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, and 6G will democratize this for consumers. One main avenue for achieving this is cost reduction. Another avenue is radio access with joint communications and sensing. 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:

- 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

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. 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.

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. Some of the parties may be dishonest or even jam the communication system. It is well known that oblivious transfer is the most
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. 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.
2. Isolation (“barrier skin”) 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) 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.
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.
5. Reliability and availability will not only be a challenge to be served at the network layer, but also at the radio layer.
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.”

**References**