ITU Workshop on security for 5G and beyond
22 August 2022

KDDI Research

Brief introduction to the ITU-T FG NET-2030 and Japan's Beyond 5G Promotion Consortium on their security-related activities

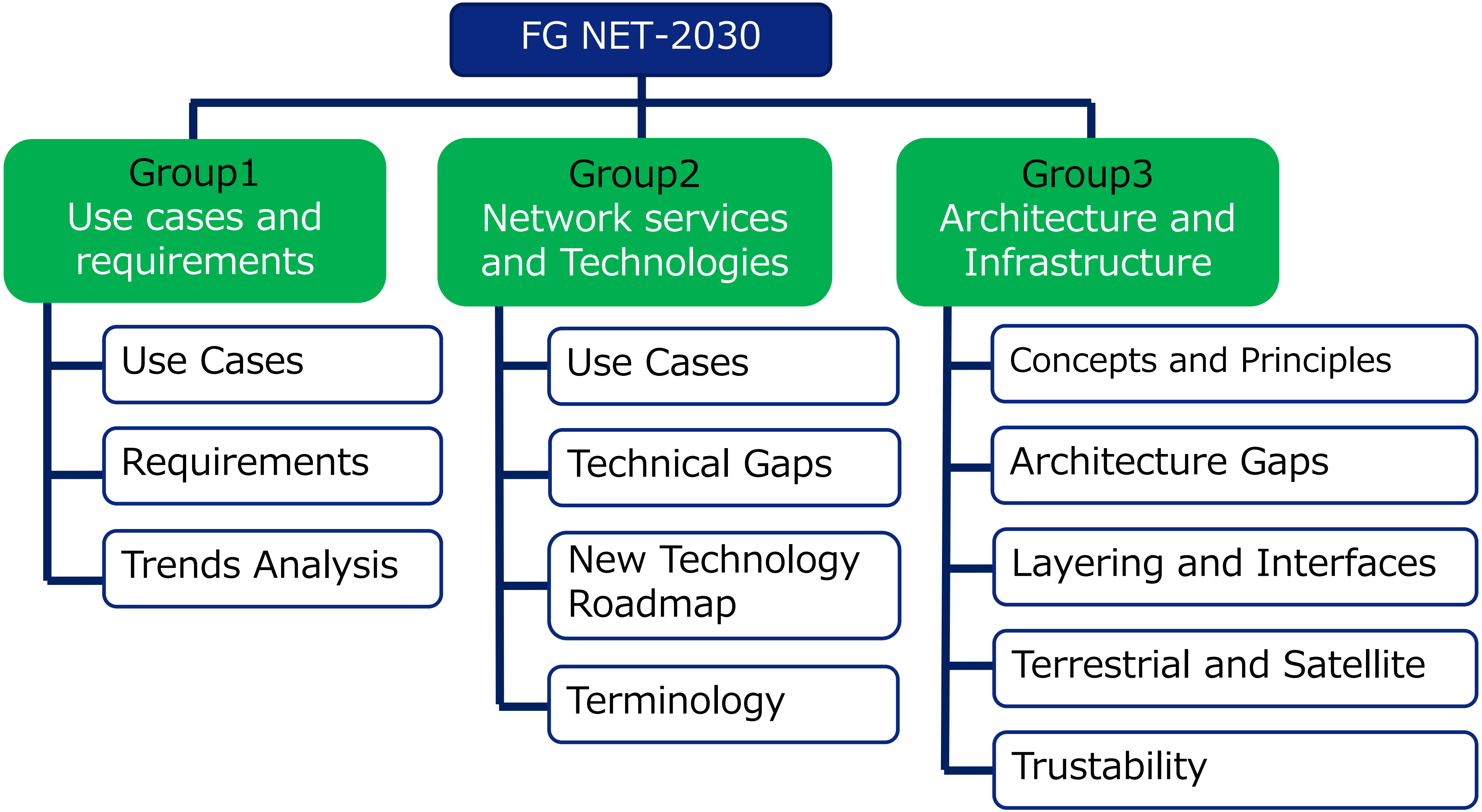
Yutaka Miyake
KDDI Research Inc.

Security Activities of ITU-T FG NET-2030

Outline of FG NET-2030

- Title: ITU-T Focus Group on Technologies for Network 2030
- Start: July 2018, End: July 2020
- Objectives:
  - To study, review and survey existing technologies, platforms, and standards for identifying the gaps and challenges towards Network 2030, which are not supported by the existing and near future networks.
  - To formulate all aspects of Network 2030, including vision, requirements, architecture, novel use cases, evaluation methodology, and so forth.
  - To provide guidelines for standardization roadmap.
  - To establish liaisons and relationships with other SDOs.
  - Network 2030 focuses on the fixed data communication networks.
- Deliverables:
  - White Paper: Network 2030 - A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond (May 2019)
  - Deliverable: New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis (October 2019)
  - Technical Report: Representative use cases and key network requirements for Network 2030 (January 2020)
  - Technical Report: Network 2030 - Gap Analysis of Network 2030 New Services, Capabilities and Use cases (June 2020)
  - Technical Report: Network 2030- Additional representative use cases and key network requirements for Network 2030 (June 2020)
  - Technical Specification: Network 2030 Architecture Framework (June 2020)
  - Technical Specification: Network 2030 - Terms and Definitions (June 2020)
  - Technical Report: Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020 (June 2020)

Structure of FG NET-2030

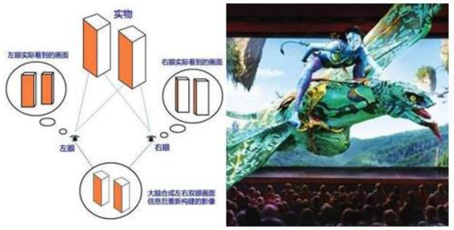


Representative use cases

KDDI Research

1. Holographic type communications (HTC)

2D Image
Flat Plane
No Real 3D Effect
Can have "3D Illusion"

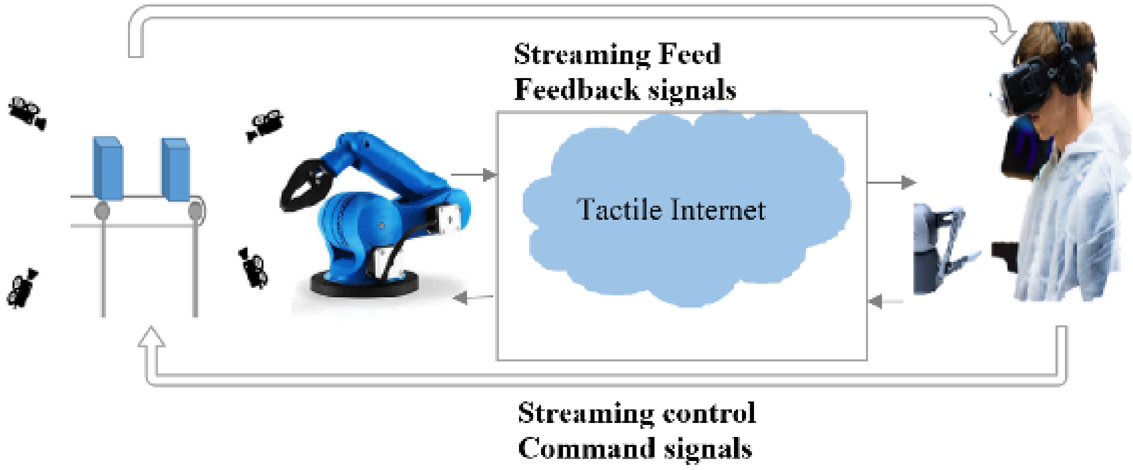


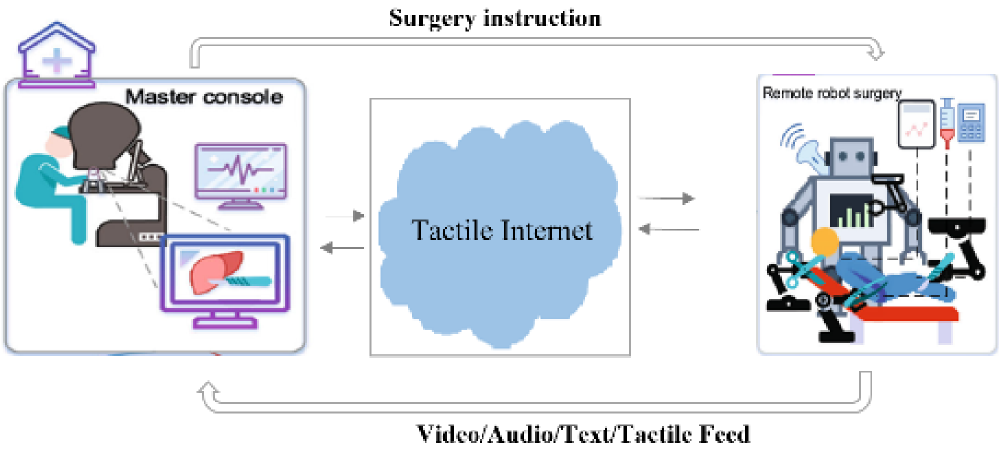
3D Movie
Binocular Parallax for 3D
Physiological Function with
Eyes and Brain

Holographic Display
All 3D Cues for Objects
(Wave-front Reconstruction)

Holographic Display can satisfy all nature human observation for 3D objects.

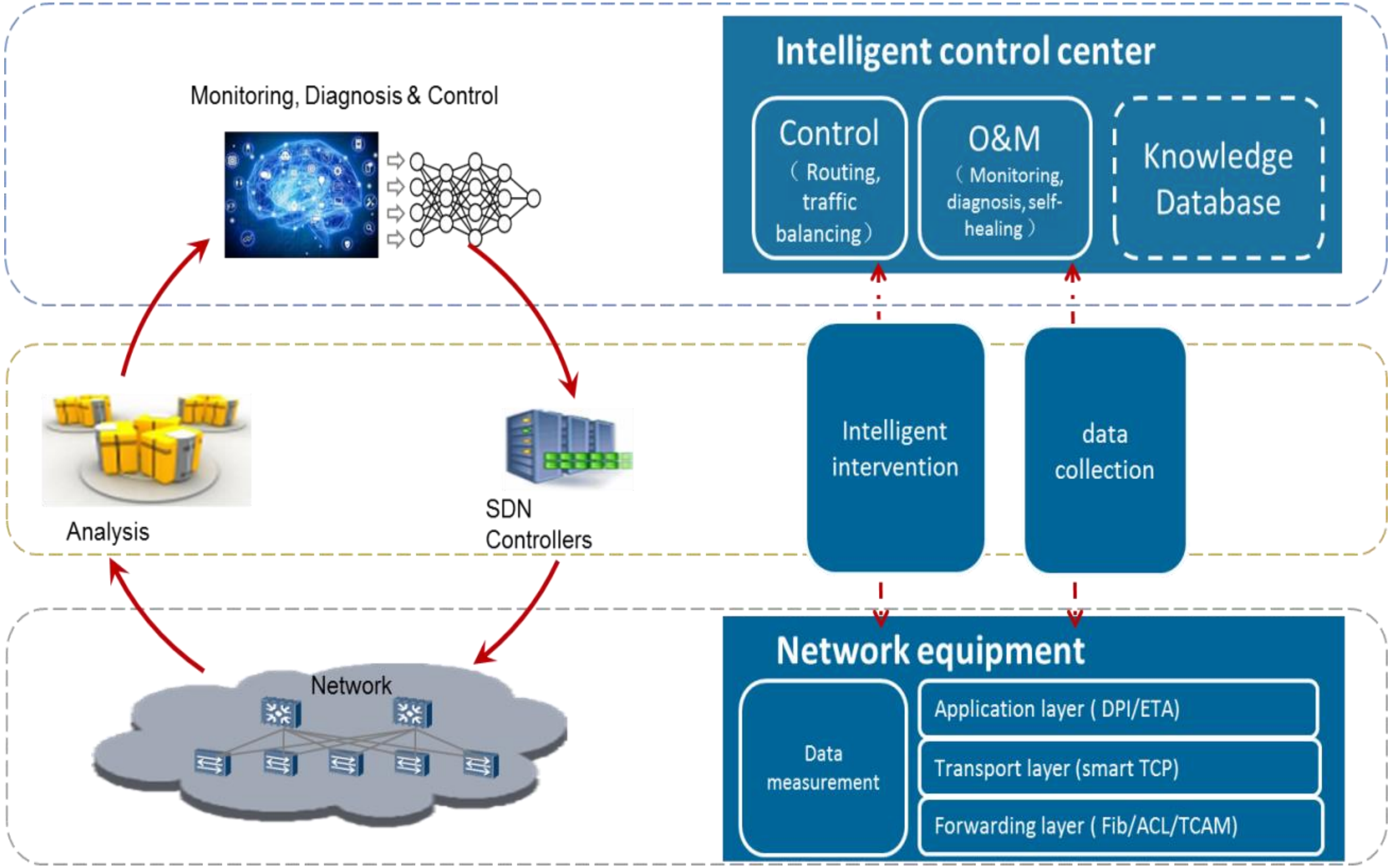
2. Tactile Internet for remote operations (TIRO)





KDDI Research

3. Intelligent operation network (ION)

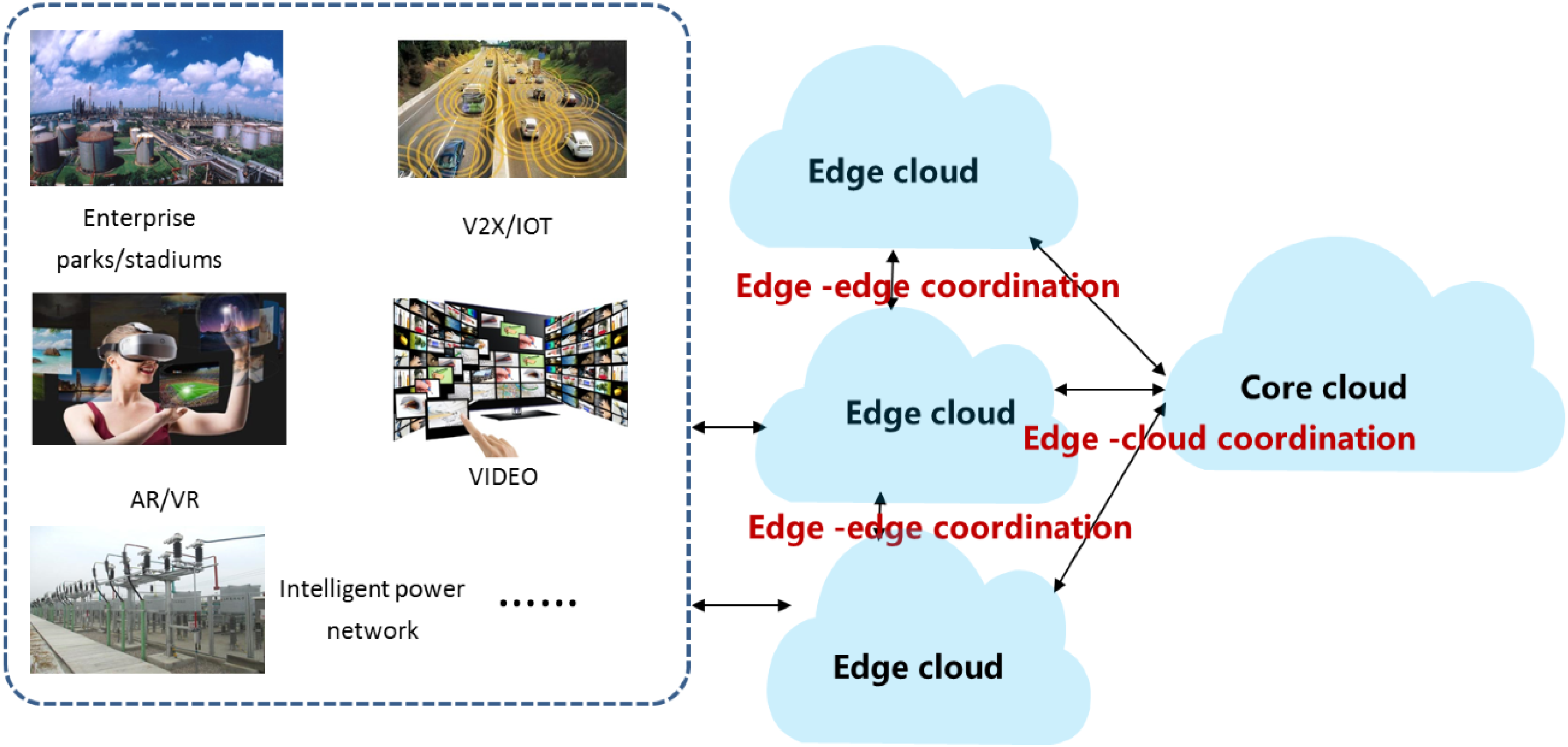


An automatic and intelligent closed-loop control expected in future networks

Representative use cases

KDDI Research

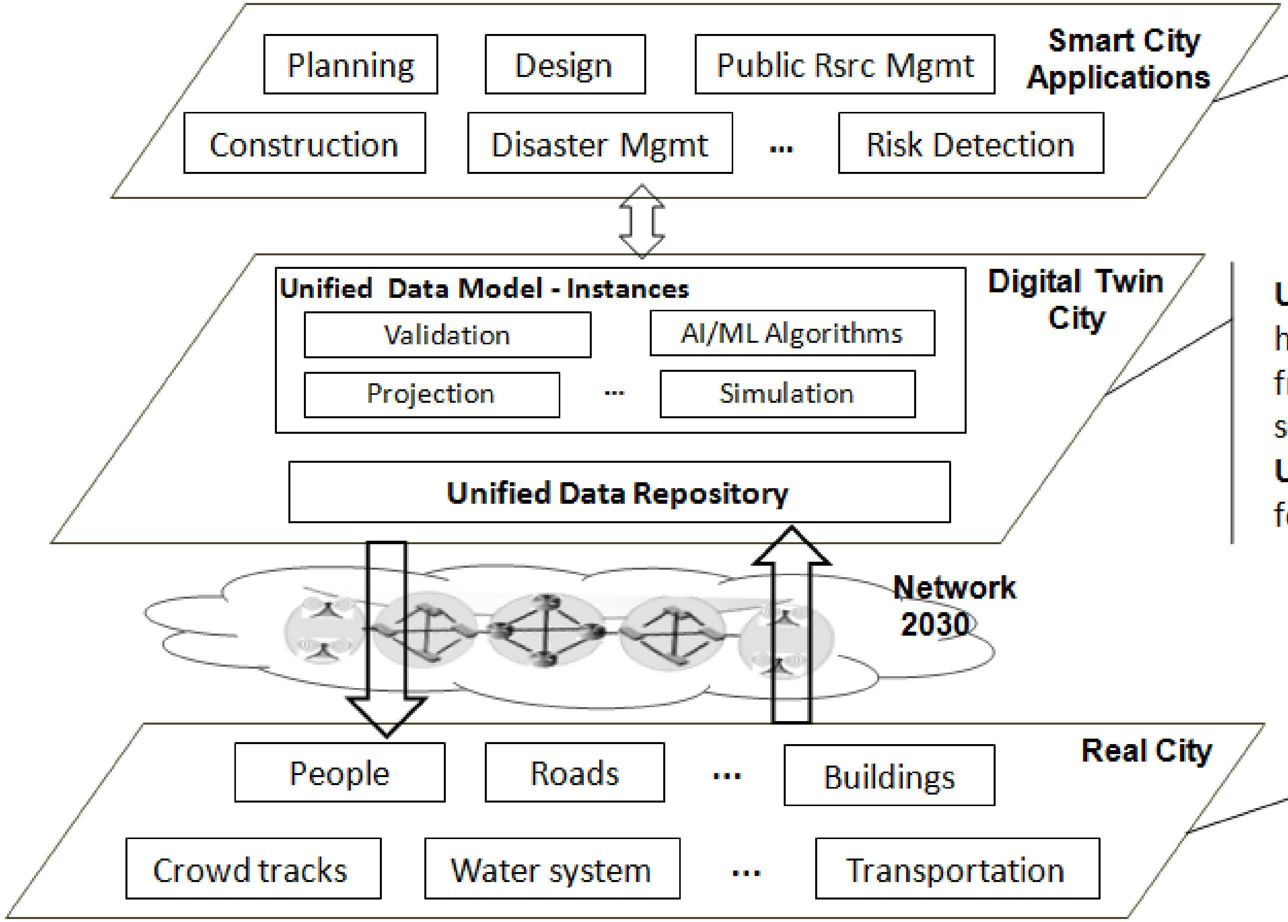
4. Network and compute convergence (NCC)



Edge cloud coordination based on network and compute convergence

Representative use cases

5. Digital twins (DT)



Smart City Application layer contains various applications deployed by city operators.

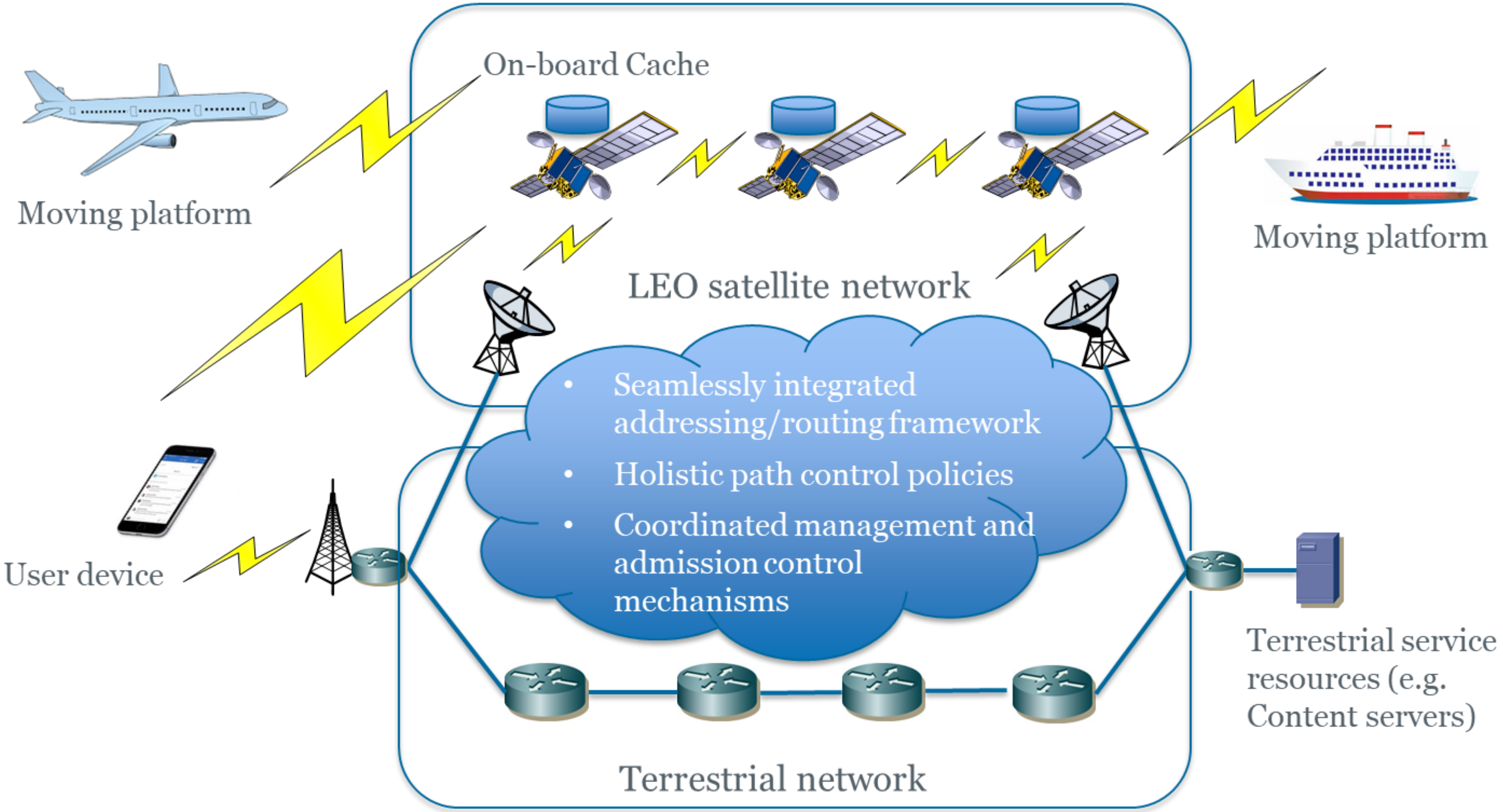
Unified Data Repository stores all historical and real-time data collected from Real City. It can be the 'single source of truth' of the smart city system. **Unified Data Models** provide instances for various smart city applications.

Real city layer contains all assets and infrastructures that can be digitized and virtualized.

Example reference framework of a Digital Twin City (DTC)

KDDI Research

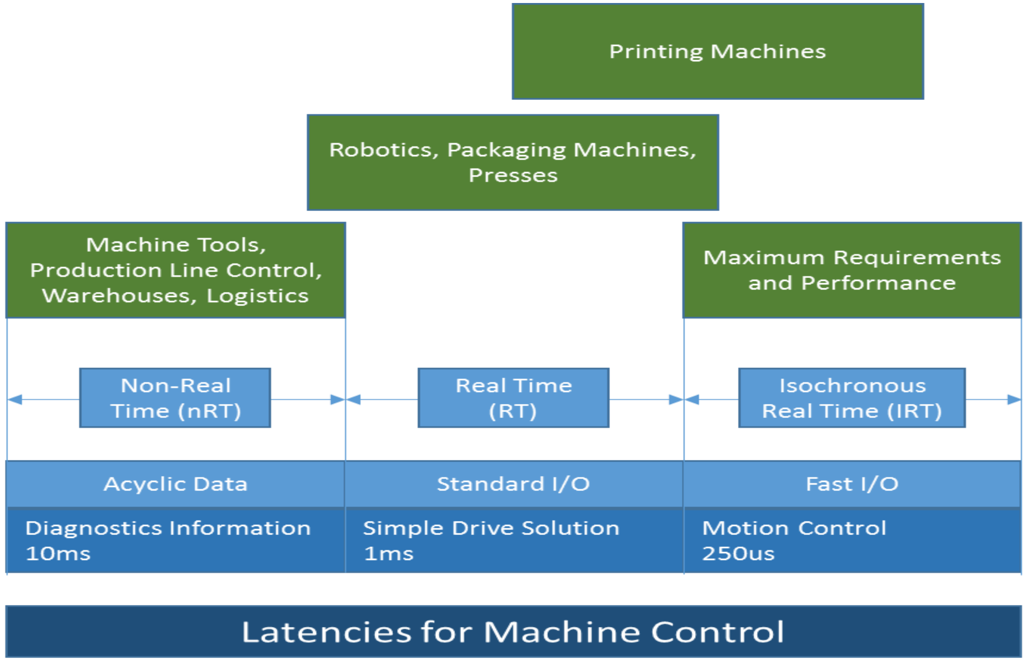
6. Digital Space-terrestrial integrated network (STIN)



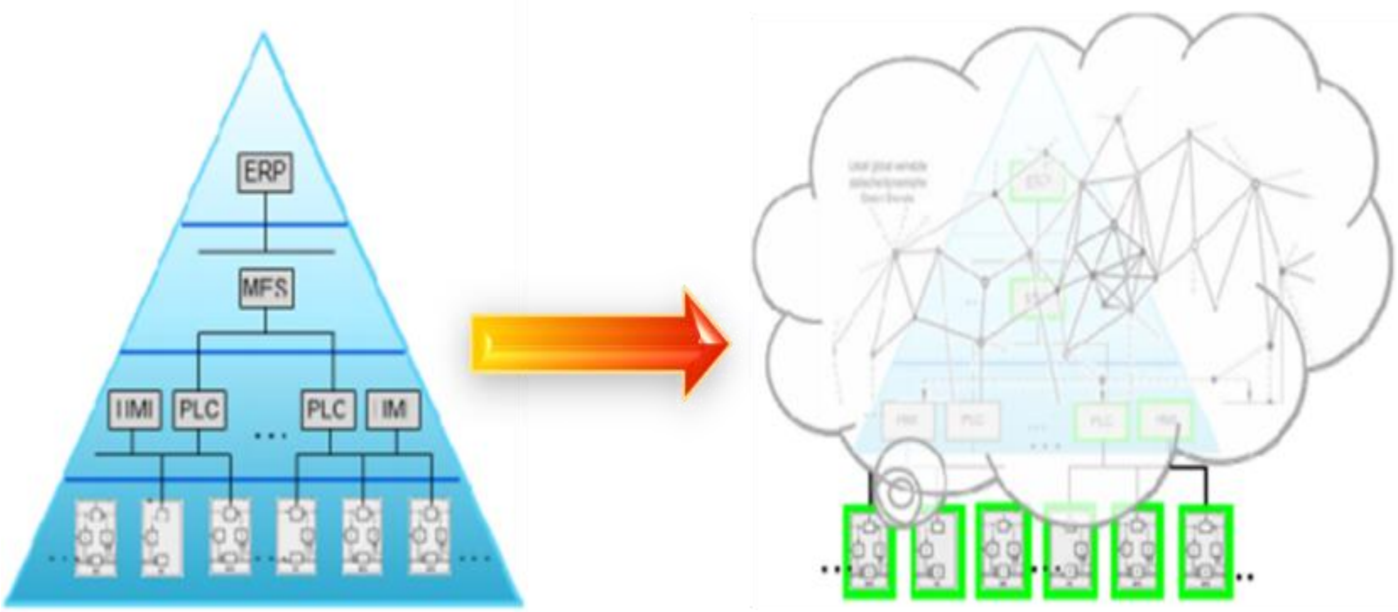
The trend of satellite and terrestrial Internet integration

Representative use cases

7. Industrial IoT (IIoT) with cloudification



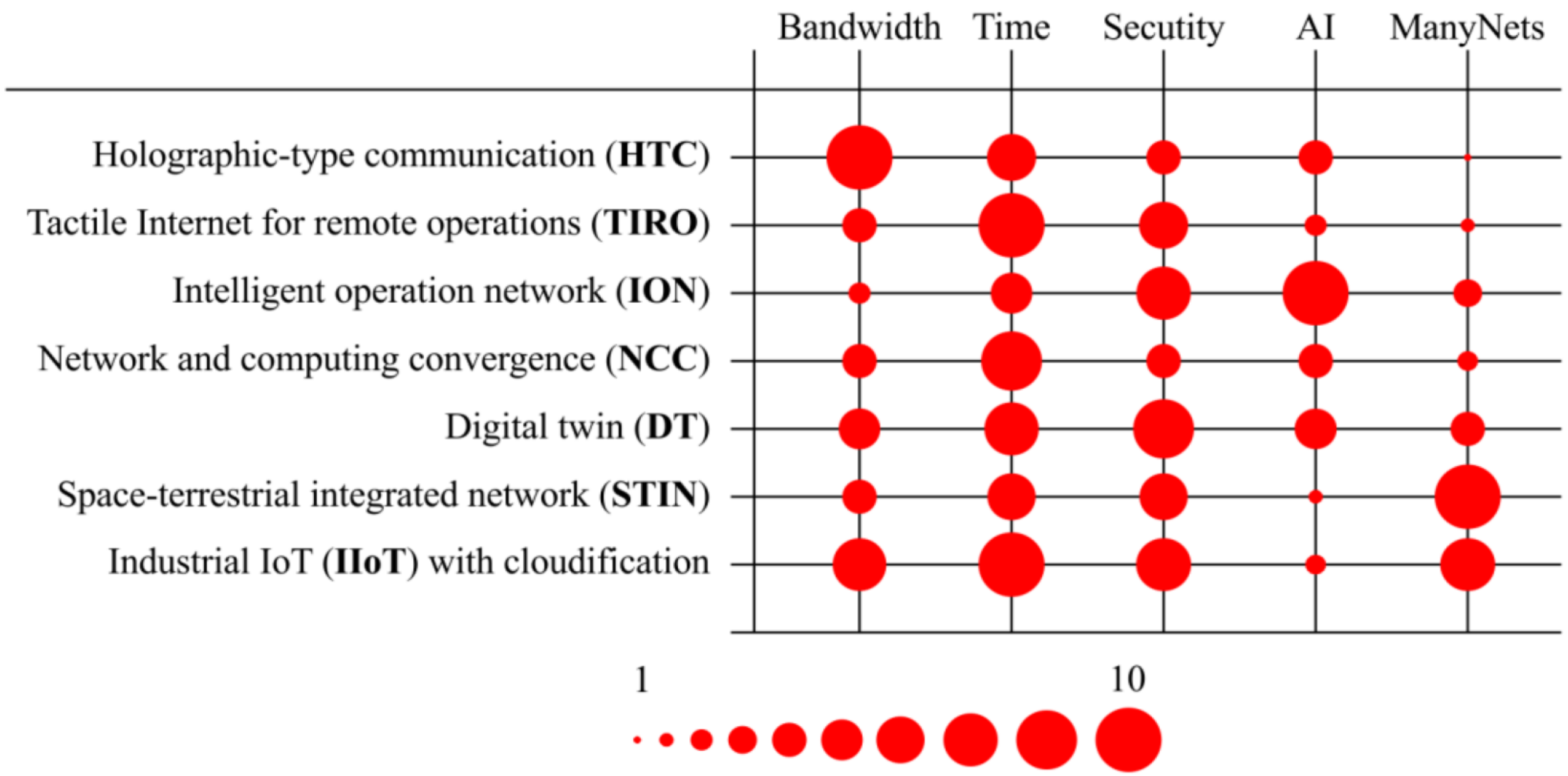
IIoT latency requirements



The trend of industrial cloudification

Graphic representations of the relative network requirements

KDDI Research



The **Security** dimension encompasses integrity, privacy protection, trustworthiness, resilience, lawful interception and traceability, with a high score indicating stringent requirements. The interpretation of this dimension includes consideration of the requirements and priorities of all stakeholders. The default score for security has been assumed to be relatively high (i.e., 5 or above in our scoring system) as all identified use cases need a secure end-to-end communication infrastructure. Furthermore, crossing regulatory boundaries or working with multi-domain networks may be required: a high score for security in these use case scenarios means that interconnectivity between different networks preserves user's identity and data integrity.

Architecture and framework for security, privacy, trust

KDDI Research

- Goals on features
  - Improved trust model
  - Efficient and scalable authentication mechanisms for AS and host-level information
  - Pseudonymous sender/receiver privacy
  - Availability in the presence of an active adversary
  - Transparency and control for forwarding paths
  - Algorithm agility
  - Class of security level
  - Decentralized trust model
- Requirements and Challenges
  - Heterogeneous trust relationships
  - Prevention of DoS and DDoS attacks at all levels (e.g., also against services, infrastructure, etc.)
  - Difficulty of providing latency guarantees
  - Protocol complexity requires formal verification
  - Large network-technology diversity
  - Software vulnerabilities throughout infrastructure and applications

Summary

■ **Approach of FG NET-2030**

Use Cases → **Requirements** → **New features, New architectures, New Framework**

■ **Security related items at FG NET-2030**

- **Almost items are extensions of the current security discussions.**
- **We need to consider security for new use cases, new functions, new mechanisms, new threats, etc. for future networks.**

■ **Activities for new network architecture including security mechanisms**

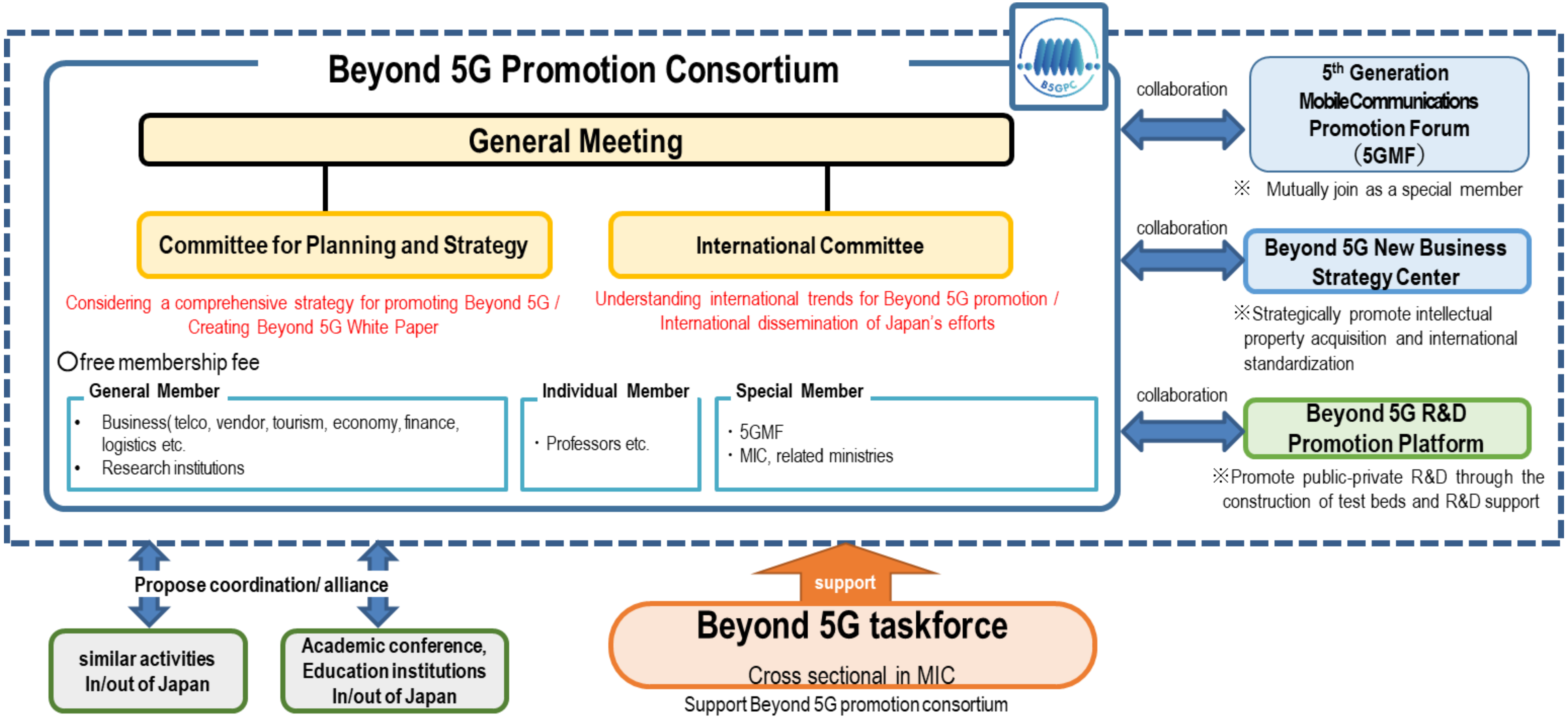
- **In FG NET-2030, SCION (SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS) was introduced as new activity.**
  - https://scion-architecture.net/

Security Activities of Japan's Beyond 5G Promotion Consortium

Beyond 5G Promotion Consortium

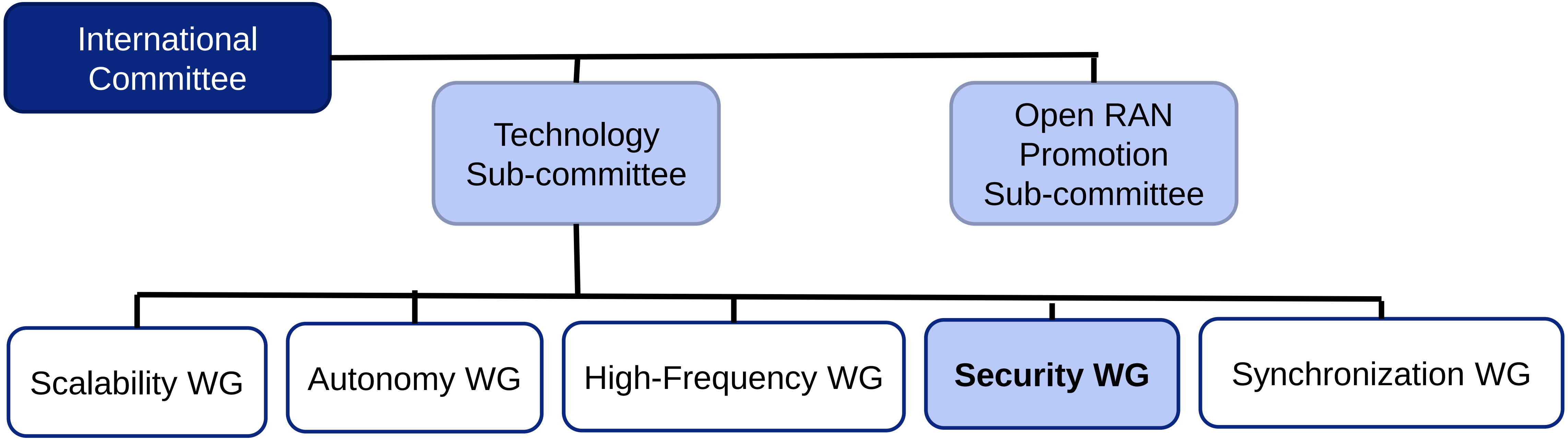
■ Purpose

- Beyond 5G Promotion Consortium aims to achieve the early and smooth introduction of Beyond 5G and to strengthen the international competitiveness of Beyond 5G in order to realize the strong and vibrant society expected in the 2030s.



Committees

- **Committee for Planning and Strategy:**
  - **Study of comprehensive strategies to promote Beyond 5GPreparation of Beyond 5G White Paper**
- **International Committee:**
  - **Identifying international trends for promoting Beyond 5GInternational dissemination of the status of Japan's efforts**



What are security topics for future networks?

Changes	Examples	Issues
New Technologies  	• Quantum Computer • AI technologies	• Future quantum computer can compromise current crypt algorithms. • AI will be used for cyber attacks. • AI itself will be target of attack.

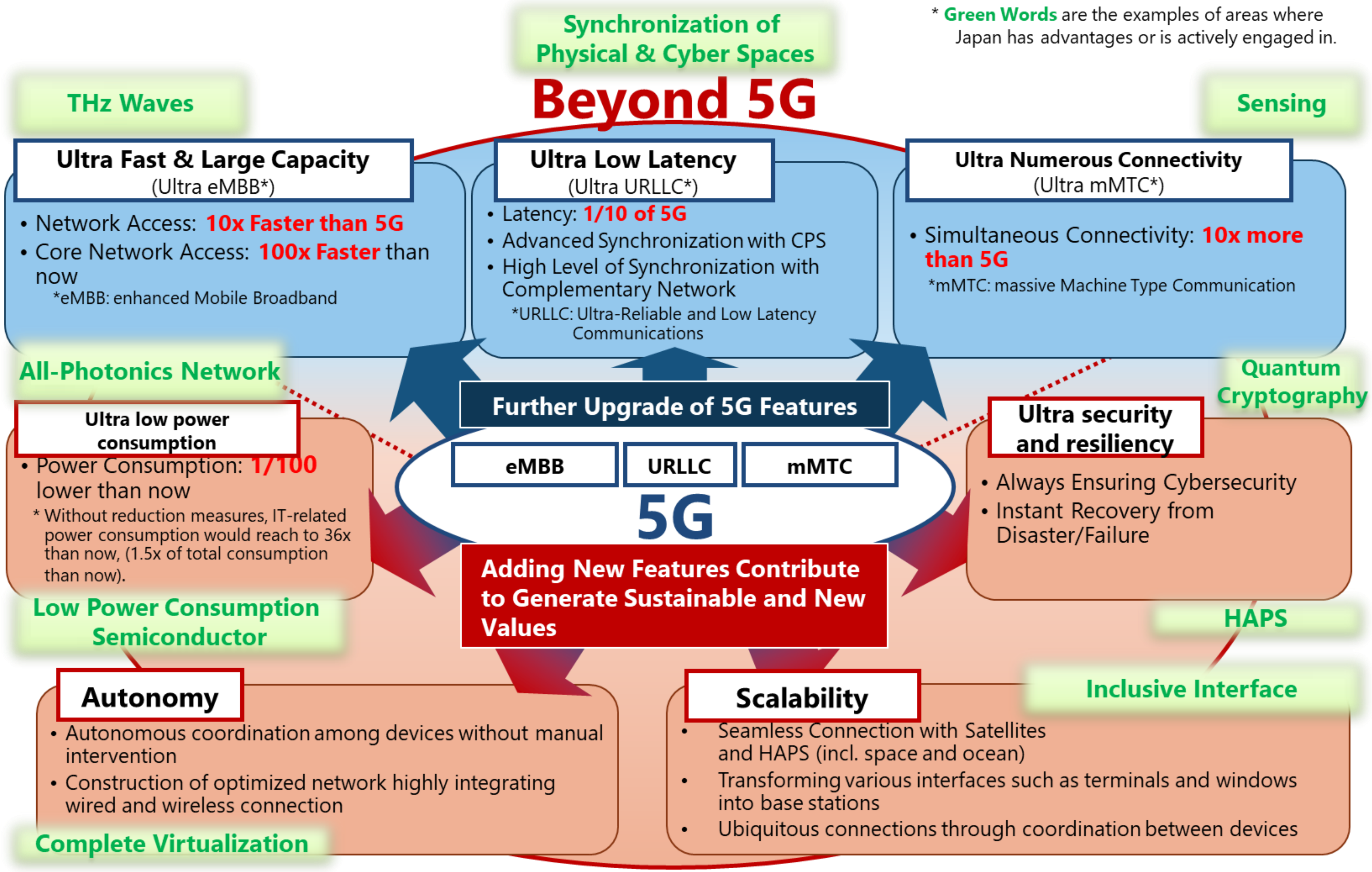
New Services (New Use Cases)

 	
	• Holographic Communication
	• Tactile Internet
	• Unmanned mobility
		• New requirements should be considered.
		  • High speed/Large bandwidth communication
		  • Extremely low latency
		  • Time sensitive communication

New Functions 	• Exposure of network and computing resource • In-time and on-time services • Security, Privacy, Trust	• API/Interconnecting should be secured. • What security/privacy/trust function will be required for B5G/6G network?
New Infrastructure 	• Space-terrestrial Integrated Network • Intelligent Operation Network	• Networks will become even more complex, and security issues (vulnerabilities, configuration mistakes) cannot be found easily.

Features for Beyond 5G

KDDI Research



https://b5g.jp/en/about.html

Security considerations for new features

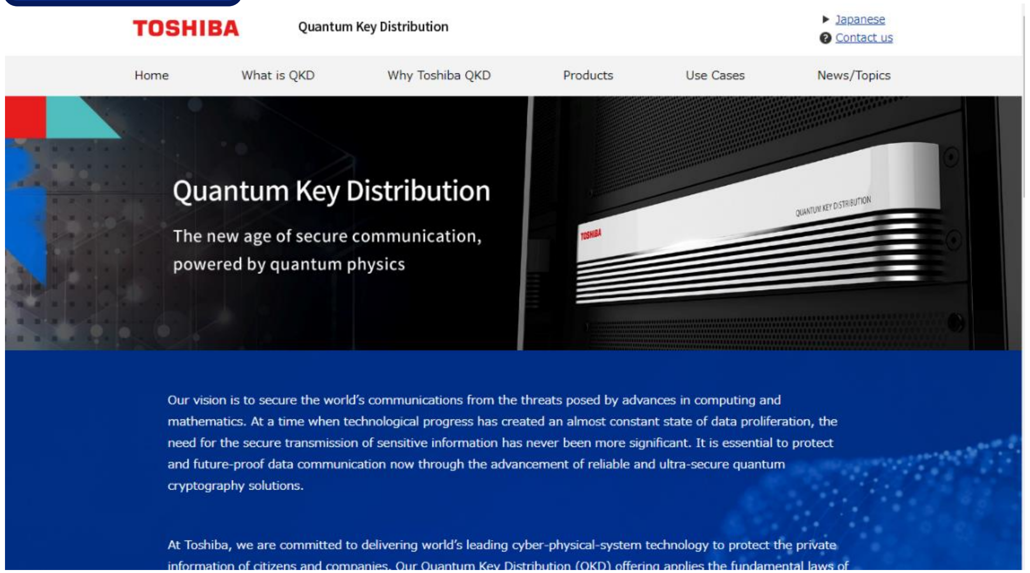
Features	Security requirements
Ultra Fast & Large Capacity	• High speed encryption/decryption • New security monitoring and processing methods
Ultra Low Latency	• Seamless security architecture • Lightweight security
Ultra Numerous Connectivity	• Efficient authentication/authorization • Efficient security processing and monitoring mechanism
Ultra low power consumption	• Security mechanisms in hardware • Lightweight security architecture
Ultra security and resiliency	• New security monitoring and defensing mechanisms • Resilience mechanism for attacks/failures • Privacy preserving mechanisms • Trustworthiness of different nodes and domains • Accounting, accountability, validation of delivered services
Autonomy	• Trust mechanism without trusted parties
Scalability	• Interoperable security mechanism between different networks/domains • Optimization of security mechanism among

Activities on QKD

KDDI Research

NICT

Toshiba



NEC

Activities on Post-Quantum Cryptography

KDDI Research

KDDI — **MLWRSign** for digital signature

2020 | OriginalPaper | Chapter

A Compact Digital Signature Scheme Based on the Module-LWR Problem

Authors: Hiroki Okada, Atsushi Takayasu, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi

Publisher: Springer International Publishing

Information and Communications Security

Read first chapter

Published in: Information and Communications Security

» Get access to the full-text

Abstract

We propose a new lattice-based digital signature scheme MLWRS
which is one of the second-round candidates of NIST's call for post-
standards. To the best of our knowledge, our scheme MLWRSign is t
security is based on the (module) learning with rounding (LWR) prob
LWR, the secret key size is reduced by approximately 30% in our sch
while achieving the same level of security. Moreover, we implement
the running time of our scheme is comparable to that of Dilithium.

NICT — **LOTUS** for public-key cryptography

Post-Quantum Cryptography

LOTUS

Home

Materials
Specifications
Implementation Code
Known Answer Tests

Related information

LOTUS

(Learning with errOrs based encryption with chosen ciphertexT secUrity for poSt quantum era)

What's LOTUS?

LOTUS is a lattice-based cryptosystem developed by NICT. LOTUS consists of LOTUS-PKE for public key encryption and LOTUS-KEM for key encapsulation. LOTUS aims at providing post-quantum security, meaning it may remain secure against large-scale quantum computers. Some highlighted properties of LOTUS are as follows:

- Its security relies on the standard Learning With Errors (LWE) assumption.
- It targets IND-CCA2 security, even with 256-bit security level (the highest security level in NIST PQC project).
- It is based on a long line of research.

News

- December 27, 2017. Initial website is up.
- January 04, 2018. Update the implementation code t failure. We thank Tancrède Lepoint for pointing out tl
- October 15, 2018. LOTUS implementation codes are

Contacts

Toshiba — **Giophantus** for public-key cryptography

International Conference on Selected Areas in Cryptography

SAC 2017: Selected Areas in Cryptography – SAC 2017 pp 215-234 | Cite as

A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations

Authors | Authors and affiliations

Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka

Conference paper
First Online: 23 December 2017

2 Citations | 686 Downloads

Part of the Lecture Notes in Computer Science book series (LNCS, volume 10719)

Abstract

In this paper, we propose a post-quantum public-key encryption scheme whose security depends on a problem arising from a multivariate non-linear indeterminate equation. The security of lattice cryptosystems, which are considered to be the most promising candidate for a post-quantum cryptosystem, is based on the shortest vector problem or the closest vector problem in the discrete linear solution spaces of simultaneous equations. However, several improved attacks for the underlying problems have recently been developed by using approximation methods, which result in requiring longer key sizes. As a scheme to avoid such attacks, we propose a public-key encryption scheme based on the "smallest" solution problem in the *non-linear* solution spaces of multivariate *indeterminate equations* that was developed from the algebraic surface cryptosystem. Since no efficient algorithm to find such a smallest solution is currently known, we introduce a new computational assumption under which proposed scheme is proven to be secure in the sense of IND-CPA. Then, we perform computational experiments based on known attack methods and evaluate that the key size of our scheme is able to be much shorter than those of previous lattice cryptosystems.

NTT — Improvement of **NTRU-HRSS** (Public-key Cryptography)

Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model ⋆

Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa

NTT Secure Platform Laboratories
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585 Japan
{saito.tsunekazu, xagawa.keita, yamakawa.takashi}@lab.ntt.co.jp
August 25, 2021

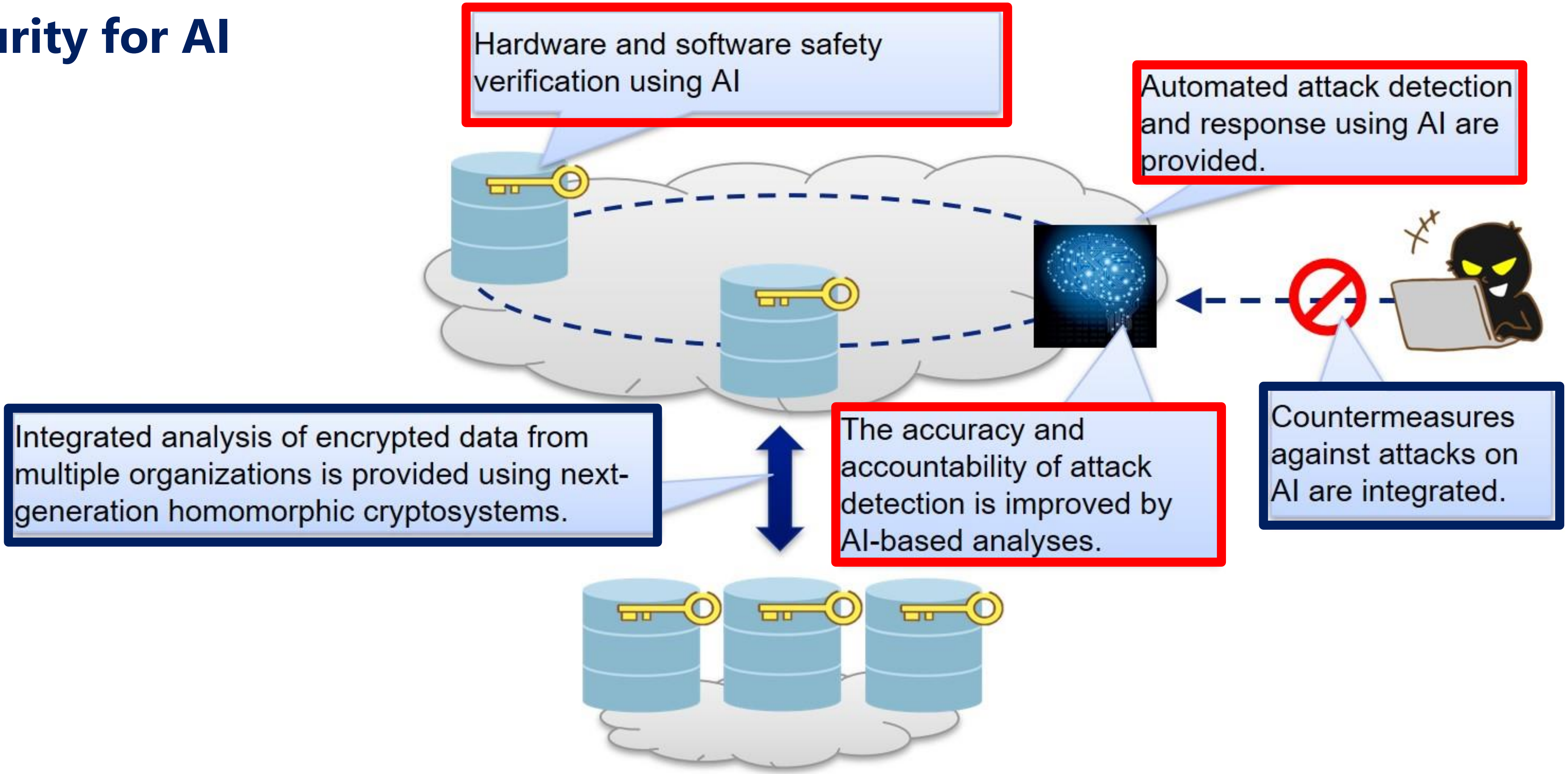
Abstract. Key-encapsulation mechanisms secure against chosen ciphertext attacks (IND-CCA-secure KEMs) in the quantum random oracle model have been proposed by Boneh, Dagdelen, Fischlin, Lehmann, Schafner, and Zhandry (CRYPTO 2012), Targhi and Unruh (TCC 2016-B), and Hofheinz, Hövelmanns, and Kiltz (TCC 2017). However, all are non-tight and, in particular, security levels of the schemes obtained by these constructions are less than half of original security levels of their building blocks.
In this paper, we give a conversion that tightly converts a weakly secure public-key encryption scheme into an IND-CCA-secure KEM in the quantum random oracle model. More precisely, we define a new security notion for deterministic public key encryption (DPKE) called the disjoint simulatability, and we propose a way to convert a disjoint simulatable DPKE scheme into an IND-CCA-secure key-encapsulation mechanism scheme without incurring a significant security degradation. In addition, we give DPKE schemes whose disjoint simulatability is tightly reduced to post-quantum assumptions. As a result, we obtain IND-CCA-secure KEMs tightly reduced to various post-quantum assumptions in the quantum random oracle model.
keywords: Tight security, chosen-ciphertext security, post-quantum cryptography, KEM.

AI Security

KDDI Research

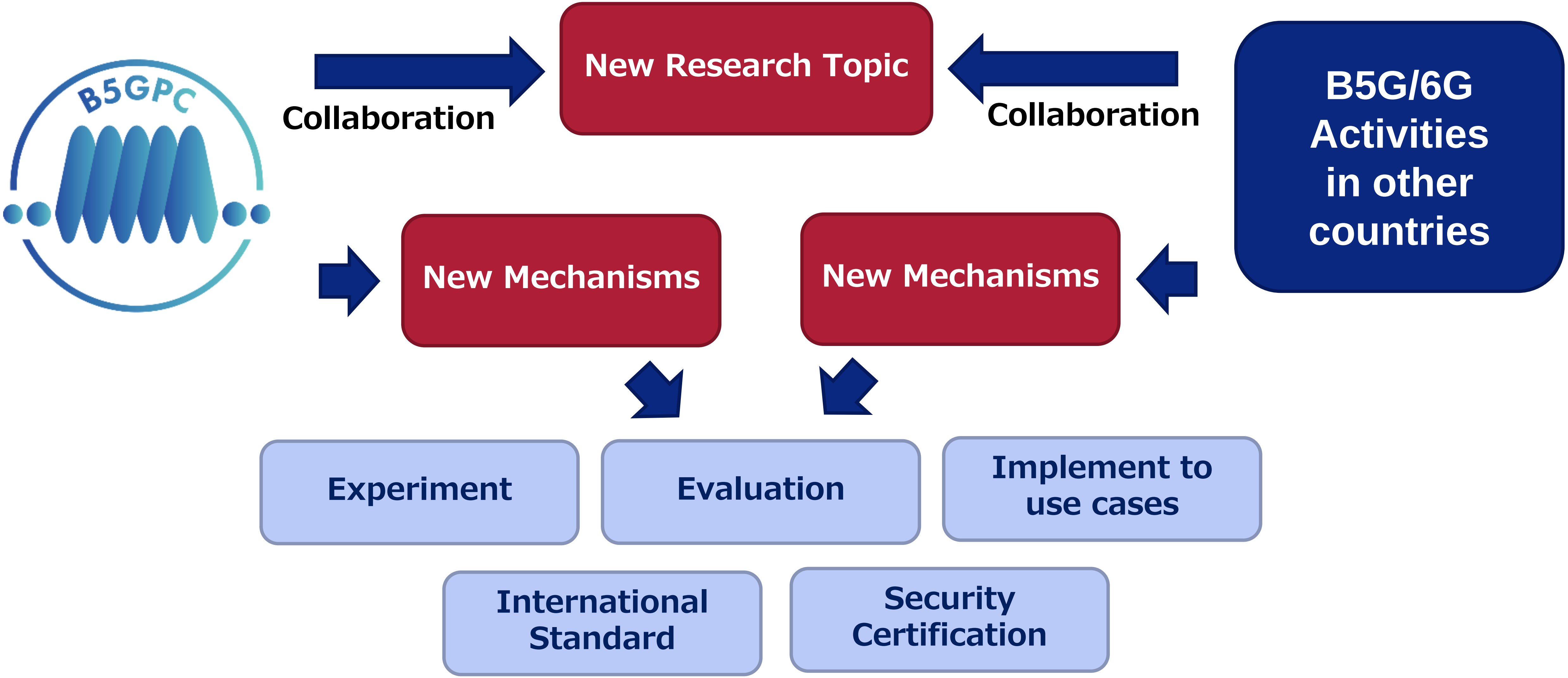
- **Security using AI**
- **Security for AI**

AI-driven technologies for attack detection and prevention



Beyond 5G/6G White Paper ver. 2.0 (KDDI/KDDI Research, Inc.)

International coordination



KDDI Research