ITU KALEIDOSCOPE ONLINE 2021

6-10 December 2021

Future industrial networks: Requirements, challenges, research and standardization needs

Marco Carugi
Huawei Technologies
European Research Center
France

Session 2: Networking requirements and solutions for IoT and industrial applications

Paper S2.3: Future Industrial Networks: Requirements, Challenges, Research and Standardization Needs

Outline

- Introduction
- Application scenarios and network challenges
- Fundamental networking technology advances
- The need of further network research and standardisation in support to future industrial applications
- Conclusion

Introduction

Future advances in networking technologies will be driven by future applications

The digital transformation is affecting most of the industries and a large spectrum of applications is expected to be deployed in future industrial networks

- machine-to-machine communications for industrial and robotic automation
- immersive and "real" user experience leveraging holograms, haptics, and other sensory data
- failsafe network services enabling mission-critical applications such as self-driving vehicles and drones, with rapid infrastructure adaptation and reaction to unexpected events
- diverse applications leveraging different types of network communications (land as well as air, space and sea communications) - e.g. mining and emergency/disaster recovery applications
- many new applications driven by artificial intelligence and depending on myriads of data feeds
- some future applications will need high precision networking services, others will be distortion tolerant

The usage of networking technologies in many facets of future industries and society requires further research and standardization efforts on networking technologies

The goal is to enrich the network with new capabilities which can address the challenges of emerging and future industrial applications.

Application scenarios and key network requirements - 1 of 2

Selected emerging industrial applications expected to be largely deployed in future industrial networks [selection aiming to highlight key network requirements]

- IoT enabled industrial and robotic applications
- Smart grid applications – see Fig.1
- Haptic communication enabled applications – see Fig. 2
- Integrated satellite-terrestrial network enabled applications – see Fig. 3

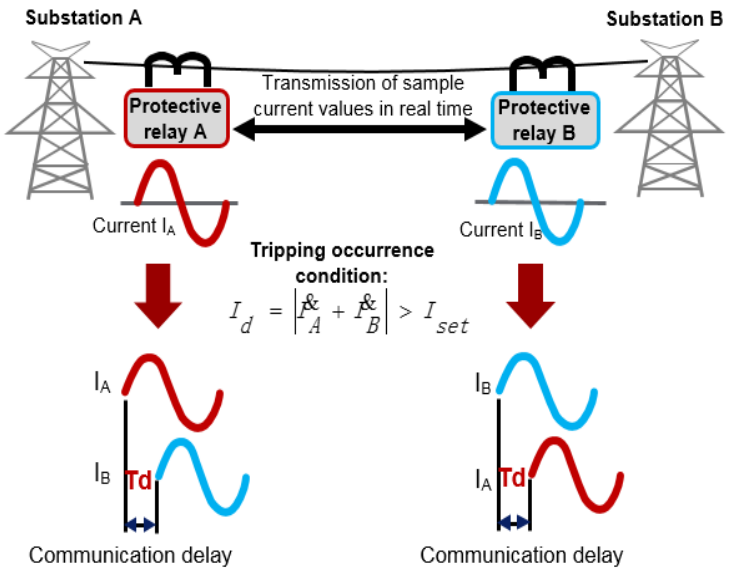


Fig. 1 Differential protection for transmission lines

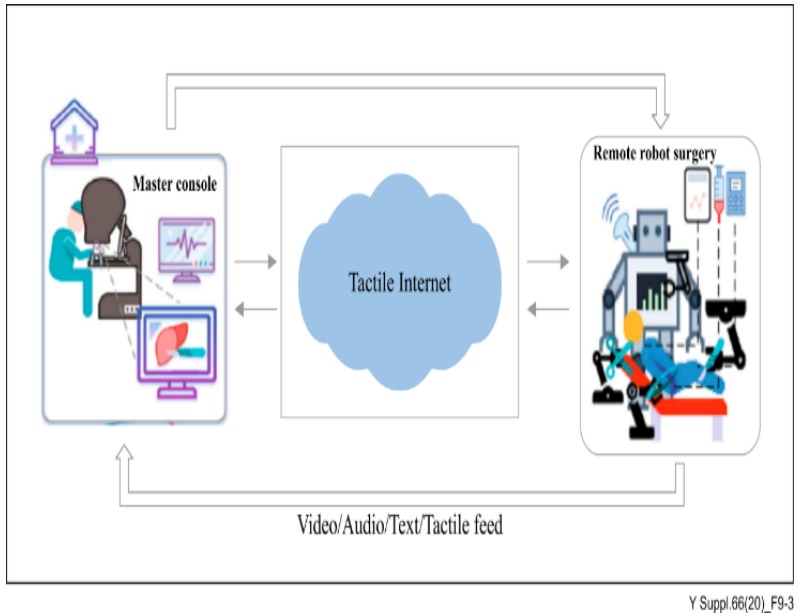


Fig. 2 Remote surgery

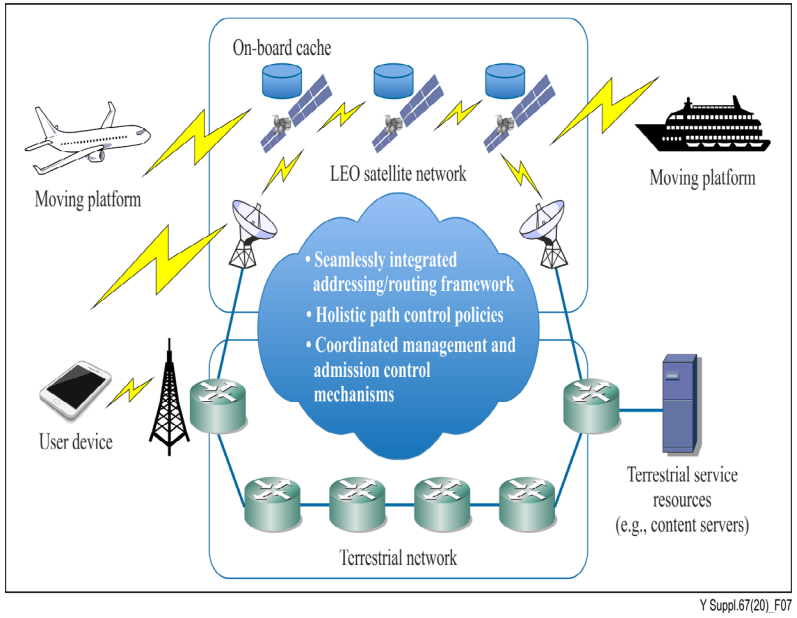


Fig. 3 Integrated satellite-terrestrial network

Application scenarios and key network requirements - 2 of 2

Key network requirements of the selected industrial applications

IoT enabled industrial and robotic applications

- **Low latency** (from sub-ms to 10 ms)
- Time synchronization (deterministic latency)
- **Small and bounded jitter** (sub-microsecond level)
- **High security and reliability**
- **Large-scale deterministic networking support**

Smart grid applications

- **Low latency** (5 ms)
- **Small and bounded jitter** (250 us)

Haptic communication enabled applications

- High bandwidth (especially important in case of remote monitoring)
- **Ultra-low and deterministic latency** (from 5 ms to sub-ms level for instantaneous haptic feedback in tactile cases)
- **Synchronization** (significantly shorter than delay)
- **High security and reliability, privacy** (for critical applications, e.g., those involving human lives and high-value machinery)
- Prioritization (based on streams' immediate relevance and criticality)

Integrated satellite-terrestrial network enabled applications

- **Flexible addressing**
- **Integrated routing framework**
- Holistic path control policies
- Coordinated management and admission control mechanisms
- Novel requirements at the satellite side (bandwidth capacity, admission control, edge computing and storage)

Network challenges

Emerging industrial applications will not only require abundant bandwidth and ubiquitous connectivity, **new network capabilities will have to be provided that are not supported today**

It is needed to move beyond best effort and support a new concept of "high precision"

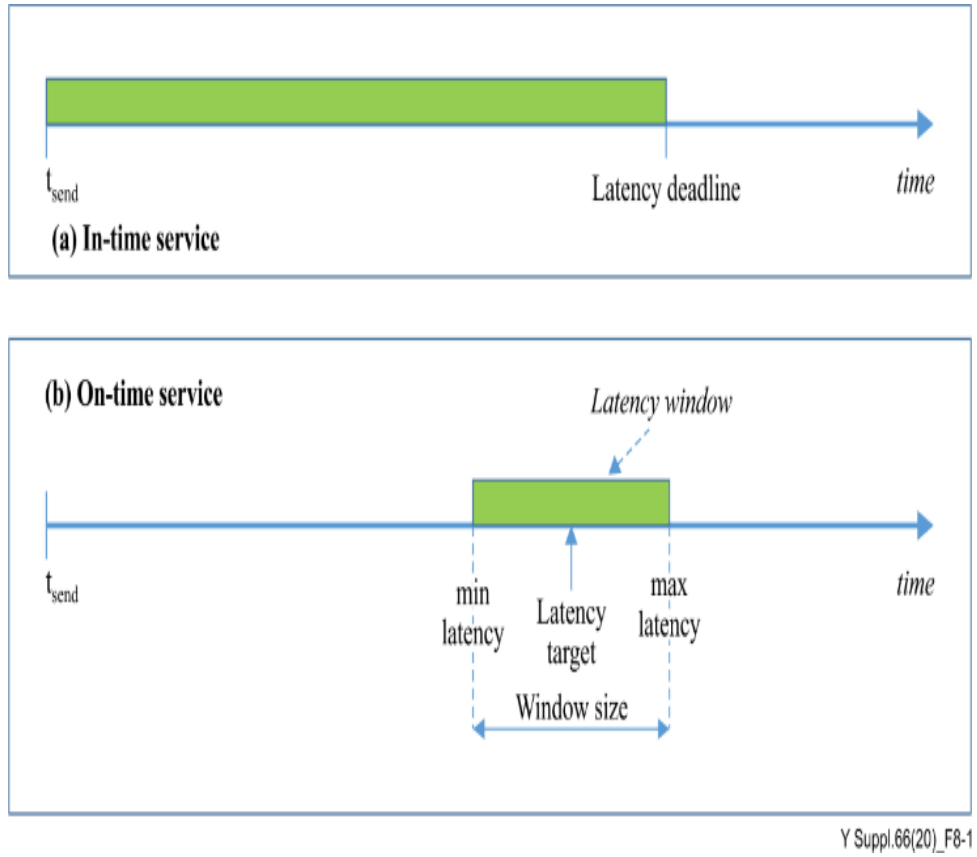
- quantifiable latency guarantees on a large scale basis
- synchronization of packet flows across multiple communication channels and communicating parties
- behavior in light of congestion and resource contention

Critical challenges of future industrial applications

- **precise timing and latency of packet delivery, coupled with ability of precise control of that latency** - technologies for support of time determinism at a large scale are essential (quantifying precise latency objectives given various constraints)
- **integrated and flexible addressing and routing mechanisms** - technologies for flexible addressing and routing are essential to leverage in a uniform way different types of network communications, and meet application requirements via (semantics-based, constraint-based) customization of packet routing
- **high security, privacy and reliability** - technologies for intrinsic security and privacy are essential to address inherent security, privacy and trustworthiness vulnerabilities of current IP based networks

Fundamental networking technology advances - Time determinism

- **“In-time" services** (latency not to be exceeded) and **“On-time" services** (maximum and minimum latency) with respect to the latency objectives imposed on the packets
  - not only engineering and optimizing the network for "low" latency, the “actual latency” needs to be measured and latency objectives provided as a specific parameter for the service
- Time deterministic capabilities need to be **applied both within and beyond single islands of communication**. Large scale layer-3 networks should support the coexistence of deterministic services and best-effort services.
- **Time deterministic capabilities need to be enabled at layer 3 for large scale support**, extending the radio capabilities back through the IP-based backhaul network and across the IP-based core network/Internet.
- It is necessary to **devise suitable data plane extensions with accompanying control plane solutions** (providing centralized, distributed and hybrid control signalling).



Fundamental networking technology advances - Flexible addressing and routing

- Increasingly varied service expectations require Service Providers to be aware of the delivered services and have sufficient information about how individual packets should be treated to meet the requirements.
- **Semantic addressing** caters to increasing number of services that utilize the network data plane. Driven by networks not limited to locator-based addressing and Internet routing solutions, but using sector specific packet forwarding solutions based on service or content identifiers, sensor/host identifiers, others – **towards the Internet integration of those vertical networks which are currently not integrated**
  - Different techniques have been proposed
  - New semantics can be deployed for new capabilities, better QoS, higher flexibility, efficiency, incremental deployment of new technologies on limited domains
- **Flexible length addressing** caters to increasing number of specialized network deployments, driven by the recognition of IP header overhead. Efficient support of variable length addressing alongside global reachability.
  - Localized forwarding based on short purpose-oriented addresses (interconnection through hierarchy)
  - Extensible address scopes allowing new network layer functionalities without standardization of extensions
- **Semantic routing** (routing packets containing IP addresses with additional semantics) and constraint-based routing can utilize flexible addressing for scoped semantic actions (enriched by provider-defined constraints)
  - Provisioning of services without explicit mapping services, latency reductions

Fundamental networking technology advances - Intrinsic security and privacy

- **Intrinsic security and privacy capabilities are needed to address inherent security, privacy and trustworthiness vulnerabilities of current IP based networks,** including source address spoofing, privacy leak, trust model weakness, and distributed denial of service (DDoS) attacks.
- Capabilities have to maximally protect user privacy, consolidate distributed trust basis, and build secure and trustable networks, in order to meet the privacy protection requirements represented by GDPR and the security and trustworthiness requirements of industry-wide interconnection
  - It is needed to verify if a packet is authorized to enter into the network and if it is sufficiently integrity protected. Advanced mechanisms for time sensitive services, advanced encryption for privacy-preserving network operations.
  - Security mechanisms could be also used for network trustworthiness, including verification of the trustworthiness of network nodes and packets themselves.
  - Privacy protection enabling mechanisms are needed, including anonymization, opaque user data, secured storage and flow anonymization.
  - It is essential to prevent common tracking at application level (and more) due to the locator-based addressing being used at the routing layer. Decoupling of the locator addressing from the user identification at routing level can make long term tracking of users impossible.
  - Additional mechanisms are needed to ensure privacy and confidentiality of network layer information with respect to cross-domain end to end services.

Need of further network research and standardisation – Time determinism

Efforts are required in terms of network technologies to enhance the network with new capabilities. Relevant research studies and standards development efforts up to present time show limitations towards the identified network requirements of emerging and future industrial applications.

- Current limitations: **the network support of time deterministic capabilities on a large scale is presently not addressed by the main concerned standardization activities**
  - IEEE TSN aims to provide deterministic service inside a LAN over a short distance, and is not routing-capable. TSN does not aim to provide on-time guaranteed service over large scale networks and over longer distances. Like IntServ, TSN is geared towards constant bit rate (CBR) traffic.
  - IETF DetNet aims to ensure a bounded latency and low data loss rates within a single network domain. Scalability remains a challenge as DetNet does not change the existing data plane, specifically constraining the study to Autonomous System-internal mechanisms. Data plane scalability issues and, again, CBR reservations.
- Research and standardization needs: **technologies that can be both effective in ensuring deterministic latency for all types of traffic and scalable to support a large number of simultaneous flows.**

Need of further network research and standardisation - Flexible addressing and routing

- Current limitations
  - **Several semantic addressing techniques have been developed but in a fragmented way**, with interoperability issues between limited domains or between individual routers, and the possibility of increased fragility or even security and privacy leakage.
  - Information Centric Networking technology (ICN) is now reaching maturity, but limited semantic-based networking support is enabled and technical discussion on ICN deployment and operation still continues.
  - Although implemented in an increasing number of limited domain deployments, flexible length addressing has not yet found its way in standardization.

- Research and standardization needs
  - A more holistic approach for architectural patterns and common building blocks based on semantic routing
  - Routing advances devising an integrated, flexible, hierarchical addressing scheme for the routing layer, enabling IPv6 backwards compatibility but also intra-domain short length addresses and integration of vertical-specific name resolution/mapping systems, such as semantic addressing.
  - Security and privacy of future addressing and routing solutions
  - New routing technologies inside limited domains for delivery of new capabilities and better QoS
  - **Robust standardization effort** (need of coexistence with legacy addressing and routing)

Need of further network research and standardisation - Intrinsic Security and Privacy

Current limitations: **some initial efforts on supporting intrinsic security and privacy in the IP based networks have been observed, but outstanding issues have been addressed with limitations and not complemented yet by relevant standardization efforts**

- Concerning security, the security and network functions offered by Secure Access Secure Edge (SASE) [Gartner, 2019] have relative low performance due to the software implementation, not suitable for applications with strict QoS requirements.
  - Enabling the IP based networks with some security functions, like device authentication, access control, DDoS attack protection, could complement the SASE software implementation.
- Concerning privacy protection, while the payload in current IP based networks is typically protected at application level, the IP overhead, which may contain valuable personal information, is still exposed for packet routing purpose: initial solutions have been provided (Gnatcatcher, iCloud Private Relay, The Onion Router) but have limitations (applications demanding highly interactive communication).
  - Making the communications in the IP based networks anonymous could be a possible solution.

Further research and standardization needs are well recognized.

Conclusion

- The network challenges raised by emerging and future industrial applications need to be addressed by relevant network technology advances.
    - Building on industrial application scenarios and related requirements on the underlying network infrastructure, advances in three networking technology areas are fundamental to address the identified network challenges: time determinism, flexible addressing and routing, intrinsic security and privacy.
- Relevant research studies and standards development efforts up to now show limitations towards the identified network requirements. It is necessary to progress as soon as possible further research studies and standardization efforts.
- **Standardization will be critical to ensure stability, scalability and interoperability of potential solutions.**
- **ITU-T has a key role to play in the context of concerted and comprehensive international standardization for networks in support to emerging and future industrial applications.**

ITU KALEIDOSCOPE
ONLINE 2021

Thank you!