Xinsheng JI, Jiangxing WU, Liang JIN, Kaizhi HUANG, Yajun CHEN, Xiaoli SUN, Wei YOU, Shumin HUO, Jing YANG, 2022. Discussion on a new paradigm of endogenous security towards 6G networks. *Frontiers of Information Technology & Electronic Engineering*, 23(10):1421-1450.
https://doi.org/10.1631/FITEE.2200060

Discussion on a new paradigm of endogenous security towards 6G networks

Key words: 6G security; New paradigm of endogenous security; Core network; Wireless access network

Corresponding author: Kaizhi HUANG
E-mail: huangkaizhi@tsinghua.org.cn
ORCID: https://orcid.org/0000-0002-7084-3826

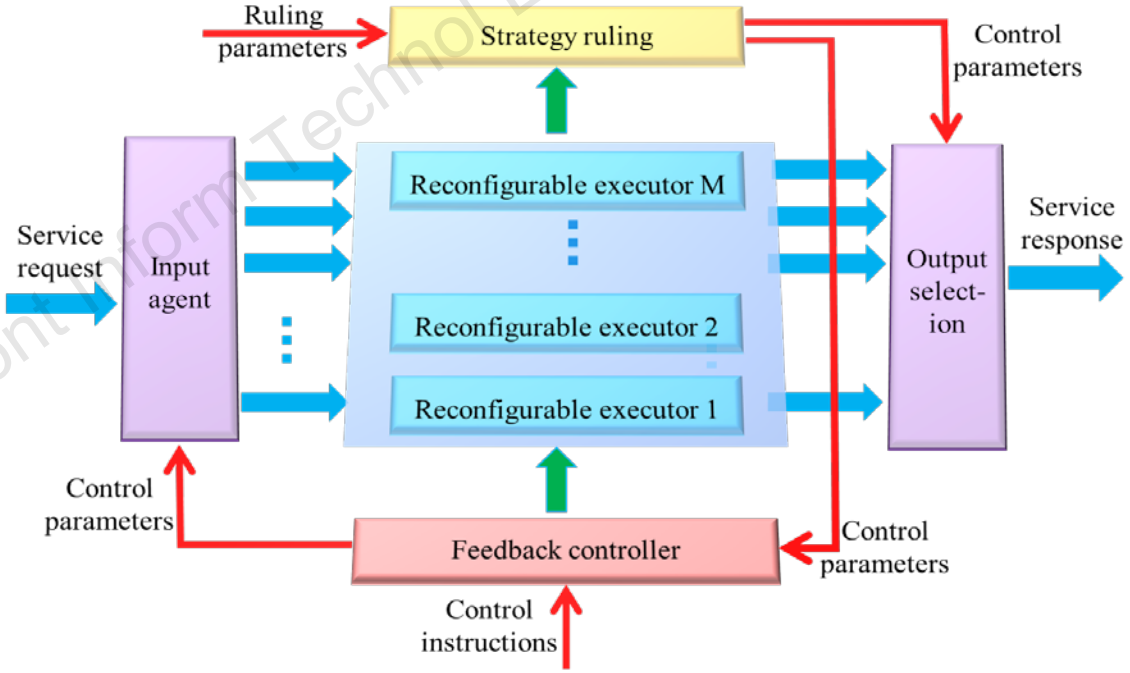
Motivation

1. The sixth-generation mobile communication (6G) networks will face more complex endogenous security problems, and it is urgent to propose new universal security theories and establish new practice norms to deal with the “unknown unknown” security threats in cyberspace.

2. 6G will achieve intelligent interconnection of everything and provide ubiquitous communication support. As a key support for the future digital world and intelligent society, the 6G network security requires in-depth planning and realization of broad functional security while fully considering information security requirements, so as to create a strong and reliable digital connection base for the future society.

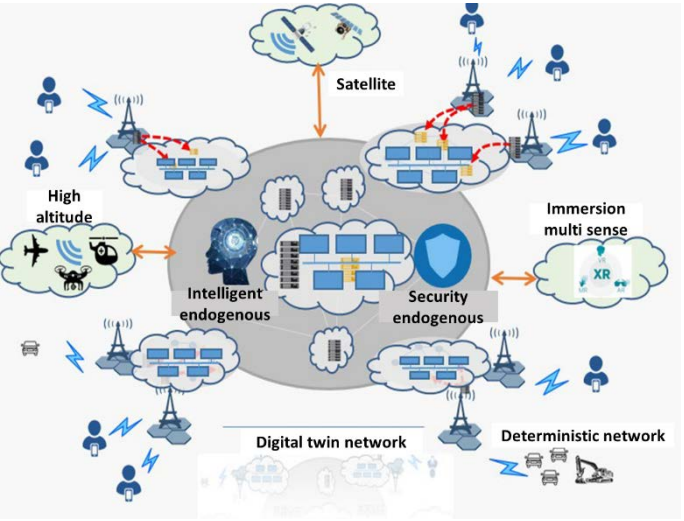
New paradigm of cyberspace endogenous security

The new paradigm of cyberspace endogenous security can provide endogenous security capabilities to deal with known and unknown security threats for 6G communication security, functional safety, and supply chain security through endogenous security function design. DHR structure is an innovative structure to realize an endogenous security function.



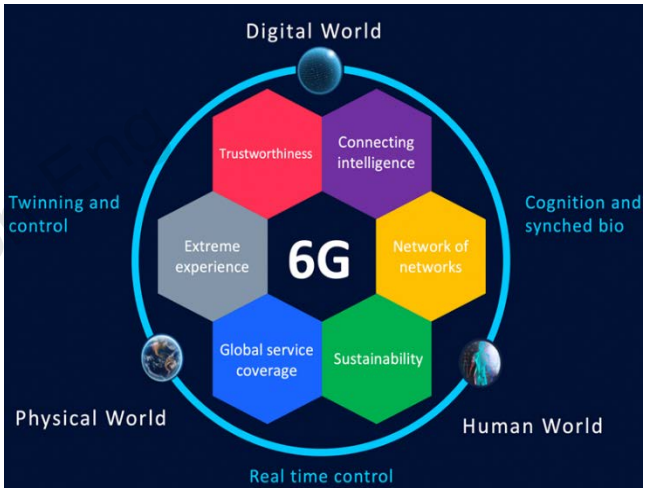
Dynamic heterogeneous redundancy (DHR) structure

Demand vision for 6G cyberspace security



China IMT-2030 6G Vision

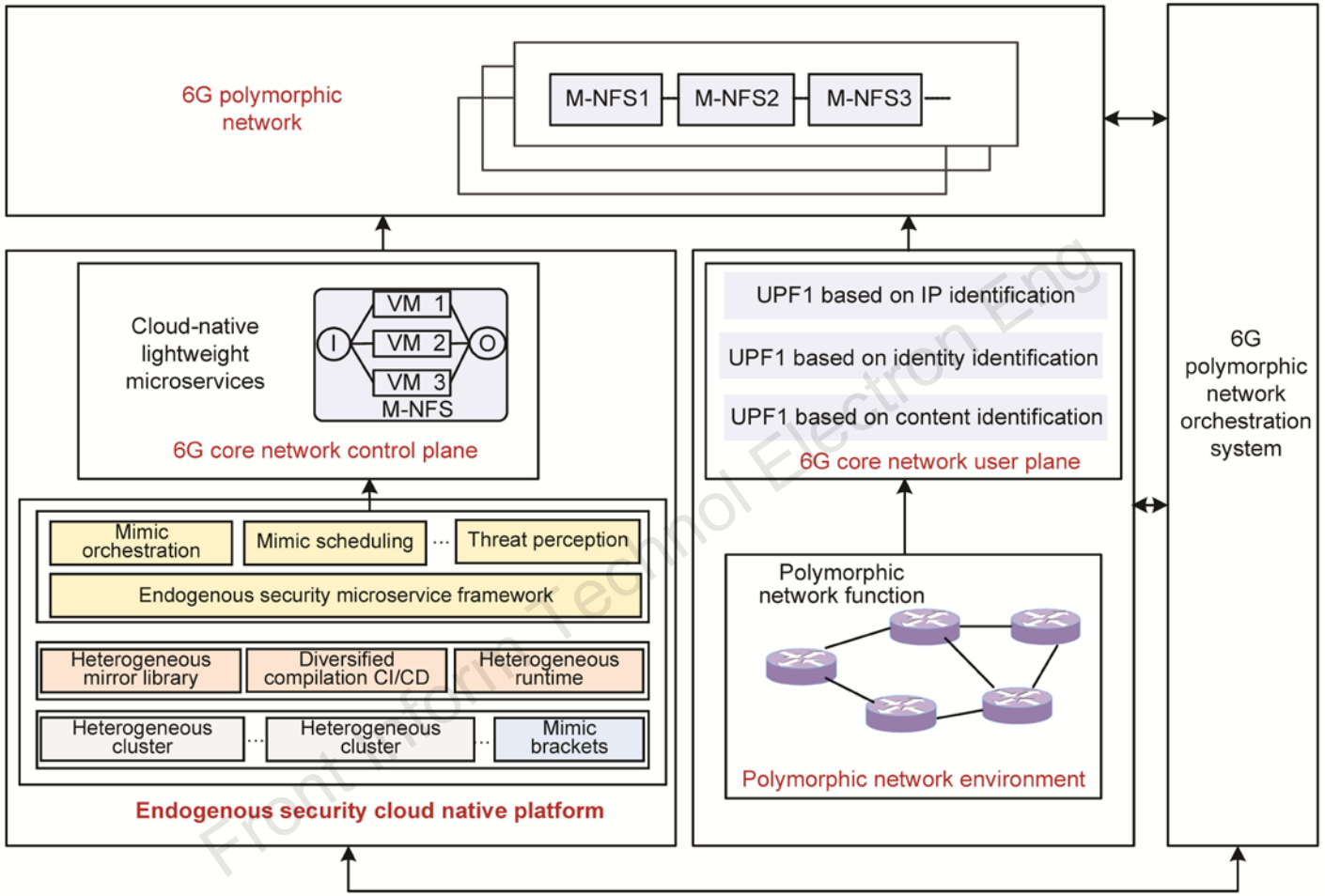
Next G Alliance Six Audacious Goals



Hexa-X 6G research challenges

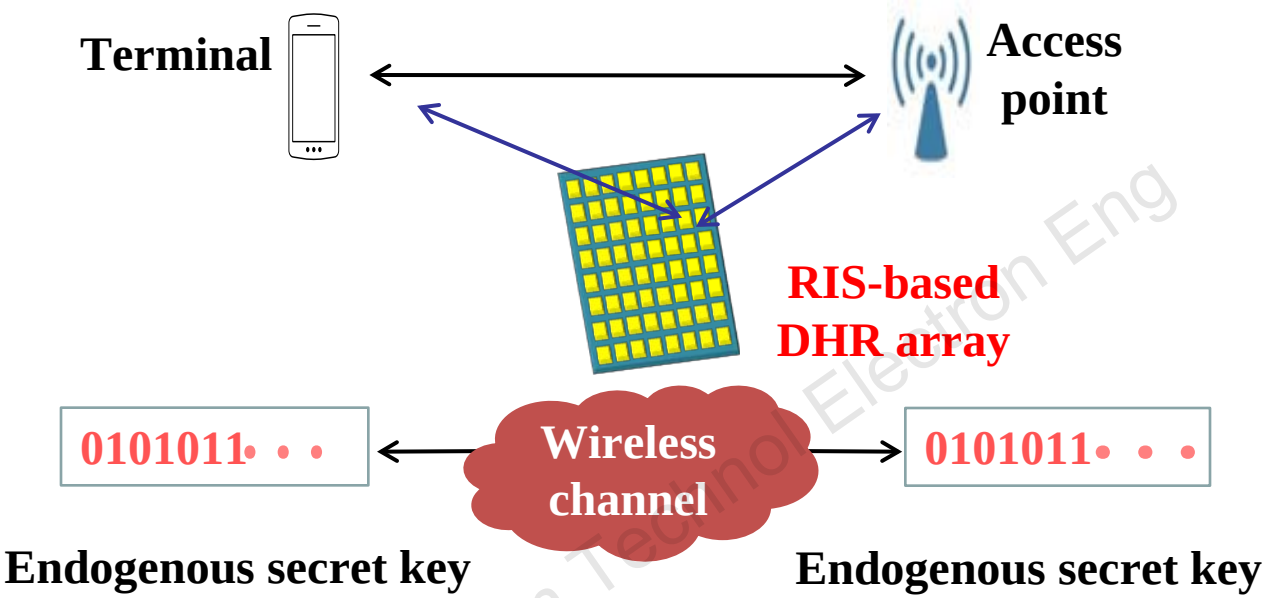
The Chinese government and research institutes are the first in the world to put forward the vision of 6G endogenous security. The United States, Europe, and Japan have also listed generalized security concepts, such as security, resilience, and dependability, as the core vision and early-launched projects of 6G.

Endogenous security for 6G core networks



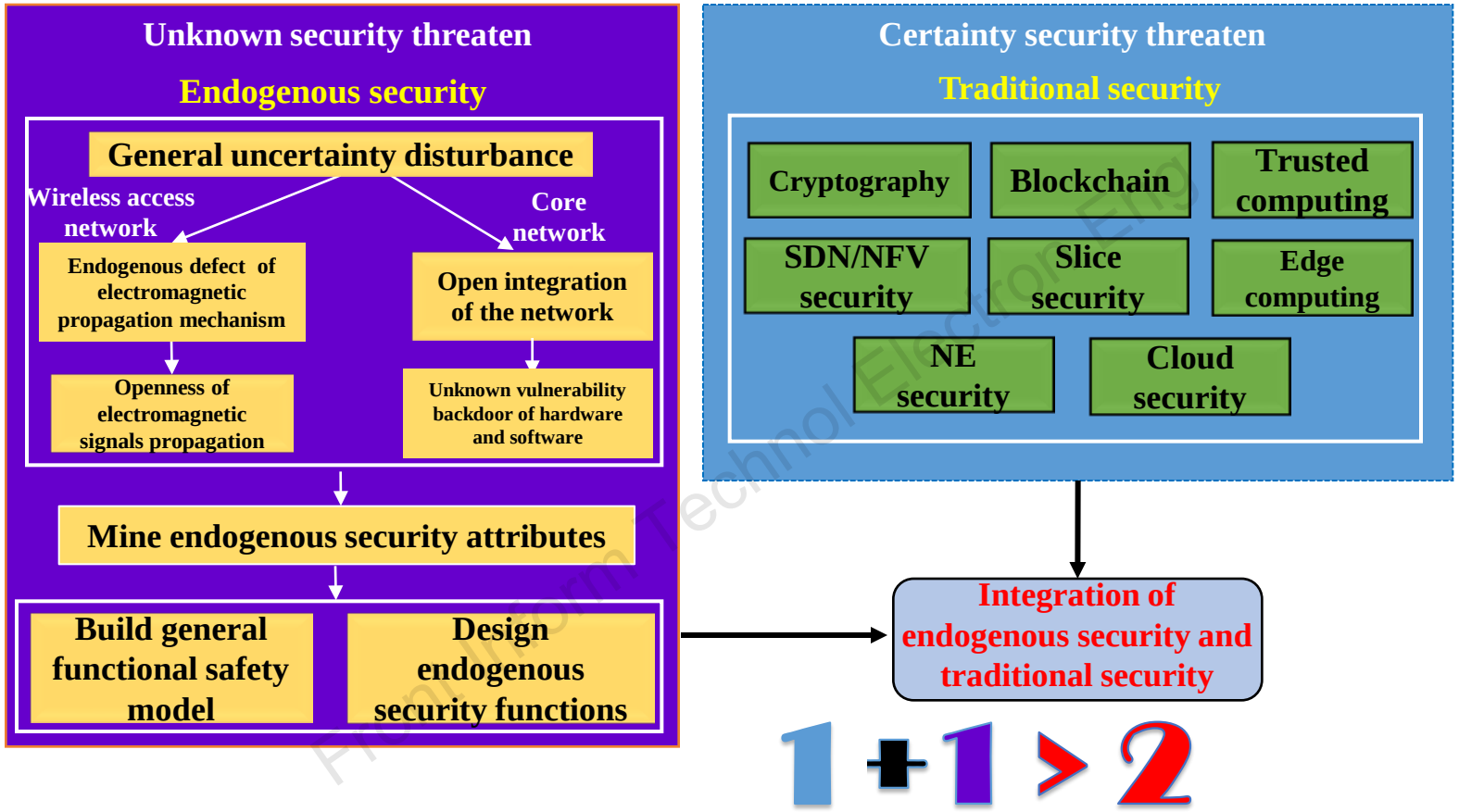
The 6G endogenous security core network includes three parts: (1) the 6G core network control plane based on the endogenous security cloud-native platform; (2) the 6G core network user plane based on the polymorphic network environment; (3) the 6G network modal construction suitable for different application scenarios.

Endogenous security for wireless access networks



The RIS-based DHR array can artificially construct wireless endogenous security attributes by reshaping the electromagnetic propagation environment. Based on the RIS-enabled DHR array, we could design generalized robustness to overcome uncertain disturbance problems at the physical layer, achieving the integrated design of functional safety and information security and providing a practice specification of the new paradigm of wireless endogenous security in 6G.

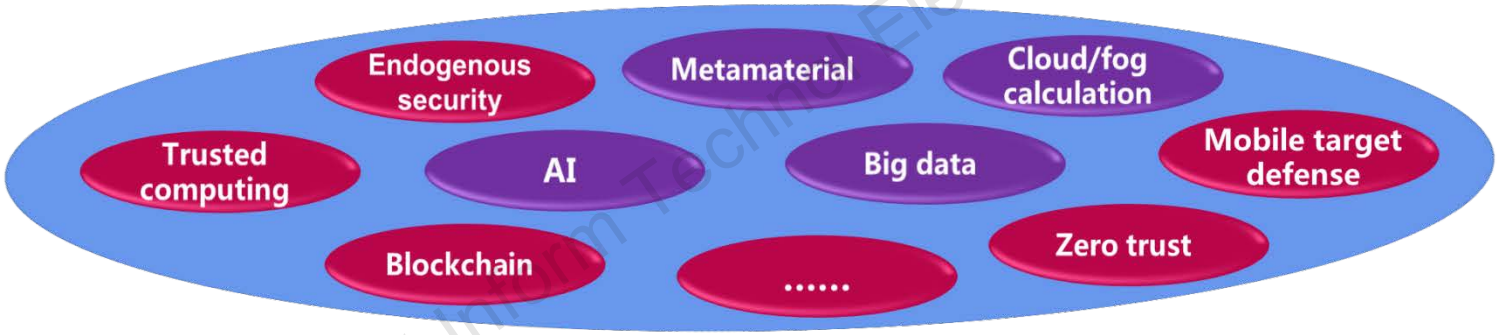
Integration of endogenous security and traditional security



- Endogenous security and traditional security are complementary to each other.
- Endogenous security and traditional security can enhance each other.

Integration of endogenous security and emerging enabling technologies

Take AI technology as an example to introduce the integration of endogenous security and AI technology. By introducing the DHR gene of endogenous security into the 6G AI application system, an endogenous security model based on the DHR structure is established in the 6G AI model.



- Establish endogenous security theory and security architecture under the 6G AI environment.
- Build endogenous security protection mechanisms and methods under the 6G AI environment.
- Design measurement, verification, and evaluation of the effectiveness of endogenous security technologies in the 6G AI environment.

Conclusions

1. 6G security will focus on the requirements of high reliability, high availability, high controllability, high confidentiality, high privacy, and so on, and explore the basic theories and key technologies of 6G cyberspace endogenous security for machine communication, ubiquitous networking, wireless transmission, and space-ground integration.

2. 6G security should be guided by the new paradigm of cyberspace endogenous security and consider the integration of endogenous security, traditional security, and emerging enabling technologies.

Xinsheng JI, first author of this invited paper, received his BE degree in Fudan University, Shanghai, China, in 1988, and his MS degree in PLA Information Engineering University, Zhengzhou, China, in 1991. He is currently a Chief Engineer of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). He is a member of the National 6G Technology R&D General Expert Group, a Chief Scientist of the wireless security field of the Collaborative Innovation Center for Wireless Communication, a Deputy Director of the National Engineering Laboratory for Mobile Network Security, and an Academic Leader of the National Science Foundation Innovation Corps. He obtained the National Science and Technology Progress Award (First Prize) three times, and the National Science and Technology Progress Award for Innovation Team once. His major research interests include next-generation mobile communication and cyber space security.

Jiangxing WU is an academician of the Chinese Academy of Engineering (CAE). He is a professor and doctoral supervisor and president of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). Some other positions he held include: Vice Chairman of the National High-tech R&D Program (863 Program) from the Ninth-Five-Year Plan to the Tenth-Five-Year Plan, Vice Chairman of the Information Technology Experts Group of the 863 Program, Director of the National Major Mobile Communication Project Evaluation Commission, Director and Chief Engineer of the China Next Generation Broadcasting Network (NGB) Experts Commission, Vice Chairman of the 3Tnet in the Eleventh-Five-Year Plan. Since 2016, he has served as Vice Chairman of the Space-Earth Integration Network Experts Group of the National Key Scientific and Technological Project during the Thirteenth-Five-Year Plan. He obtained the National Science and Technology Progress Award (First Prize) three times. Some other awards granted to him include: the title of National Outstanding Scientific and Technological Worker in 1997, Outstanding Contribution Award of the National Science and Technology Research Program in 2001, the title of Young and Middle-Aged Experts with Outstanding Contributions in 2003, First-Level Prize of National Teaching Achievement in 2009, and the National Innovation Competition Award in 2017. The scientific research team he led won the National Science and Technology Progress Award for Innovation Team in 2015. His research interests include cyberspace security and network architecture.

Kaizhi HUANG, corresponding author of this invited paper, received her BE degree in digital communication and MS degree in communication and information system in 1995 and 1998, respectively, from PLA Information Engineering University, and her PhD degree in communication and information system in 2003 from Tsinghua University. She is currently a professor of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). She is an expert in the evaluation of national key R&D projects and NSFC projects, and won one National Science and Technology Progress and Innovation Team Award. Her research interests include wireless network security and signal processing.