A Review of "Toward Pre-standardization of Reputation-based Trust Models Beyond 5G"

José María Jorquera Valero*[1], Pedro Miguel Sánchez Sánchez[1], Manuel Gil Pérez[1], Alberto Huertas Celdrán[2], and Gregorio Martínez Pérez[1]

[1]Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain
[2]Communication Systems Group (CSG), Department of Informatics (IfI), University of Zurich UZH, 8050 Zürich, Switzerland

***Abstract*—Mobile telecommunication networks have exponentially grown in recent years, resulting in complex relationships among entities. Establishing trust and reputation models is crucial for feasible communications in 5G and beyond networks to provide chains of services between cross-operators/domains with security and trustworthiness. Lack of automated, efficient, and scalable models is a significant challenge to achieving generalized connectivity beyond 5G networks. This article proposes a pre-standardization approach to reputation-based trust models by reviewing literature and extracting pivotal requirements and key performance indicators (KPIs). Besides, this manuscript seeks to establish, through a set of recommendations, a common framework for developing and implementing trust and reputation models that are automated, efficient, and scalable. Thereby, these models will enable entities in mobile telecommunications networks to rely on each other fully as well as cover essential conditions of future secure and privacy-preserving networks.**

***Index Terms*—Trust and reputation, trust standardization, requirements, 5G**

Tipo de contribución: *Investigación ya publicada*

I. Introduction

The emergence of 5G networks has brought new technologies and approaches that aim to address the limitations of previous generations [1]. One of the most significant changes in 5G is the support of a multi-stakeholder business model, which requires reliable cross-domain service chains to ensure the expected Quality of Service (QoS) and diminish risky connections that may compromise data integrity, user privacy, and the tasks being executed. In this vein, trust is one of the enabling technologies demanded to support 5G and beyond networks into a new era of more secure and trustworthy communications. In particular, 5G needs to guarantee trustworthy trading of heterogeneous services and resources for its dynamic and distributed ecosystem.

Trust is the measurable degree of assurance and belief derived from past interactions, combined with the expected value for future engagements. Prior trust models need to be adapted to the new trends and requirements of telecommunication networks. On the one hand, prior trust models were principally centered on end-users since they were the principal entity on which trust should be evaluated. Yet, today's 5G relationships are settled end-to-end (E2E). Therefore, such establishments entail the assessment of not only end-users, but also new stakeholders such as resource consumers, software suppliers, network service, and resource providers. On the other hand, trust models should evolve to embrace novel methods that have not been explored before, such as zero-touch [2] and zero trust paradigms [3]. In this sense, models require new designs and principles to facilitate automatic integration with other vital 5G services, such as decentralized marketplace [4], and avoid providing implicit trust to any entity in an intra- or inter-domain scenario (*zero trust*).

This work summarizes the research published in [5], whose main contributions were:

- Identification of requirements and KPIs from previous trust model standardization (pre-5G) and 5G/Beyond 5G (B5G) trust models to be met for upcoming approaches.
- Design of an abstract trust and reputation model for beyond 5G networks as well as a set of recommendations as part of a pre-standardization approach.

II. Requirements and KPIs progression from pre-5G to beyond 5G

Requirements and KPIs have a close relationship with the technologies and enforcement scenarios. Thus, requirements and KPIs tend to evolve together with new telecommunication generations, though some remain or are slightly adapted. In this regard, the extended version of this work [5] has thoroughly analyzed pre-5G, 5G, and B5G requirements (43 in total) and KPIs (11 in total) for reputation-based trust models. Concretely, this article summarized the most important requirements and KPIs for 5G and B5G trust models after initially analyzing research papers, research projects, and regulatory organizations.

Among the new requirements that should be considered in upcoming 5G trust models, we can underline the need for E2E relationships extending beyond a particular network section or asset to encompass the entire service chain. 5G scenarios also boost decentralized approaches, which entail eliminating central trustor entities. This eye-catching characteristic allows higher interconnection across domains, where data immutability, security by cryptography, and privacy-preserving should be ensured when sharing data among peers. Another crucial requirement, driven by NIST [3], is the absence of trust between entities participating in the same administrative domain or with which a long-standing relationship existed. To meet this zero trust requirement, trust models may leverage intra- and inter-domain policies or access control mechanisms that enable identification, authentication, and authorization of all entities engaged in trust-related procedures.

On the other hand, 5G-oriented trust models should be aligned zero-touch approach in terms of data pre-processing, information gathering, and trust establishment. They need to be automatic, efficient, and scalable. Finally, there are pre-5G requirements propagated toward new trust models, such as mitigating well-known trust attacks, reducing the excess power of newcomers, keeping track of historical interactions, etc.

ISBN:978-84-8158-970-2

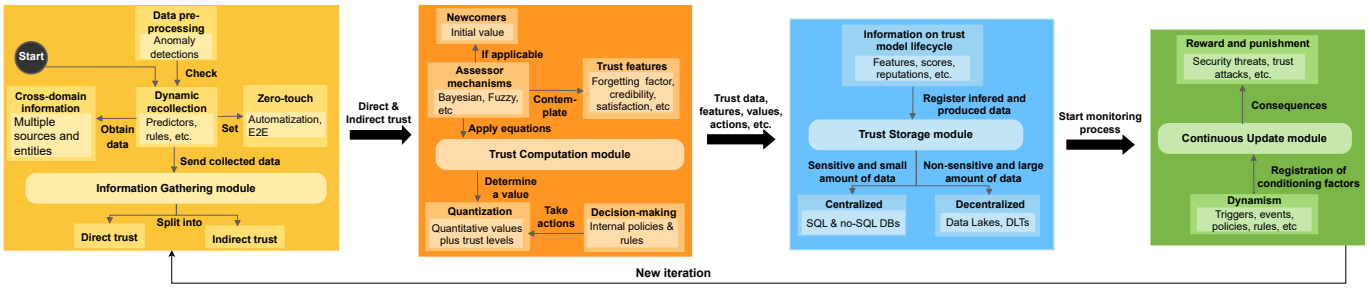

Fig. 1: Overview of trust and reputation model modules.

When it comes to KPIs, new trust-based models should think about the need for automatizing the trust establishment process, by overcoming a minimum user satisfaction, as well as enabling its automatic renegotiation when a stakeholder is joining or leaving the trust link. Likewise, such models should boost transparency and openness through the divulgation of external APIs used and public specifications to homogenize information flows. Last but not least, other pivotal KPIs can be the capability to analyze full-service chains without impacting the performance of other services consuming from trust models or the adaption of distributed, shared, cryptographically secure, and immutable technologies to integrate them with trust models and, consequently, ameliorate them.

III. Recommendations for Suitable Trust and Reputation Models Beyond 5G

In [5], a high-level reputation-based trust model has been designed to enable its adaption and development in 5G regardless of application scenario. In this sense, a set of guidelines were provided, bearing in mind prior requirements and KPIs. Fig. 1 displays the main modules to build trust over 5G and B5G networks.

Firstly, the *Information Gathering module* is a dynamic and multi-time mechanism triggered by predictors, rules, and data-driven or even-driven models, among others, to automatically collect and process information. This mechanism should be context-dependence, therefore irregularities in the data collected or changes in trust relationships need to be monitored and registered. Thereby, such a mechanism should also bring detection mechanisms to ensure the pre-processing steps will not disrupt the behavior of other modules that are fed with such information. These data recollection steps should contemplate automatization themselves following zero-touch approach [2], as well as distinguish information coming from own historical record (direct trust) and recommenders (indirect trust). Afterward, the *Trust Computation module* carries out the calculation and decision-making processes. Such a module should deal with newcomers and their privileges and participation in the system, seeking a balance between rights and opportunities to be elected. This module should also be in charge of palliating crucial factors such as time degradation, user's evaluation credibility, subjectivity, or dimension weighting, to name but a few. Additionally, the Trust Computation module assesses trust; however, there is no agreement on how to quantify it across different domains, so trust models need to choose the best method for their specific scenarios, i.e., continuous quantitative values, labels, fuzzy sets, etc. Finally, the output will power the decision-making process together with the defined actions, policies, and rules.

Keeping track over time is key for reinforcing future trust forecasting, which is the main goal of the *Trust Storage module*. In multi-stakeholder and cross-domain scenarios, solutions based on Data Lakes and distributed ledgers are gaining prominence against conventional databases. Real-time artificial intelligence-driven actions, decentralization, and immutability are the main characteristics pushing toward the integration of trust models with these trendy technologies. Last but not least, the *Continuous Update module* should consider reward and punishment mechanisms to adapt trust scores based on crucial triggers, i.e., security threats, changes in trust relations, or SLA violations, which induce dynamism and automatization in real time.

IV. Conclusions

This works analyzes the characteristics and limitations of reputation-based trust model standardization approaches in the current research field and, in consequence, recommend a set of novel requirements and KPIs to be considered by upcoming trust models involved in 5G and beyond scenarios. Furthermore, an abstract trust and reputation model beyond 5G is presented, consisting of four modules that fulfill the requirements and KPIs using novel technologies and methods, which can be used in multiple scenarios due to its level of abstraction. Last but not least, each module describes the upmost important steps and actions to be performed so as to determine a trustworthy stakeholder.

Acknowledgments

This work has been supported by the European Commission through 5GZORRO (grant no. 871533) and Hexa-X (grant no. 101015956) projects as part of the 5G PPP in Horizon 2020.

References

[1] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 90–96, 2014.

[2] G. Carrozzo *et al.*, "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture," in *2020 European Conference on Networks and Communications*, 2020, pp. 254–258.

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST Special Publication 800-207, 2020.

[4] A. Fernández-Fernández *et al.*, "Multi-party collaboration in 5G networks via DLT-enabled marketplaces: A pragmatic approach," in *Joint European Conference on Networks and Communications & 6G Summit*, 2021, pp. 550–555.

[5] J. M. Jorquera Valero, P. M. Sánchez Sánchez, M. Gil Pérez, A. Huertas Celdrán, and G. Martínez Pérez, "Toward pre-standardization of reputation-based trust models beyond 5G," *Computer Standards & Interfaces*, vol. 81, pp. 1–17, 2022.