Smart City and IoT Resilience, Survivability, and Disruption Tolerance: Challenges, Modelling, and a Survey of Research Opportunities

James P.G. Sterbenz[*†‡]
jpgs@{ittc.ku.edu|comp.{lancs.ac.uk|polyu.edu.hk}}

Presenter: Bei Zhang

IoT (Internet of things)

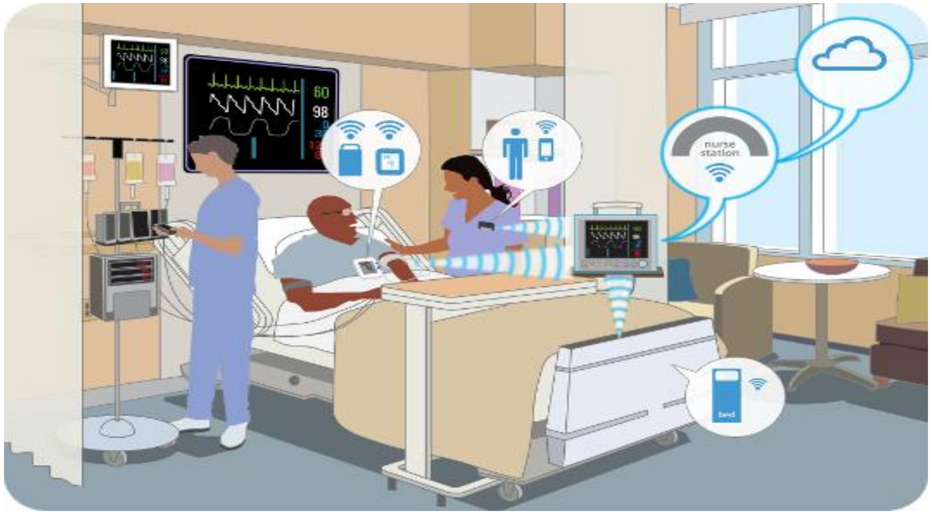
attaching a wide variety of devices to the network

- sensors and cameras
- home appliances
- home and industrial control devices
- health monitoring
- entertainment delivery

IoT

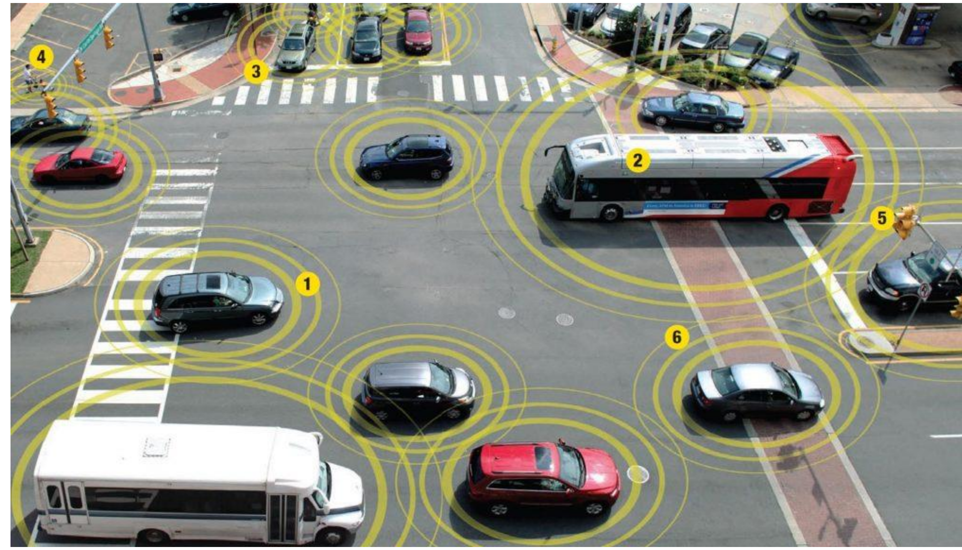
Smart Appliances

Wearable Tech



Healthcare

smart cities



- Use a navigation system to find the best route based on real-time conditions
- Alert drivers of potentially hazardous situations in time to avoid crashes
- Be guided to an empty parking space by a smart sign
- Detect and respond promptly to traffic incidents
- Reroute traffic in response to road conditions or weather emergencies
- Give travelers real-time traffic and weather reports

Why challenges ?

From IoT (Internet of things) toward smart cities

The IoT Market

As of 2013, 9.1 billion IoT units

Expected to grow to 28.1 billion IoT devices by 2020

Lund, D., Turner, V., MacGillivray, C., & Morales, M. (2014, May). Worldwide and Regional Internet of Things (IoT) 2014 – 2020 Forecast: A Virtuous Circle of Proven Value and Demand. Retrieved January 25, 2016, from http://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf

Attacking IoT

Default, weak, and hardcoded credentials

Difficult to update firmware and OS

Lack of vendor support for repairing vulnerabilities

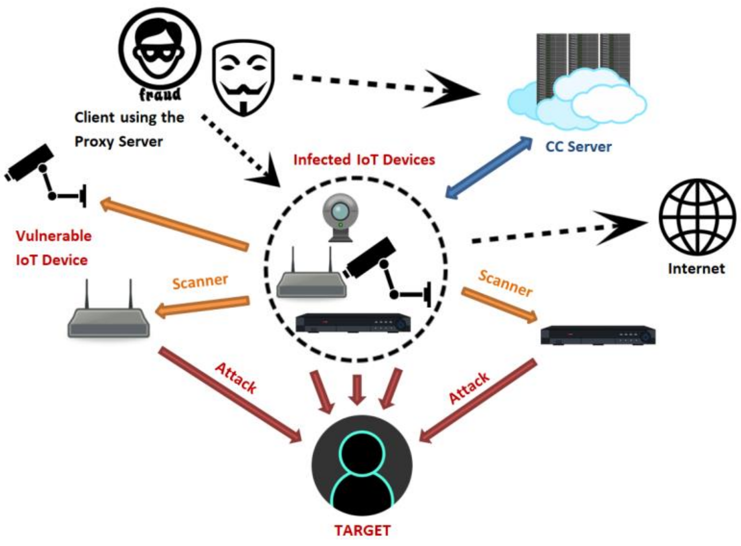
Vulnerable web interfaces (SQL injection, XSS)

Coding errors (buffer overflow)

Clear text protocols and unnecessary open ports

DoS / DDoS

Physical theft and tampering



challenges

The incorporation of the IoT in the context of smart cities **significantly increases this complexity**, not only in the number of nodes and structure, but also in the increased heterogeneity of protocols and mechanisms .

From a user perspective, the IoT provides even **less ability to understand** and control internal operations than mobile smartphone platforms, with an even **greater risk of their hijack** by malware without the knowledge of the user until too late, and without the ability to protect with antivirus and intrusion detection defences.

Smart cities are in the **early stages of deployment**, in which ICT (information and communication technology) is deeply embedded all aspects of city operation and service delivery.

challenges

Smart city : several interdependent critical infrastructures

1. the Internet (including mobile telephony networks and the IoT)

2. power grid

3. transportation networks

Capturing, modelling, and ensuring resilience of these interdependencies is not trivial

Current IoT Models

IEEE

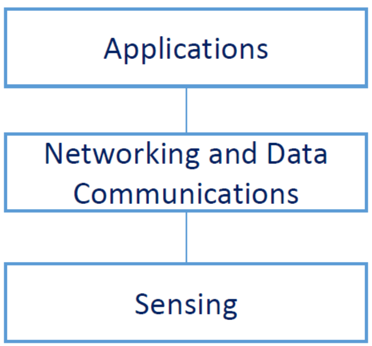


Fig. 1. IEEE P2413 three-level IoT model [11]

International Telecommunication Union

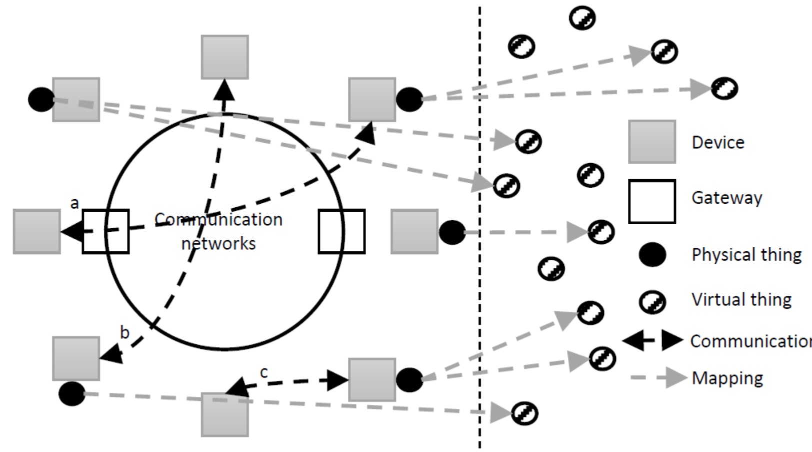


Fig. 2. ITU Y.2060 IoT model [13]

“a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”

Current IoT Models

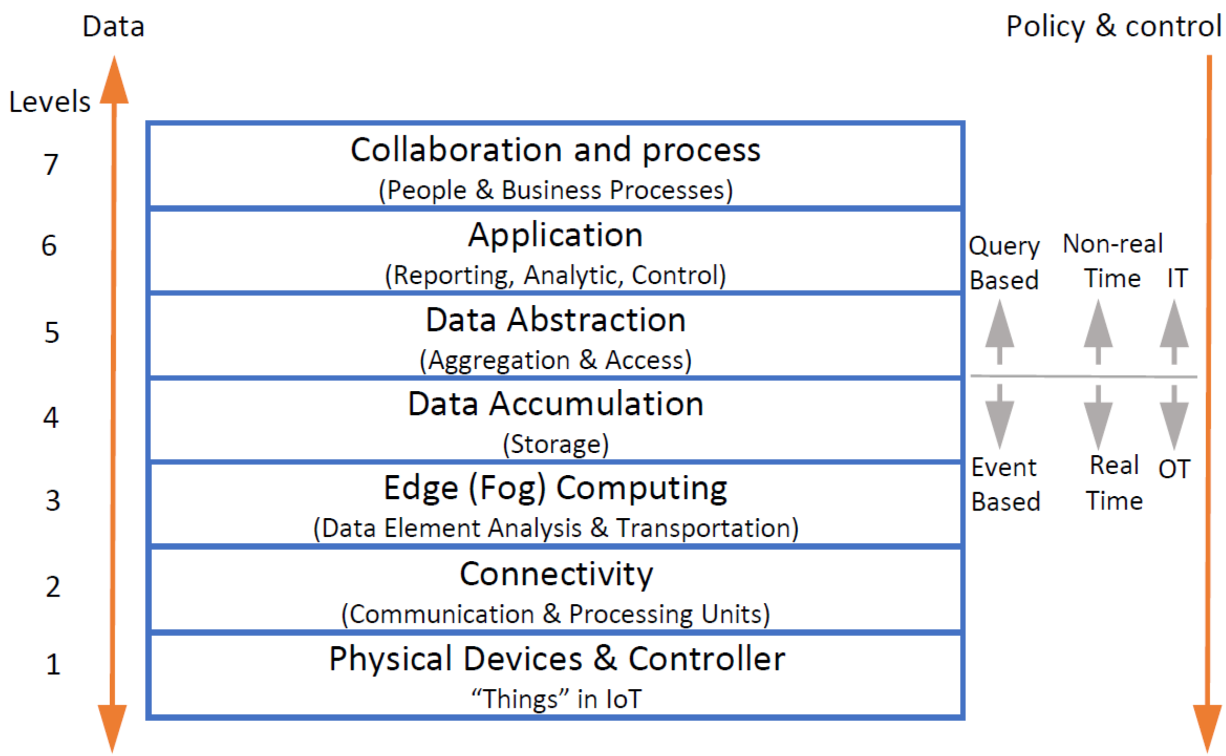


Fig. 3. Cisco IoT reference model [14]

emphasising edge-cloud computing
no insight into the multilevel network structure
nor the protocols employed

Multilevel Network Structure

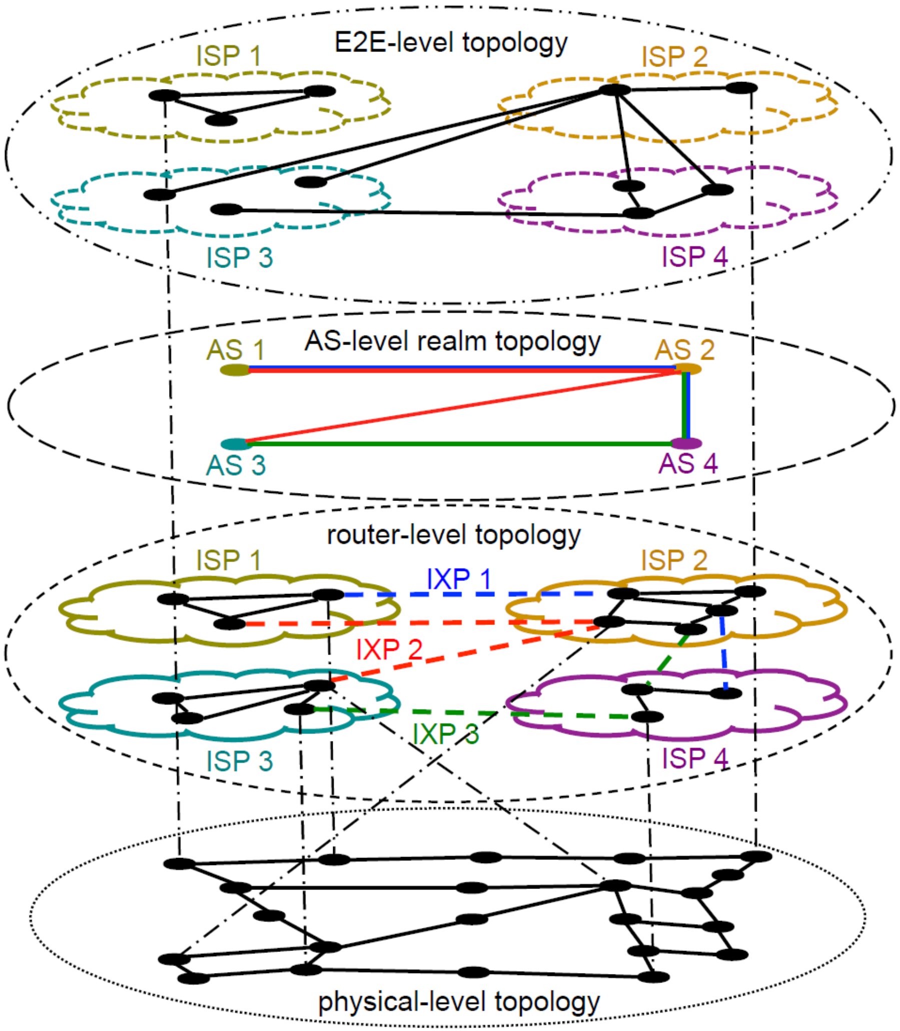


Fig. 4. Multilevel Internet graph model

the end-to-end (E2E) topology interconnecting end systems running applications.

AS-level realm topology, interconnected by BGP (Border Gateway Protocol) in the conventional Internet.

router-level topology for each service provider, mapping onto a subset of the lower vertices but with arbitrary edges. Each service provider AS (autonomous system) domain is a realm, defining a policy and trust boundary.

physical infrastructure, including **physical links** (fibre, wire, and wireless) and **all network components**: switch and router hardware, data centre components and end systems

Toward an IoT Network Model

- **Model that captures the complexity and heterogeneity** of this environment, but in a multilevel form

- **Modelling resilience** to attacks and large-scale disasters requires a graph-theoretic approach Methods

- a simulation-based approach to **model the protocols, traffic, and application scenarios**

IoT smart city model

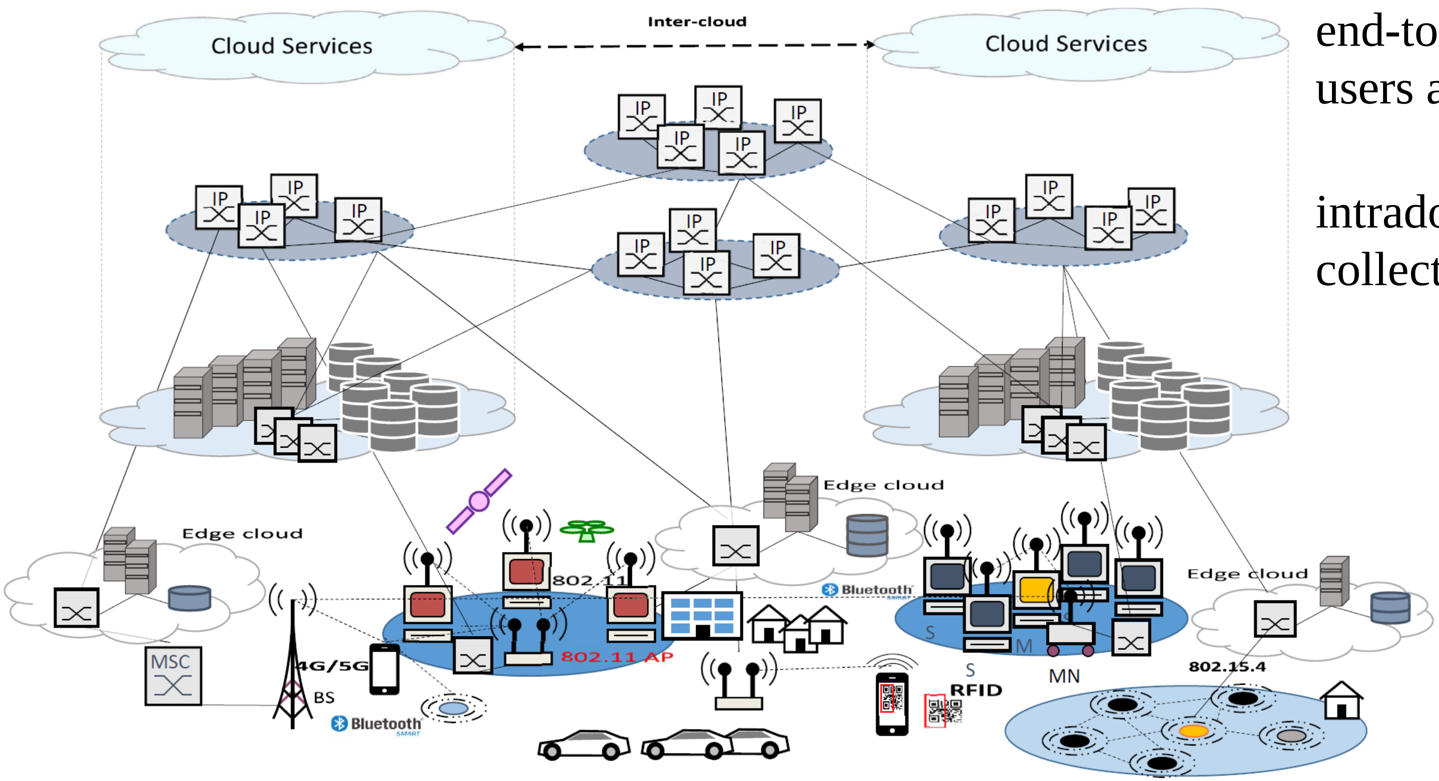


Fig. 6. Multilevel smart city IoT model

end-to-end graph connecting users and services

intradomain routing layer: collection of IP routers

The lowest level: the IoT things, sensors, home and enterprise networks, VANETs, edge- and core-cloud data centres, mobiletelephony networks, and all other physical network components including drones and satellite links

structural complexity, wide variety of protocols

islands of resilience

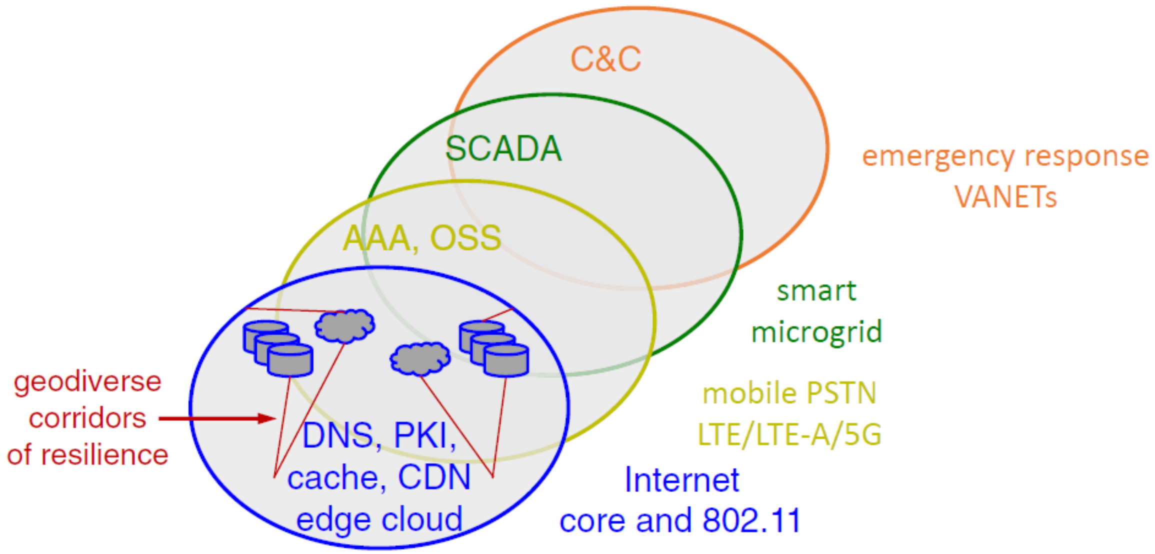


Fig. 7. Island of resilience

islands that can continue to operate
whether the core undergoes a massive failure
the links to the core are severed

Keep the island to continue operating

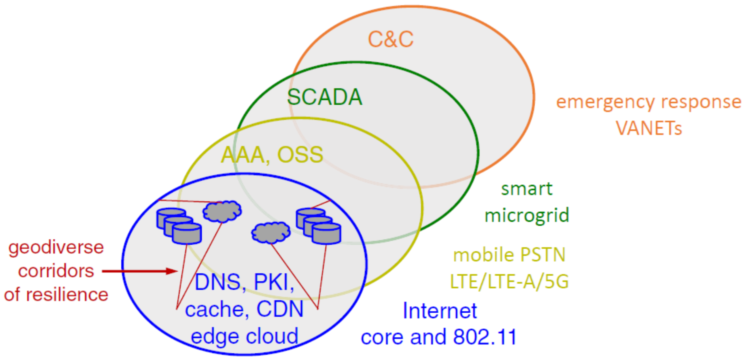


Fig. 7. Island of resilience

the needed network services such as Web caches, CDN servers, DNS servers, PKI infrastructure, and edge clouds should be within each isolatable island, replicated for redundancy

4G LTE-advanced and emerging 5G mobile networks continue to integrate with the traditional Internet, these services also need to be within islands

the island boundaries of critical interdependent infrastructure should align. a severable **micro-grid** powers the network infrastructure island, while the network island slice provides transport for the **microgrid SCADA** (supervisory control and acquisition)

resilient vehicular and airborne ad hoc and disruption-tolerant networks providing smart city connectivity are part of the island

other infrastructure boundaries should align, such as emergency response and supporting VANET (vehicular MANET) networks

corridors of resilience

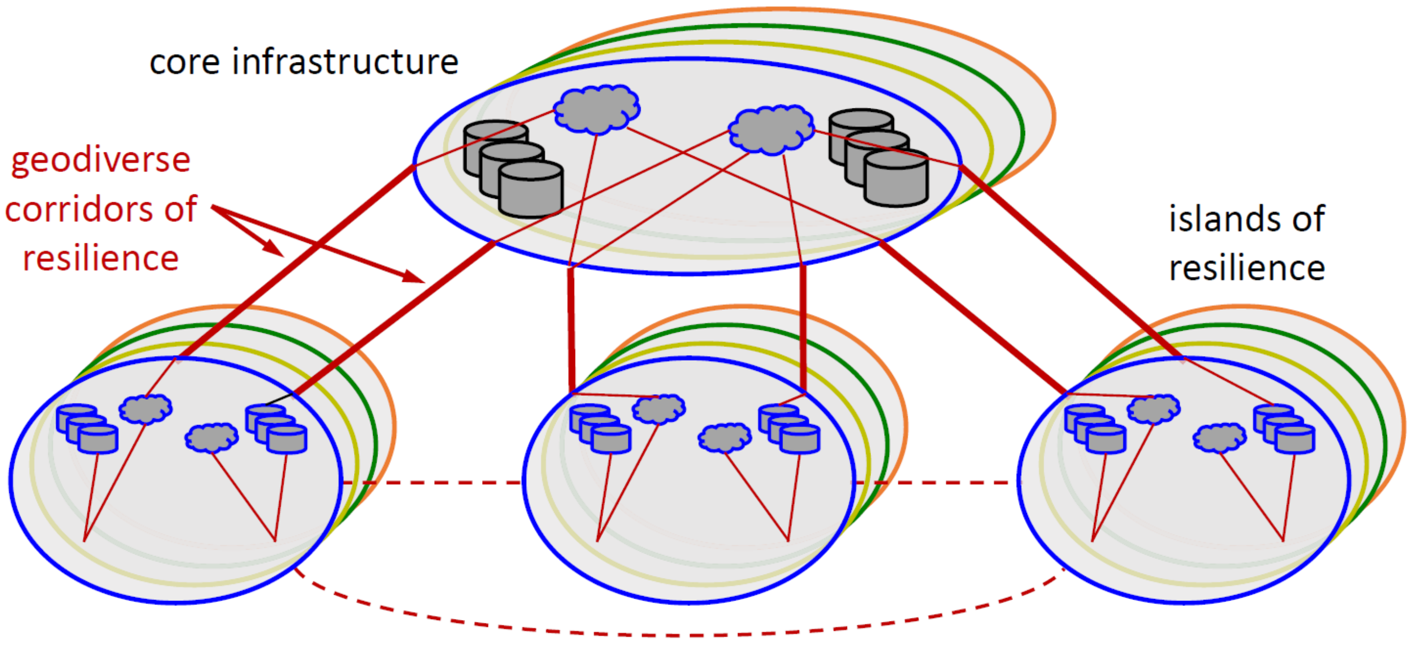


Fig. 8. Islands and corridors of resilience

Islands will be connected to the core and to one another in geodiverse corridors of resilience

These corridors are engineered for high resilience, geographically separated to survive large-scale disasters and attacks, with support for multipath routing and transport

Summary

- The main challenge is to abstract the extreme complexity and heterogeneity of this environment
- A framework for a multilevel smart city IoT model has been presented
- The concepts of islands and corridors of resilience are introduced as an architectural construct to improve resilience