6G Technology | DOI:10.1145/3512996

On 6G and Trustworthiness

BY GERHARD P. FETTWEIS AND HOLGER BOCHE

THE FIRST TWO generations of cellular—1G/2G—enabled ubiquitous voice connectivity. 3G/4G enabled broadband Internet. Even generations introduced services for business customers, and odd generations democratized them for consumers. 5G is enabling network-controlled robotics and XR, the Tactile Internet for business verticals,[4] and 6G will democratize this for consumers. One main avenue for achieving this is cost reduction.[6] Another avenue is radio access with joint communications and sensing.[7] New services are envisioned, such as low-altitude air traffic control, detecting, for example, bird migration and adapting drone services accordingly.

Not only data but physical and virtual objects will be controlled with 6G. This requires addressing *trustworthiness* of the system and its services at an unprecedented level. Indeed, trustworthiness must be understood in a new context, as we envision:

The trustworthiness of 6G technology has crucial implication. The University of Oulu in Finland recently acquired a self-driving car from Toyota to be used as a piece of research equipment where researchers can install their own instruments for testing.

- Localization of unheard precision,
- Sensing—not only radio and camera sensing, and
- Gesture recognition—also emotions.

How can we provide these new qualities without compromising legal and societal requirements, for example, General Data Protection Regulation (GDPR)? Every opportunity of improving sensing is an opportunity for *spying*. Trustworthiness for 6G is key. It comprises:

- Privacy
- Security
- Integrity
- Resilience
- Reliability
- Availability
- Accountability
- Authenticity
- Device independence

Every opportunity of improving sensing is an opportunity for spying. Trustworthiness for 6G is key.

Mathematical Frameworks

For communication tasks beyond Shannon's theory for message transmission, like event-driven-communication, transmission of status states, and joint communication and sensing, we must develop a Post-Shannon information theory. Several Post-Shannon transmission and storage schemes achieve exponential gains compared to the Shannon and Turing approaches.[2,6] Besides, initial Post-Shannon transmission methods allow a secure transmission of information, which cannot be broken even by quantum computers of arbitrary complexity. One important feature of 6G is resilience by design. This is particularly interesting since the successful execution of jamming attacks by an attacker cannot be detected by Turing machines.[6]

However, we must not only design systems that are robust against attacks from the outside, but also from within. Many cryptographic tasks have emerged in the last decade. Important examples are oblivious transfer, secure computing, bit commitment, and information masking. These tasks involve two or more untrusted parties with different types of behavior.[1] Some of the parties may be dishonest or even jam the communication system. It is well known that oblivious transfer is the most

PHOTO BY MIKKO TORMANEN, COURTESY OF UNIVERSITY OF OULU

powerful cryptographic two-party primitive.

We must develop new information theoretic tools to achieve oblivious transfer, secure computation, and information masking under real-world communication conditions.[10] Combining quantum communication with classical communication offers additional advantages. It is an interesting research question if one can combine tools from quantum information theory like entanglement with classical tools from the theory of zero-knowledge proofs to achieve device and hardware independent trustworthiness.

Platforms for Trustworthiness

Building a computing platform for trustworthiness poses enormous challenges; new tools are required, as previously noted. Some major ones are:

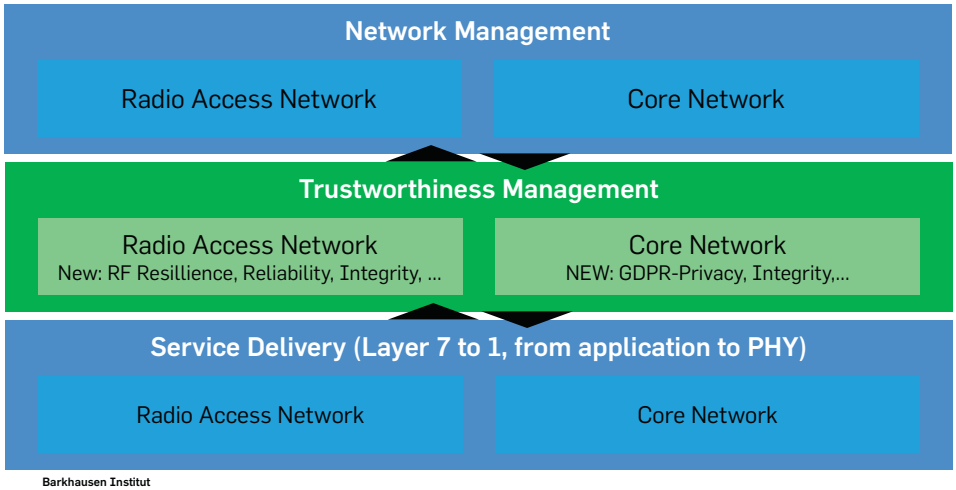
1. The hardware/operating system platform must be trustworthy. Today's separate design must change to an integrated approach.[3]
2. Isolation ("barrier skin"[5]) must guarantee GDPR conformance, for any (cloud) services.
3. With increasing sensing capabilities of terminals, the raw sensing data must be isolated (for example, encrypted[11]) at the source. Specialized processing containers in the edge or in terminals will ensure, for example, that identity and location are only accessed by approved services. The orchestration could be carried out by a meta operating system.[12]
4. Integrity will be a major issue. Current cellular standards are written in English text—not machine readable. 6G must be specified in an ontology that allows formal verification and cross-checks of implementation code, including updates. This ensures trust in cellular infrastructure adhering to specification.[9]
5. Reliability and availability will not only be a challenge to be served at the network layer, but also at the radio layer.[8]
6. Network resilience has always been key for telecommunications. But this must be extended to the Radio Access Network as 6G will control mobile robots, including classical steps: monitor, respond, and counter.
7. An open question regards device independence: Can this be addressed in the context of trustworthiness, or must standardized platforms be adopted?

The step from 5G to 6G is not small, in fact, it's huge; as the vision of 6G enabling personal mobile robotics and XR requires far more than an "update."

Must the network receive a new functional layer? Not only addressing network management and service delivery, but trustworthiness and integrity as a separate functionality, as illustrated in the accompanying figure.

Conclusion

The step from 5G to 6G is not small, in fact, it's huge; as the vision of 6G enabling personal mobile robotics and XR requires far more than an "update." Maybe even a new layer in network operations should be included, as trustworthiness will be a process not only for designing systems but must also be guaranteed during services. This is a grand challenge for electrical and computer engineering. C



Projected need for introducing a new *Trustworthiness Management Layer* (green).

References

1. Ahlswede, R., Csiszar, I. On oblivious transfer capacity. *Information Theory, Combinatorics, and Search*. LNCS 7777 (2013). Springer.
2. Ahlswede, R. and Dueck, G. Identification via channels. *IEEE Trans. Info. Theory 35*, 1 (Jan. 1989), 15–29.
3. Asmussen, N. et al. M3: A hardware/operating-system co-design to tame heterogeneous manycores. *ASPLOS 2016*.
4. Fettweis, G. The tactile Internet: Applications and challenges. *IEEE Vehicular Tech. Mag. 9*, 1 (Mar. 2014), 64–70.
5. Fettweis, G. Beyond 5G: What could it be? Presentation at IEEE 5G Summit Dresden, 2019; http://www.5gsummit.org/dresden-2019/
6. Fettweis, G. Boche, H. 6G: The personal tactile Internet—Open questions for information theory. *IEEE BITS the Info. Theory Mag.* DOI: 10.1109/MBITS.2021.3118662
7. Fettweis, G. et al. Joint Communications and Sensing. ITG Position paper; https://bit.ly/3EGwTcg/
8. Hößler, T. et al. Mission availability for wireless URLLC. In *Proceedings of IEEE Globecom*, 2019; DOI: 10.1109/GLOBECOM38437.2019.9013362.
9. Köpsell, S. et al. Open-RAN risk analysis. BSI Study (in German); https://bit.ly/3zbd6kj
10. Pereg, U. et. al. Classical State Masking over Quantum Channels. Sept. 2021; arXiv:2109.12647.
11. Vaikuntanathan, V. Homomorphic Encryption References; https://people.csail.mit.edu/vinodv/FHE/FHE-refs.html
12. Vilanova, L. et al. Caladan: A distributed meta-OS for data center disaggregation. In *Proceedings of the 10th Workshop on Systems for Post-Moore Architectures*, 2020.

Gerhard P. Fettweis is Scientific Director and CEO of the Barkhausen Institute, and Vodafone Chair Professor at TU Dresden, Germany. He coordinates the 5G++Lab Germany, and is PI at centers: 6G-life, CeTI, 5G++Lab Germany, and EKFZ.

Holger Boche is a professor and Chair at TU Munich. He coordinates the 6G Hub "6G-life" in Germany, and is PI at centers: 6G-life, CASA, and MCQST.

The authors thank their funding agencies and companies, particularly the centers listed in their affiliations.