonte 2020, siendo la Universidad de Murcia uno

de los principales colaboradores y líder de un paquete de trabajo centrado en la automatización de la confianza, seguridad e inteligencia artificial. Las publicaciones relacionadas se enumeran de la siguiente manera:

- Adriana Fernández-Fernández, Michael De Angelis, Pietro G Giardina, James Taylor, Paulo Chainho, José María Jorquera Valero, Leonardo Ochoa-Aday, Diego R López, Gino Carrozzo, M Shuaib Siddiqui, "**Multi-party collaboration in 5G networks via DLT-enabled marketplaces: A pragmatic approach**", *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 550-555.
  DOI: 10.1109/EuCNC/6GSummit51104.2021.9482487

- José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Alexios Lekidis, Javier Fernandez Hidalgo, Manuel Gil Pérez, Muhammad Shuaib Siddiqui, Alberto Huertas Celdrán, Gregorio Martínez Pérez, "**Design of a security and trust framework for 5G multi-domain scenarios**", *Journal of Network System Management*, vol. 30, art. no. 7, pp. 1-35, 2022.
  DOI: 10.1007/s10922-021-09623-7
  JIF 2022: 3.6 (Q3)

- José María Jorquera Valero, Manuel Gil Pérez, Gregorio Martínez Pérez, "**A security and trust framework for decentralized 5G marketplaces**", séptimas Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), 2022, pp. 237-240, Bilbao, España.

5 Conclusiones y trabajo futuro

El crecimiento abrupto de servicios y dispositivos interconectados ha implicado, a su vez, un aumento en el número y tipo de relaciones entre entidades. Debido a la naturaleza de las redes 5G, cada vez es más común establecer relaciones con entidades pertenecientes a diferentes dominios administrativos. De hecho, uno de los desafíos a los que se enfrentan los usuarios finales a diario es la alta demanda de recursos para cubrir cargas de trabajo y mantener la calidad de servicio (QoS), lo cual es resultado del impulso de los servicios y dispositivos interconectados. Por lo tanto, los usuarios finales suelen depender con frecuencia de servicios, recursos e infraestructura ofrecidos por proveedores de infraestructura de red o proveedores de servicios/recursos de red, con el objetivo de mejorar sus capacidades actuales.

Sin embargo, la amplia variedad de oportunidades y soluciones útiles para respaldar la implementación de servicios, recursos o infraestructuras que permitan a los usuarios finales cubrir ciertas picos de carga introduce un nivel de confianza predeterminado en algunos casos. Dependiendo de los requisitos de los usuarios finales, pueden estar interesados en contratar soluciones para ampliar sus capacidades, como los enfoques de Infraestructura como Servicio (del inglés Infrastructure-as-a-Service, IaaS), cuando desean configurar recursos informáticos virtualizados en función de sus requisitos y servicios específicos, o los mercados, cuando, por el contrario, solo están interesados en utilizar recursos de terceros sin la necesidad de configurarlos desde cero ni mantenerlos. No obstante, los mercados están ganando protagonismo, ya que permiten solicitar recursos o servicios bajo demanda, lo que los hace útiles en escenarios altamente dinámicos donde se buscan soluciones flexibles y extensibles.

En ambos escenarios, la confianza es un pilar fundamental a considerar antes de establecer una relación comercial o seleccionar un servicio o recurso disponible, ya que la confianza puede ayudar a predecir cómo se comportará una entidad en un futuro cercano al conocer sus interacciones previas. No obstante, los mercados generalmente no permiten opciones de filtrado o características basadas en la confianza, pero suelen ofrecer a los usuarios finales opciones avanzadas para filtrar los recursos disponibles en función del rendimiento, el hardware o las características de ubicación, etc. Por otro lado, los modelos de confianza existentes no deben utilizarse directamente en escenarios de redes 5G de vanguardia, ya que constantemente surgen nuevas tendencias y desafíos. Por lo tanto, los modelos de confianza deben avanzar hacia nuevos enfoques que analicen y contemplen los nuevos requisitos, propiedades, características e indicadores clave de rendimiento (KPI) de la red y del negocio.

Con el objetivo de contribuir a las retos y limitaciones anteriores, esta Tesis Doctoral se centró en analizar los desafíos y brechas de los modelos de confianza basados en reputación en escenarios 5G y proponer una solución confiable para soluciones de provisión de servicios y recursos bajo demanda, especialmente en mercados de servicios multiparte. Teniendo en cuenta el principal objetivo y sub-objetivos enumerados en la Sección 2, se han logrado las siguientes contribuciones destacadas:

- En primer lugar, una revisión exhaustiva de la literatura sobre modelos de confianza y reputación en escenarios 5G. Mediante este análisis, Article 1–ACM_CSUR presentó un análisis en profundidad de las propiedades y características de suma importancia para los modelos de confianza. Además, se identificaron ocho habilitadores significativos y se revisaron y compararon los artículos más recientes relacionados con la confianza. Además, Article 1–ACM_CSUR describió una serie de tendencias y desafíos que posteriormente marcaron el rumbo de esta tesis.

- En segundo lugar, un enfoque de pre-estandarización para modelos de confianza basados en reputación más allá de 5G. Se derivó una colección integral de requisitos y KPIs al revisar y comparar documentos de (pre-)estandarización, proyectos de investigación y organizaciones reguladoras. Además, se sugirieron un conjunto de recomendaciones preliminares para abordar aspectos cruciales de las redes futuras y abordar la falta de modelos de confianza y reputación estandarizados más allá de la era 5G, tal como se describe en Article 2–Elsevier_CSI.

- En tercer lugar, un análisis de nuestro marco de confianza basado en reputación al enfrentar diferentes ráfagas de ataques relacionados con la confianza. Se creó un modelo adaptado de *PeerTrust* para calcular puntuaciones de confianza basadas en información estadística inferida de ofertas de productos, proveedores de red y recomendadores. Además, se diseñó un mecanismo de recompensa y castigo basado en acuerdos de nivel de servicio para adaptar continuamente los valores de confianza de una relación en curso cuando se producía una violación de un SLA, una predicción de infracción o una detección de infracción en tiempo real. Article 3–IEEE_TDSC también detalló un caso de uso basado en el borde en el que el marco propuesto se integró sin problemas con otros servicios vinculados a un mercado, desarrollados en el proyecto europeo 5GZORRO. Los experimentos demostraron que nuestro marco de reputación era resistente a los ataques de difamación y a los ataques *on-off*.

Estos hallazgos de investigación se han publicado en revistas de alto impacto indexadas en el JCR para compartir los resultados e influir potencialmente en la comunidad de investigación en general, como objetivo principal. Además, los resultados se han monitorizado

de cerca y se han compartido con el consorcio 5GZORRO y la Comisión Europea. Sin embargo, aún queda un camino considerable por recorrer en la implementación de modelos de confianza para escenarios 5G y B5G. Sin duda, existen desafíos sin resolver que requerirán contribuciones sustanciales en el futuro.

Más específicamente, la estandarización oficial de los modelos de confianza basados en reputación es fundamental para homogeneizar soluciones y avanzar en la misma dirección. Hasta la fecha, ha habido iniciativas individuales y organizaciones reguladoras (como ITU-T Y.3053) que buscan establecer modelos de confianza en los ámbitos de la investigación y la industria, respectivamente. Sin embargo, actualmente no existe una guía integral ni un estándar adoptado universalmente aplicable a la mayoría de las personas, independientemente del escenario de implementación específico. En este sentido, organizaciones como TM Forum e ITU-T X.5Gsec-t iniciaron esfuerzos para abordar la falta de estandarización en los modelos de confianza, pero desafortunadamente, las versiones públicas de estos borradores aún no están disponibles. En línea con los esfuerzos de estandarización, también existen otros requisitos previos, como un vocabulario común, modelos de información, modelos de procesos comerciales, APIs y métricas de evaluación, que deben abordarse antes de lograr un enfoque de estandarización final.

Como trabajo futuro, esta Tesis Doctoral identifica en primer lugar la necesidad de ampliar la resiliencia de nuestro marco de confianza basado en reputación, ya que los ataques *on-off* y los ataques de difamación no son los únicos que pueden afectar el comportamiento adecuado de los modelos de confianza. También deben abordarse ataques como el inflado de la reputación, la colusión o la manipulación de votos. Otro hito próximo es la aplicación de modelos impulsados por inteligencia artificial en lugar de algoritmos puramente estadísticos basados en ecuaciones personalizadas. Según nuestras experiencias personales durante esta Tesis Doctoral, los modelos estadísticos como PeerTrust o similares son capaces de proporcionar resultados precisos sin penalizar el rendimiento del ciclo de vida completo de los modelos de gestión de confianza. Sin embargo, cuando se realiza la comparación entre modelos estadísticos, este es un proceso complicado porque generalmente implica el (re)diseño o (re)definición de un nuevo conjunto de ecuaciones para cada modelo puramente estadístico. Por lo tanto, dicho proceso implica un elevado consumo de tiempo en contraste con lo que sucede cuando se comparan varios modelos de inteligencia artificial de manera más ágil en términos de *precision*, *recall* o *F1-score*. Asimismo, un modelo de confianza impulsado por la IA podría beneficiarse de la gran cantidad de datos de seguimiento que existen, además de la capacidad predictiva que algunos de estos modelos pueden proporcionar.

Además, esta investigación también detecta la necesidad de incorporar características de seguridad como otro pilar crucial de los modelos de confianza para soluciones más allá de 5G. La confianza y la seguridad, junto con la privacidad, son los fundamentos para ensamblar la futura sexta generación (6G) de las telecomunicaciones móviles. Por lo tanto, la seguridad es una de las principales preocupaciones al diseñar las futuras redes 6G. Esto se evidencia por algunas líneas de investigación de 6G que se centran en diseñar futuras redes 6G evaluando la seguridad de un servicio de red en un entorno de aplicación particular. En este sentido, nuestro modelo de confianza podría evolucionar hacia una función de evaluación de confianza impulsada por inteligencia artificial, capaz de garantizar aspectos de seguridad a partir de un conjunto de tecnologías aplicables a expertos en el dominio 6G. Por lo tanto, nuestro modelo de confianza, ampliado, podría respaldar el descubrimiento de una solución neutral y basada en propósitos para determinar la confiabilidad de los proveedores de infraestructura y red mediante el análisis de sus propiedades de seguridad y privacidad, tecnologías y patrones de amenazas, y teniendo en cuenta los requerimientos del

usuario a lo largo de su procesamiento de información habilitado por inteligencia artificial.

Bibliography

[1] D. Jiang and G. Liu, "An overview of 5G requirements," *Springer 5G Mobile Communications*, pp. 3–26, 2016.

[2] P. Roy, A. Tahsin, S. Sarker, T. Adhikary, M. A. Razzaque, and M. M. Hassan, "User mobility and quality-of-experience aware placement of virtual network functions in 5G," *Computer Communications*, vol. 150, pp. 367–377, 2020.

[3] N. Hassan, K.-L. A. Yau, and C. Wu, "Edge computing in 5G: A review," *IEEE Access*, vol. 7, pp. 127 276–127 289, 2019.

[4] J. Guo, C. Li, Y. Chen, and Y. Luo, "On-demand resource provision based on load estimation and service expenditure in edge cloud environment," *Journal of Network and Computer Applications*, vol. 151, p. 102506, 2020.

[5] H. N. Qureshi, M. Manalastas, S. M. A. Zaidi, A. Imran, and M. O. Al Kalaa, "Service level agreements for 5G and beyond: Overview, challenges and enablers of 5G-healthcare systems," *IEEE Access*, vol. 9, pp. 1044–1061, 2020.

[6] S. Bhat, R. Udechukwu, R. Dutta, and G. N. Rouskas, "Network service orchestration in heterogeneous 5G networks using an open marketplace," *IET Networks*, vol. 6, no. 6, pp. 149–156, 2017.

[7] M. Usman, M. R. Asghar, I. S. Ansari, F. Granelli, Q. H. Abbasi, and K. Qaraqe, "A marketplace for efficient and secure caching for IoT applications in 5G networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.

[8] A. Fernandez-Fernandez, E. Coronado, A. Erspamer, G. Samaras, V. Theodorou, and S. Siddiqui, "Unlocking the path towards intelligent telecom marketplaces for beyond 5G and 6G networks," *IEEE Communications Magazine*, vol. 61, no. 3, pp. 28–34, 2023.

[9] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, and T. Subramanya, "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture," in *2020 European Conference on Networks and Communications (EuCNC)*, 2020, pp. 254–258.

[10] M. Bradbury, A. Jhumka, T. Watson, D. Flores, J. Burton, and M. Butler, "Threat-modeling-guided trust-based task offloading for resource-constrained internet of things," *ACM Transactions on Sensor Networks*, vol. 18, no. 2, pp. 1–41, 2022.

[11] C. Benzaïd, T. Taleb, and M. Z. Farooqi, "Trust in 5G and beyond networks," *IEEE Network*, vol. 35, no. 3, pp. 212–222, 2021.

[12] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, and R. Sharma, "Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G," *Journal of Information Security and Applications*, vol. 67, p. 103179, 2022.

[13] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in internet of things," *Sensors*, vol. 19, no. 6, p. 1467, 2019.

[14] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Computing Surveys*, vol. 48, no. 2, pp. 1–40, 2015.

[15] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, 2017.

[16] S. Jaswal and M. Malhotra, "A detailed analysis of trust models in cloud environment," in *Second International Conference on Data Science, E-Learning and Information Systems*, 2019, pp. 1–5.

[17] K. Thangaramya, K. Kulothungan, S. Indira Gandhi, M. Selvi, S. Santhosh Kumar, and K. Arputharaj, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN," *Soft Computing*, vol. 24, pp. 16 483–16 497, 2020.

[18] R. Jiang, Y. Kang, Y. Liu, Z. Liang, Y. Duan, Y. Sun, and J. Liu, "A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance," *International Journal of Production Economics*, vol. 247, p. 108469, 2022.

[19] H.-J. Li, Q. Wang, S. Liu, and J. Hu, "Exploring the trust management mechanism in self-organizing complex network based on game theory," *Physica A: Statistical Mechanics and its Applications*, vol. 542, p. 123514, 2020.

[20] S. Priya and R. Ponmagal, "Trust based reputation framework for data center security in cloud computing environment," in *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023, pp. 1041–1047.

[21] A. Kanwal, R. Masood, M. A. Shibli, and R. Mumtaz, "Taxonomy for trust models in cloud computing," *The Computer Journal*, vol. 58, no. 4, pp. 601–626, 2015.

[22] F. Tang, B. Mao, Y. Kawamoto, and N. Kato, "Survey on machine learning for intelligent end-to-end communication toward 6G: From network access, routing to traffic control and streaming adaption," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1578–1598, 2021.

[23] A. Fernández-Fernández, M. De Angelis, P. G. Giardina, J. Taylor, P. Chainho, J. M. Jorquera Valero, L. Ochoa-Aday, D. R. López, G. Carrozzo, and M. S. Siddiqui, "Multiparty collaboration in 5G networks via DLT-enabled marketplaces: A pragmatic approach," in *2021 Joint European Conference on Networks and Communications & 6G Summit*, 2021, pp. 550–555.

[24] C. Benzaid and T. Taleb, "AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions," *IEEE Network*, vol. 34, no. 2, pp. 186–194, 2020.

[25] S. Rose, S. Mitchell, and S. Connelly. (2020) Zero trust architecture, NIST Special Publication 800-207.

[26] F. Gómez Mármol and G. Martínez Pérez, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems," *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 185–196, 2010.

[27] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6G white paper: Research challenges for trust, security and privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[28] C. Benzaid, P. Alemany, D. Ayed, G. Chollon, M. Christopoulou, G. Gür, V. Lefebvre, E. M. de Oca, R. Muñoz, J. Ortiz, A. Pastor, R. Sanchez-Iborra, T. Taleb, R. Vilalta, and G. Xilouris, "White paper: Intelligent security architecture for 5G and beyond networks," https://doi.org/10.5281/zenodo.4288658, 2020, [Online; accessed 22-August-2023].

[29] International Telecommunication Union-T Y.3052, "Overview of trust provisioning for information and communication technology infrastructures and services," https://www.itu.int/rec/T-REC-Y.3052, 2017, [Online; accessed 22-August-2023].

[30] European Commission, "Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks," https://cordis.europa.eu/project/id/871533, 2020, [Online; accessed 22-August-2023].

[31] J. Jorquera Valero, M. Gil Pérez, and G. Martínez Pérez, "A security and trust framework for decentralized 5G marketplaces," in *VII National Cybersecurity Research Conference (JNIC)*, 2022, pp. 237–240.

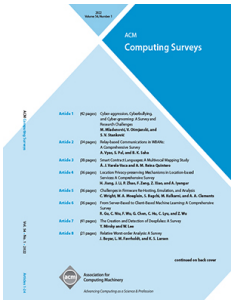
[32] P. G. Giardina et al., "5GZORRO D4.3: Final prototype of zero touch service management with security and trust," https://doi.org/10.5281/zenodo.7665890, 2022, [Online; accessed 22-August-2023].

Publications composing

the PhD Thesis

1

Survey of Trust Models and Enablers for 5G and Beyond Scenarios



Title:	Cutting-edge assets for trust in 5G and beyond: requirements, state of the art, trends, and challenges
Authors:	José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Manuel Gil Pérez, Alberto Huertas Celdrán, Gregorio Martínez Pérez.
Journal:	ACM Computing Surveys
JIF:	16.6 Q1-D1 (2022)
Publisher:	ACM
Volume:	55
Number:	11
Pages:	1–36
Month:	Nov
Year:	2023
DOI:	10.1145/3572717
Status:	Published

Abstract

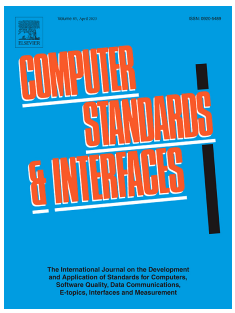
In 5G and beyond, the figure of cross-operator/domain connections and relationships grows exponentially among stakeholders, resources, and services, with reputation-based trust models being one of the capital technologies leveraged for trustworthy decision-making. This work studies novel 5G assets on which trust can be used to overcome unsuitable decision-making and address current requirements. First, it introduces a background and general architecture of reputation-based trust models. Then, it analyzes pivotal 5G assets on which trust can enhance their performance. In addition, this article performs a comprehensive review of the current reputation models applied to 5G assets and compares their properties, features, techniques, and results. Finally, it provides current trends and future challenges to conducting forthcoming research in the area.

Keywords

Trust and reputation models · Trust management · Requirements · 5G and beyond

2

Guidelines for reputation-based trust models



Title:	Toward pre-standardization of reputation-based trust models beyond 5G
Authors:	José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Manuel Gil Pérez, Alberto Huertas Celdrán, Gregorio Martínez Pérez.
Journal:	Computer Standards & Interfaces
JIF:	5.0 Q1 (2022)
Publisher:	Elsevier
Volume:	81
Pages:	1-18
Month:	Apr
Year:	2022
DOI:	10.1016/j.csi.2021.103596
Status:	Published

Abstract

In the last years, the number of connections in mobile telecommunication networks has increased rampantly, and in consequence, the number and type of relationships among entities. Should such interactions are to be profitable, entities will need to rely on each other. Hence, mobile telecommunication networks demand trust and reputation models that allow developing feasible communications in 5G and beyond networks, through which a group of entities can establish chains of services between cross-operators/domains, with security and trustworthiness. One of the key obstacles to achieving generalized connectivity beyond 5G networks is the lack of automatized, efficient, and scalable models for establishing security and trust. In this vein, this article proposes a pre-standardization approach for reputation-based trust models beyond 5G. To this end, we have realized a thorough review of the literature to match trust standardization approaches. An abstract set of requirements and key performance indicators has been extracted, and some pre-standardization recommendations proposed to fulfill essential conditions of future networks and to cover the lack of common trust and reputation models beyond 5G.

Keywords

Trust and reputation model · Trust standardization · Requirements · KPIs · Trustworthiness relationships · Beyond 5G

3

Trust for on-demand service provisioning

Title:	SLA-driven trust and reputation management framework for 5G distributed service marketplaces
Authors:	José María Jorquera Valero, Vasileios Theodorou, Manuel Gil Pérez, Gregorio Martínez Pérez
Journal:	Transactions on Dependable and Secure Computing
JIF:	7.3 Q1-D1 (2022)
Publisher:	IEEE
Pages:	1-13
Year:	2023
DOI:	10.1109/TDSC.2023.3292589
Status:	Accepted, In Press

Abstract

The fifth generation (5G) is characterized by massive growth in the number of stakeholders, interconnected devices, and available services distributed under different administrative domains. Distributed marketplaces aim at facilitating stakeholders in the quest and hiring of third-party resources and services. Establishing trustworthiness in such an open ecosystem is a cornerstone for the final deployment of these marketplaces in 5G networks and beyond. Hence, it is essential to build trust management systems that ensure the selection of reliable parties or assets in 5G distributed marketplaces. Thus, a reputation-based trust management framework is proposed to analyze stakeholder behavior patterns and predict trust scores to establish trustworthy relationships across domains. Furthermore, an Service Level Agreement (SLA)-driven reward and punishment mechanism is designed and developed on top of the reputation-based trust framework. Such a mechanism enables continuously adapting trust scores by gathering breach predictions, breach detections, and SLA violations in real time. Furthermore, an edge-based use case is presented to contextualize our reputation-based framework in a tangible enforcement scenario. In conclusion, four experiments were conducted on real-life testbeds demonstrating that our framework fairly distinguishes misbehaviors with a 67% accuracy, when a 50% population is corrupted, and is resilient to on-off and bad-mouthing attacks.

Keywords

Trust framework · reputation · SLA-driven · 5G · distributed marketplace