Privacy and Security Challenges in Internet of Things

Manik Lal Das
DA-IICT, Gandhinagar

Disclaimer

Many third party copyrighted material is reused within this talk under the 'fair use' approach, for sake of educational purpose only. As a consequence, the usage of this presentation is restricted, and is falling under usual copyrights usage.

Thank you for your understanding!

Internet of Things (IoT)

The definition of *Internet of Things* (IoT) evolves around the central concept : "***a world-wide network of interconnected objects***", where objects can be

- addressable through unique identity
- accessible through Internet (sometimes via intelligent interface)
- self organized and repairable

Internet of Things (IoT)

The definition of *Internet of Things* (IoT) evolves around the central concept : "***a world-wide network of interconnected objects***", where objects can be

- addressable through unique identity
- accessible through Internet (sometimes via intelligent interface)
- self organized and repairable

A world of intelligent, adaptive, self organized sensors, actuators, other devices and systems that use various network technologies to connect each and every objects of physical world to web of world.

Computing Trends

Pre-computer era

H2H

Wired Computing era

H2M

Wireless Computing era

H2M

Web of world

M2M

What is Machine-to-Machine (M2M) ?

- **Machine**-To-Machine
  - Device (e.g. water meter) which is monitored by means of sensors.

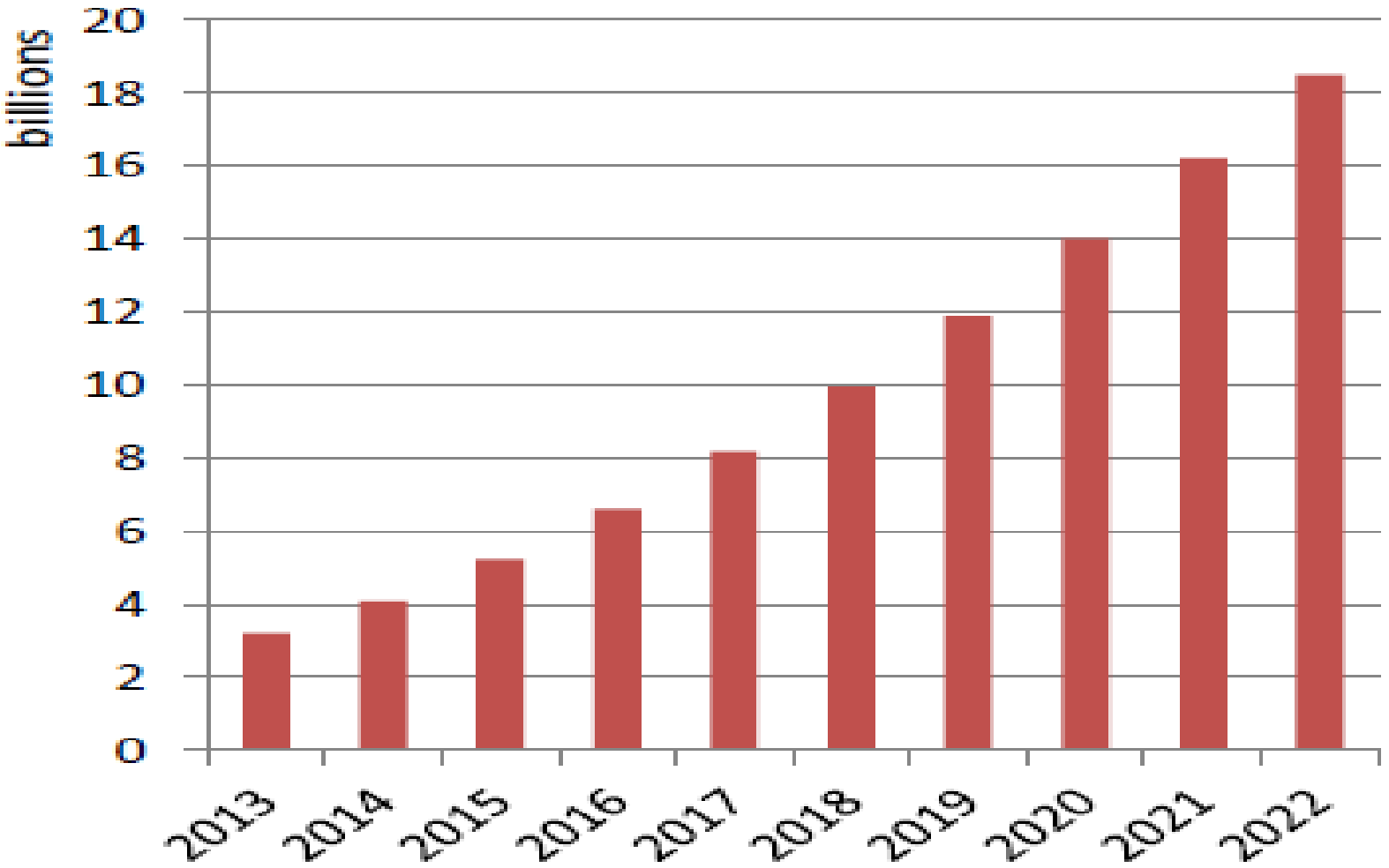
- Machine-**To**-Machine
  - Network which facilitates end-to-end connectivity between machines.
  - Composed of radio, access network, gateway, backend server.

- Machine-To-**Machine**
  - Device (e.g. valve) which is instructed to actuate.
  - Device (e.g. computer) which automatically controls and instructs other machines.

H2M ➔ M2M

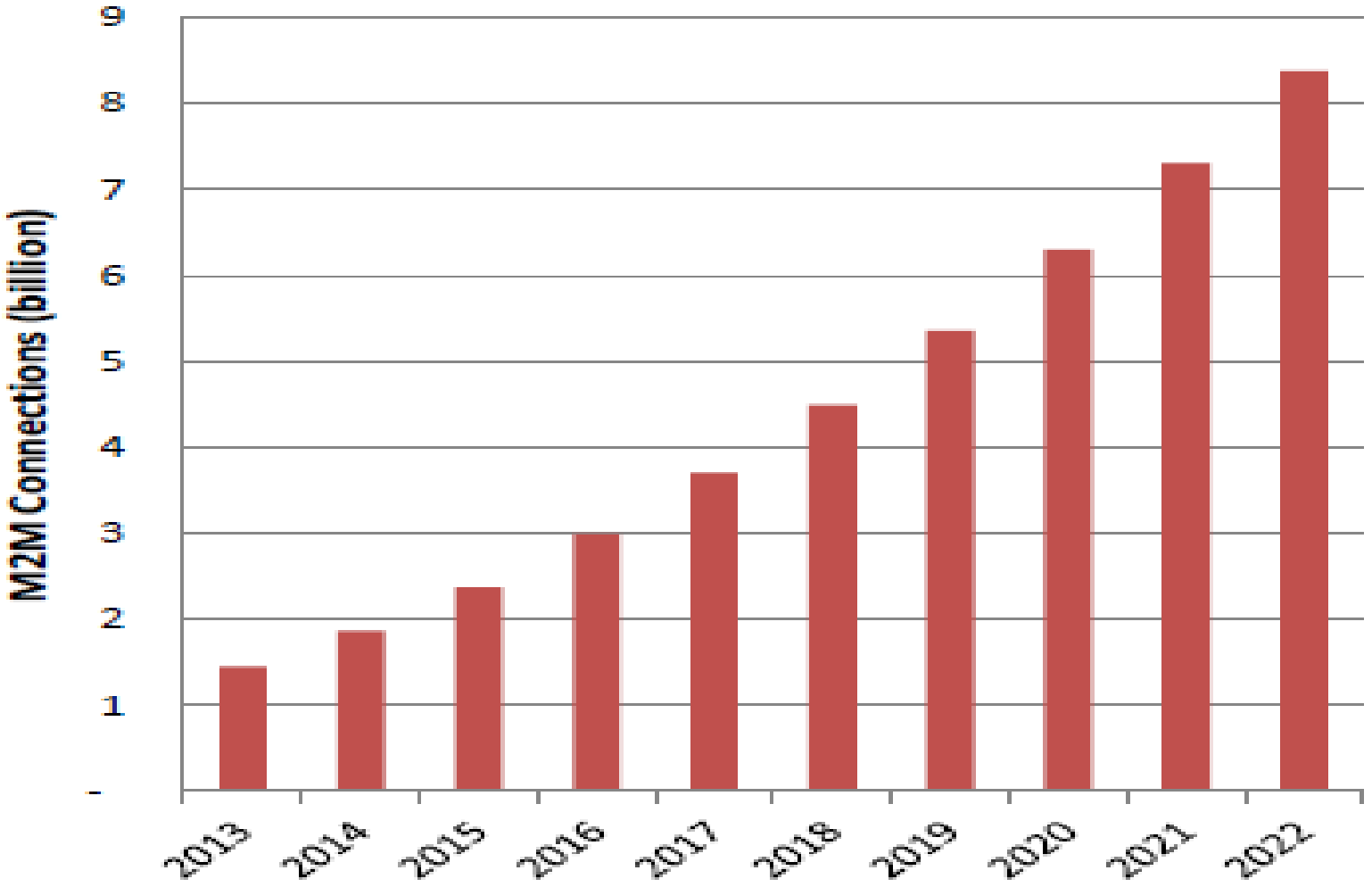
- **INSTRUMENTED**
  - Event capturing and filtering for timely response.
  - Embedded computing delivers innovative solutions.
- **INTERCONNECTED**
  - Anytime-Anywhere-Anything connectivity.
- **INTELLIGENT**
  - Human-computer-interface, user behaviour, business intelligence

Global M2M connections 2013-22



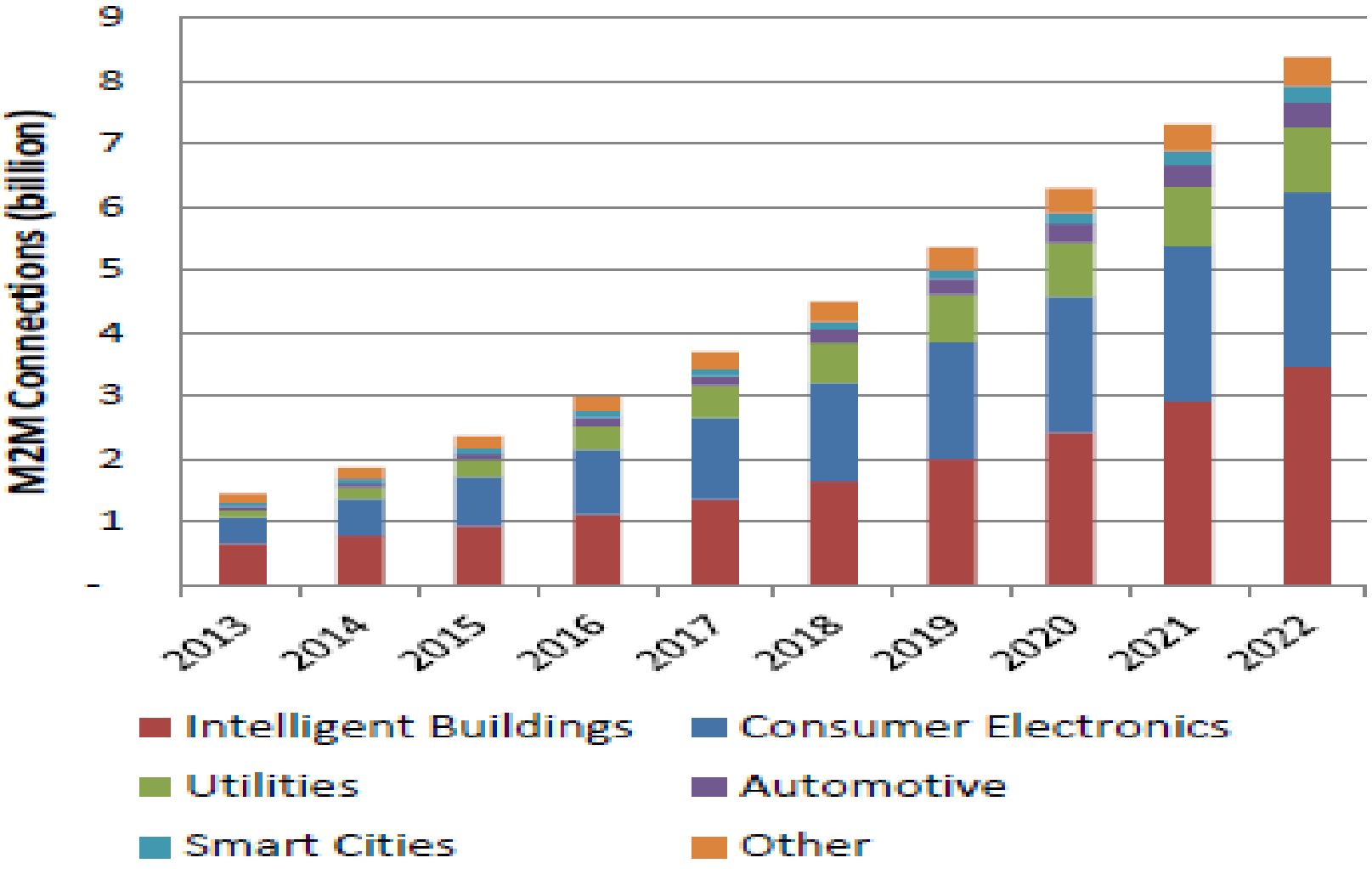
Courtesy: Machina Research

Asia M2M connections 2013-22



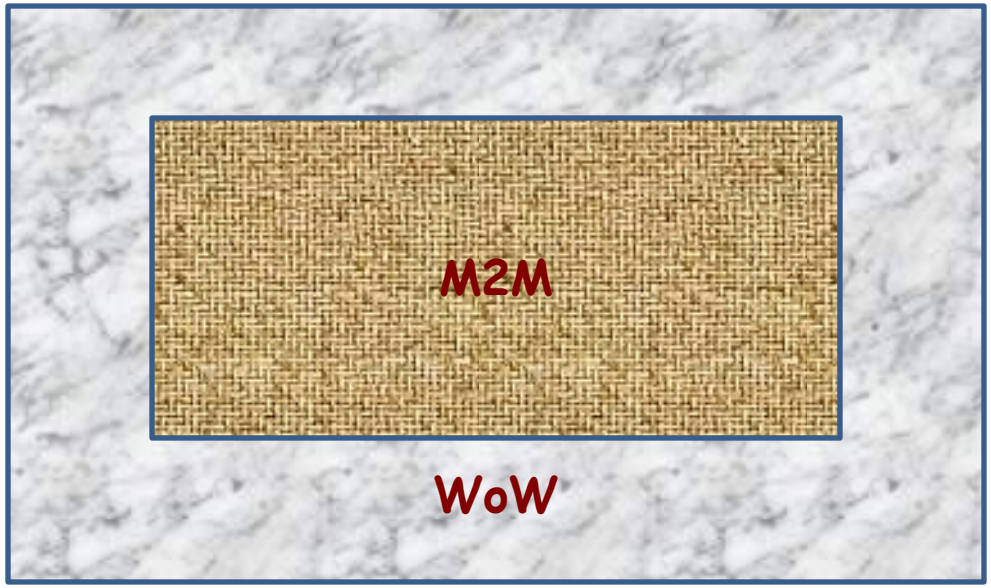
Courtesy: Machina Research

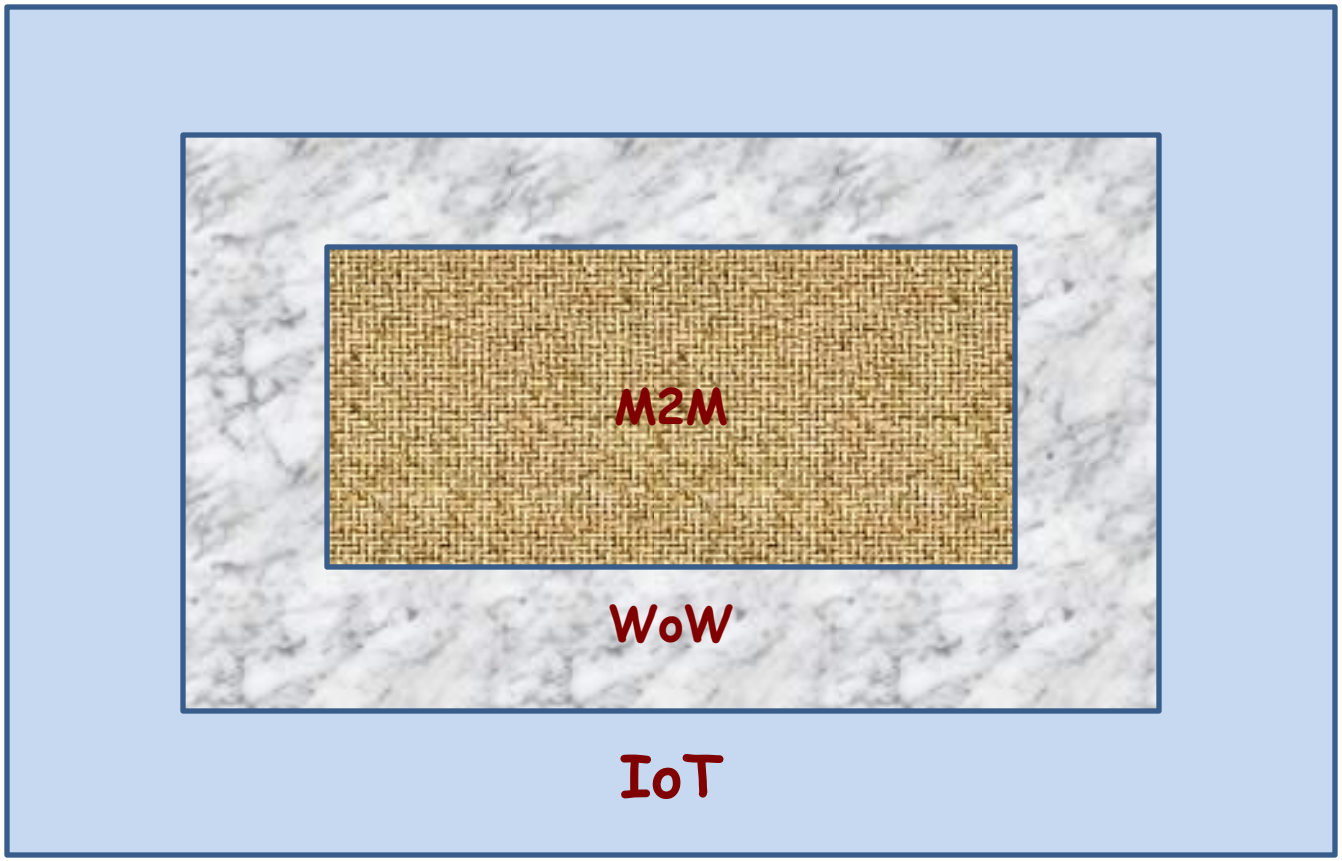
M2M connections: Driven by IB and CE



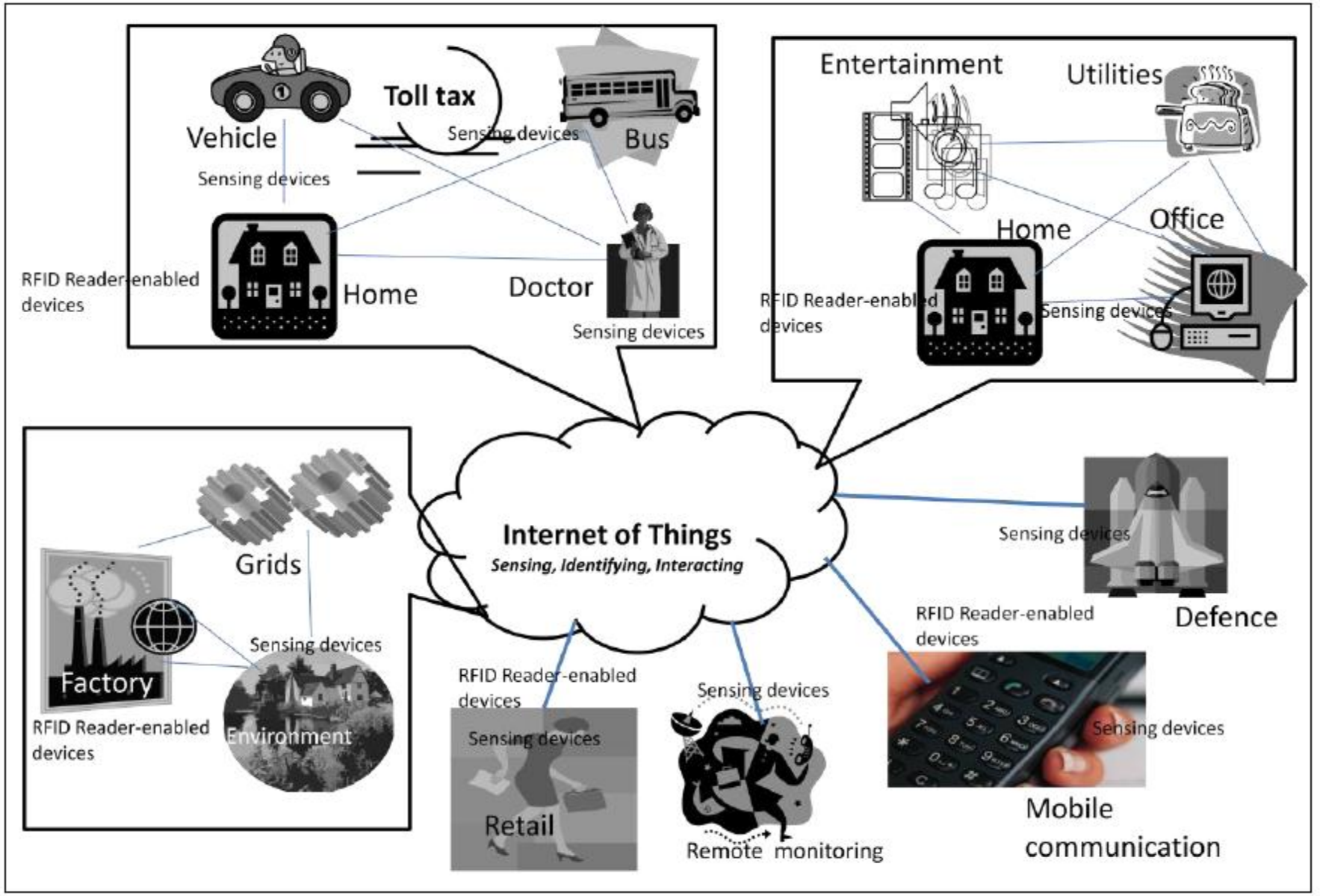
Courtesy: Machina Research


M2M


M2M
WoW


M2M
WoW
IoT

IoT Scenario



IoT Perspectives

Technological perspectives

- IoT requires context-based technological advancement, keeping consumers' convenience as the primary concern.

- Security, privacy, trusts, ownership of data as well as services are important concerns that would bring significant challenges and opportunities to manufacturers, developers, service providers and service consumers.

IoT Perspectives

Business perspectives

- Tremendous potential of electronic business has already been arrived and that is going to be scaled up in multiple folds in IoT scenarios.
- The factors that could work for adopting IoT in industry are Standards, specification, compliance, interoperability, integration, security, privacy, trusts, and ownership.
- The maximum beneficiary of IoT infrastructure is industry itself.

IoT Perspectives

Economic perspectives

- The economic perspectives of IoT offer two kinds of incentives – consumers and suppliers.
  - **consumers** would benefit from IoT infrastructure in terms of **time management** (e.g. connecting home appliances to office premises), **flexibility** (e.g. anytime-anywhere service), **security** (e.g. door/vehicle-lock/unlock alarm to mobile handset), and **revenue** (e.g. smart energy, smart transport, smart shopping).
  - **suppliers** would benefit by generating revenues in terms of smart services, smart devices and smart technology to assess vulnerabilities and addressing them for consumers satisfaction.

    Small scale service providers can use third party infrastructure for resource sharing/pooling, and large scale providers can make best use of small industries' services.

IoT Perspectives

Human perspectives

- Intellectual property, technologies, and information on core processes reside in human minds can be used in IoT in a controlled way depending upon consumers and suppliers requirement.

- Manufacturers can act as a single source and/or a single point of failure for mission-critical application.

- Security and privacy of objects could pose a serious threat to applications and human as well.

IoT Standards/Specificaton

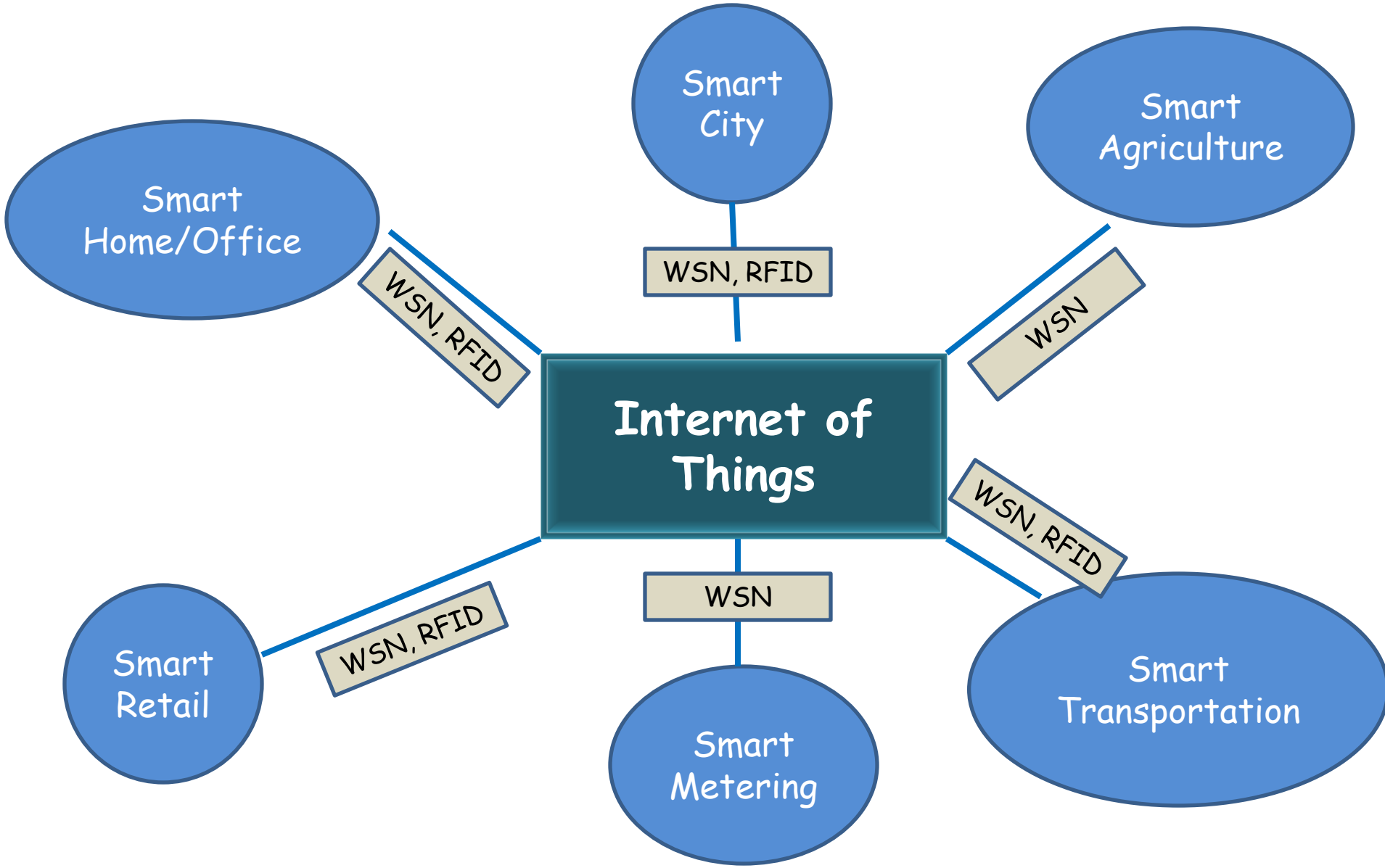
- **IETF**
  - 6LoWPAN Working Group (WG)
  - ROLL (Routing Over Low-power Lossy Networks) WG
  - CoRE WG (REST for IoT, CoAP)
  - TLS WG (DTLS)

- **ETSI**
  - M2M system standardization (CoAP)

- **IEEE Standard Association IoT**
  http://standards.ieee.org/innovate/iot/

…

IoT actors/applications



Smart shopping carts

- All items in the shopping centre are RFID tag-enabled.
- As items add into the cart, items details scanned by the reader.

Source: http://www.rfidjournal.com/article/articleprint/3868/-1/1/

Smart Refrigerator

- Recognize what's been put in it.
- Recognize when *items* are removed.
- Notify you when *items* are expired.
- Shows recipes that most closely match with what is available in it.
- Access refrigerator from a handheld device (from office or shopping complex).

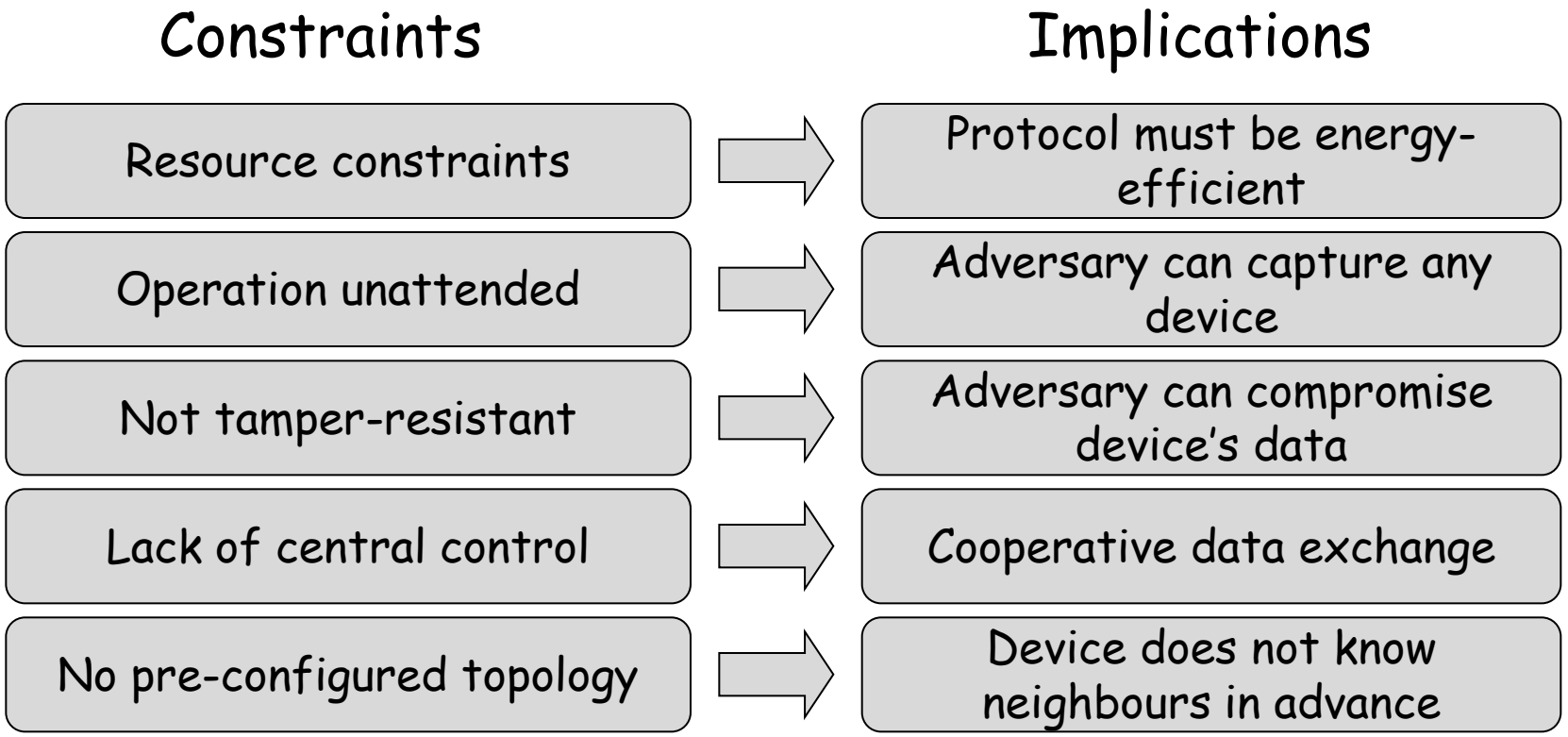
Source: http://cs.nyu.edu/~jml414/ui/assign3/smart_refrig.html

IoT actors

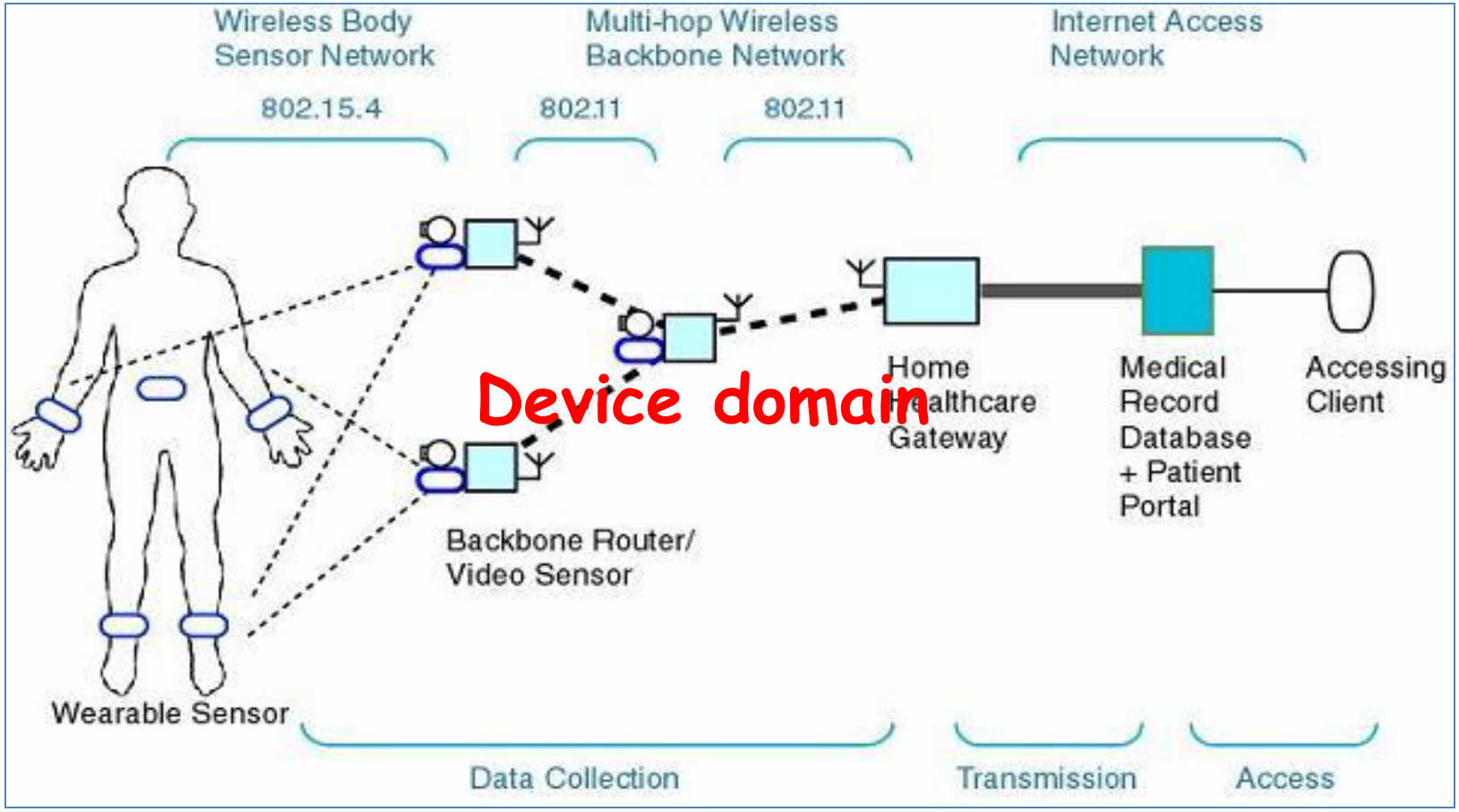
- **Constrained device** is a low-cost, low-power device that might have following functionality:
  - communicate on short distances (WSN, RFID)
  - sense environmental data (WSN)
  - perform limited data processing

- The communication between devices and other entities rely on radio wave, which is susceptible to many attacks.

Characteristics of Constrained Device



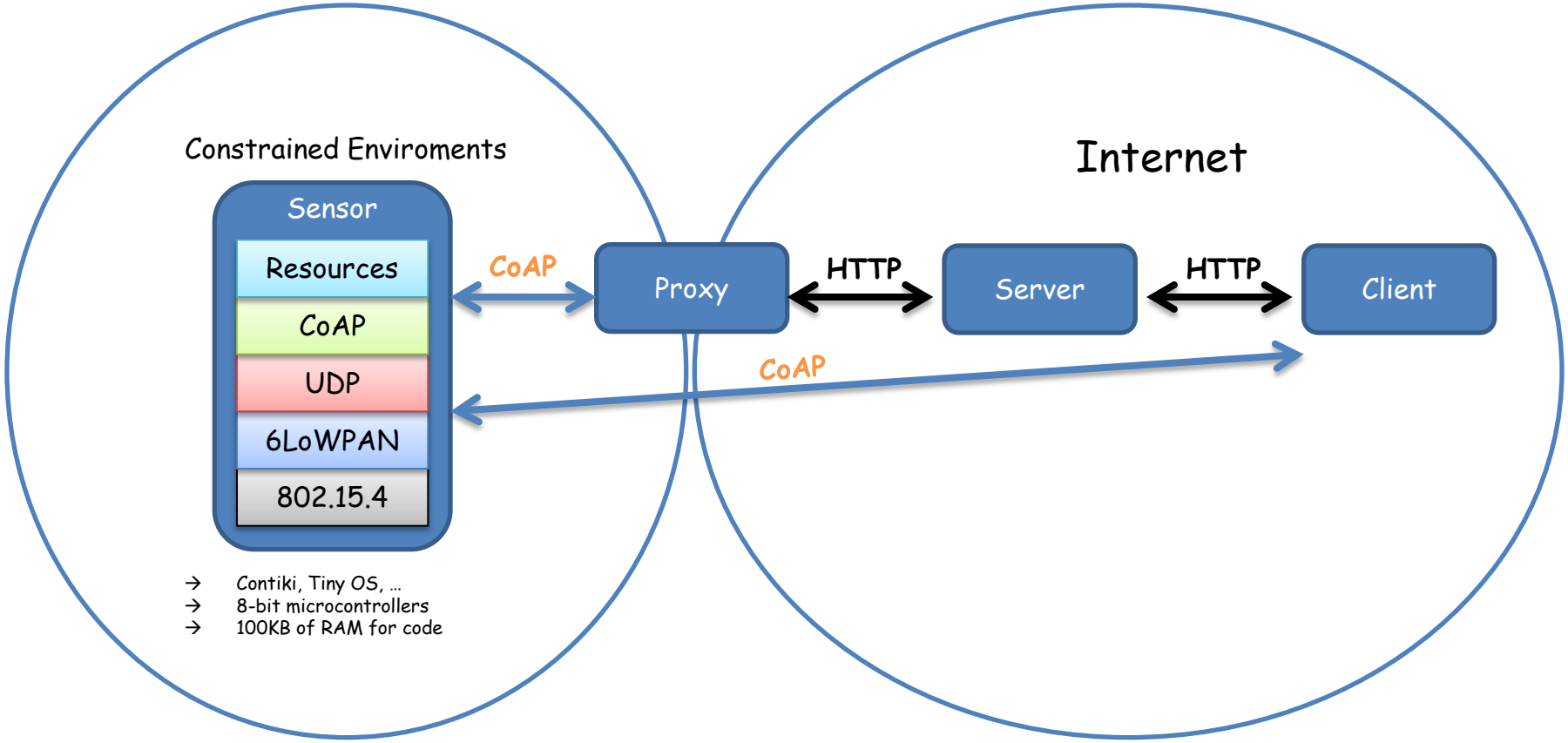
Network domain



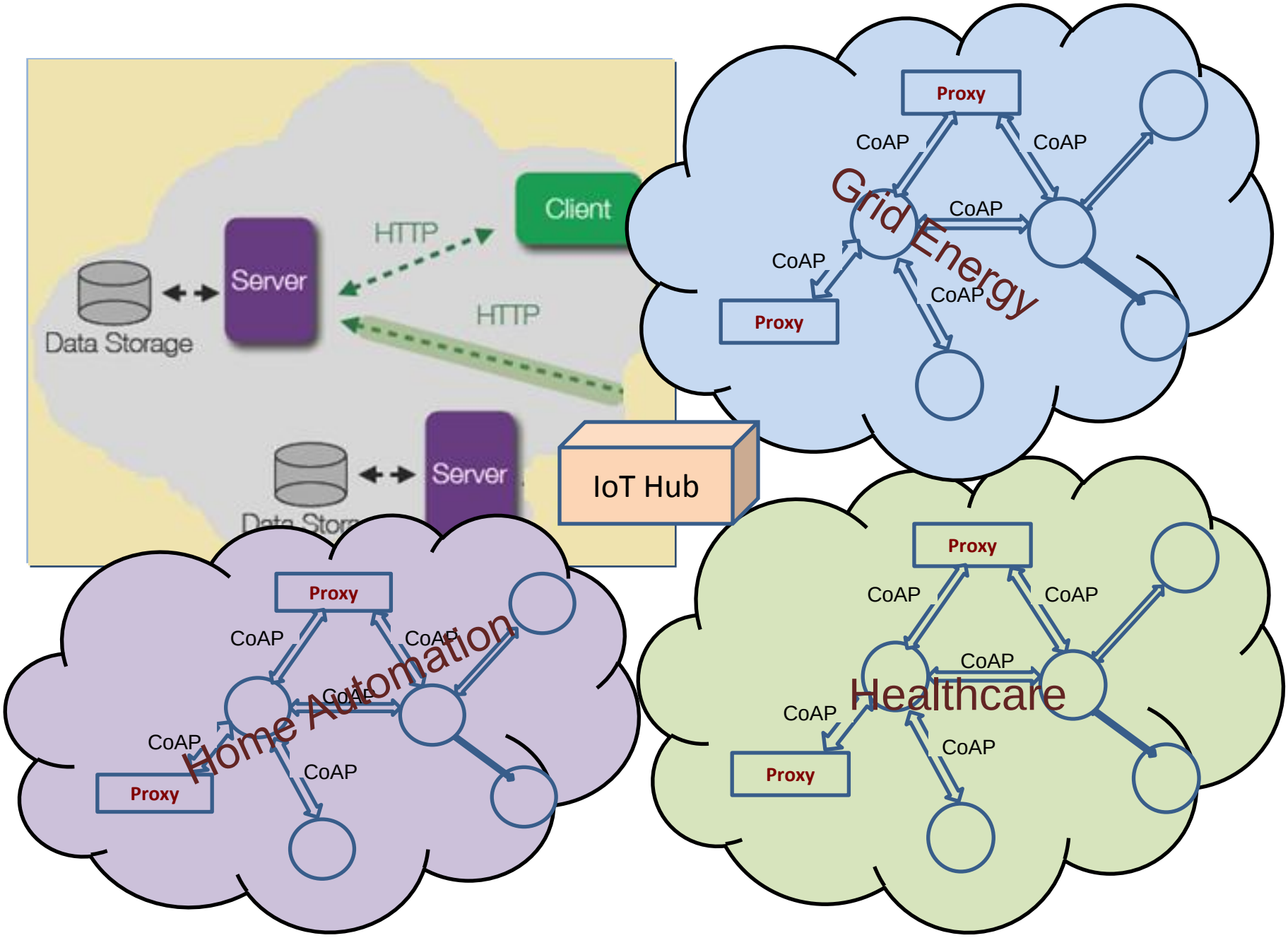
Device domain

Application domain

CoAP: Constrained Application Protocol [RFC 7252]



CoAP is an **application layer** protocol that enables **web services** for **constrained devices** and networks.


Client
HTTP
Server
Data Storage
HTTP
Server
IoT Hub
Proxy
CoAP
CoAP
Grid Energy
CoAP
CoAP
Proxy
Proxy
CoAP
CoAP
Home Automation
CoAP
CoAP
Proxy
Proxy
CoAP
CoAP
Healthcare
CoAP
CoAP
Proxy

Internet is possibly the victim of its success as far as security is concerned

Security – figure out what you mean…

- In an objective sense, security measures the **absence of threats** to acquired values.

- In a subjective sense, security measures the **absence of fear** that such values will be attacked.

- **Security is a system property**. Security is much more than a set of functions and mechanisms.

Privacy – again figure out what you mean…

Object Privacy: eavesdropping, tracking, stealing data.

Location Privacy: tracking, monitoring, revealing data.

On one hand, entity who carries device-enabled does not want to be tracked by the terminal, which could preserve its privacy.

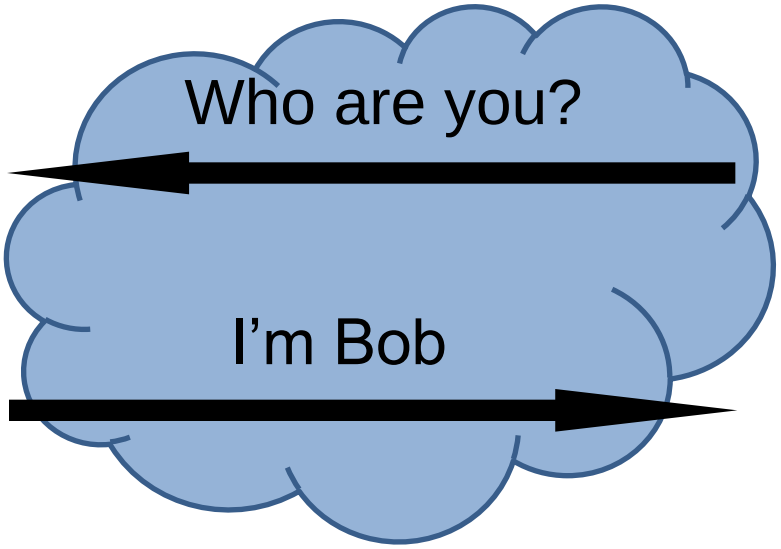
On the other hand, one requires tracing device-enabled criminals or suspicious objects in a controlled way, which could save money, national assets and human lives.

Security and Privacy challenges

- Authentication, Integrity, Confidentiality, …, based on application requirement.
  - Universal authentication
  - Identity management
  - Authorized access of data
  - Availability of data (a big challenge in near future!)
- Lightweight security protocol for constrained environments.
- Privacy preserving service.
- Trust and ownership issues.

A Two-party game

Prover



Verifier

Authentication, integrity

A Two-party game…contd.

Challenge c

Response $f(x,c)$

Confirmation $f(x,c')$

Prover

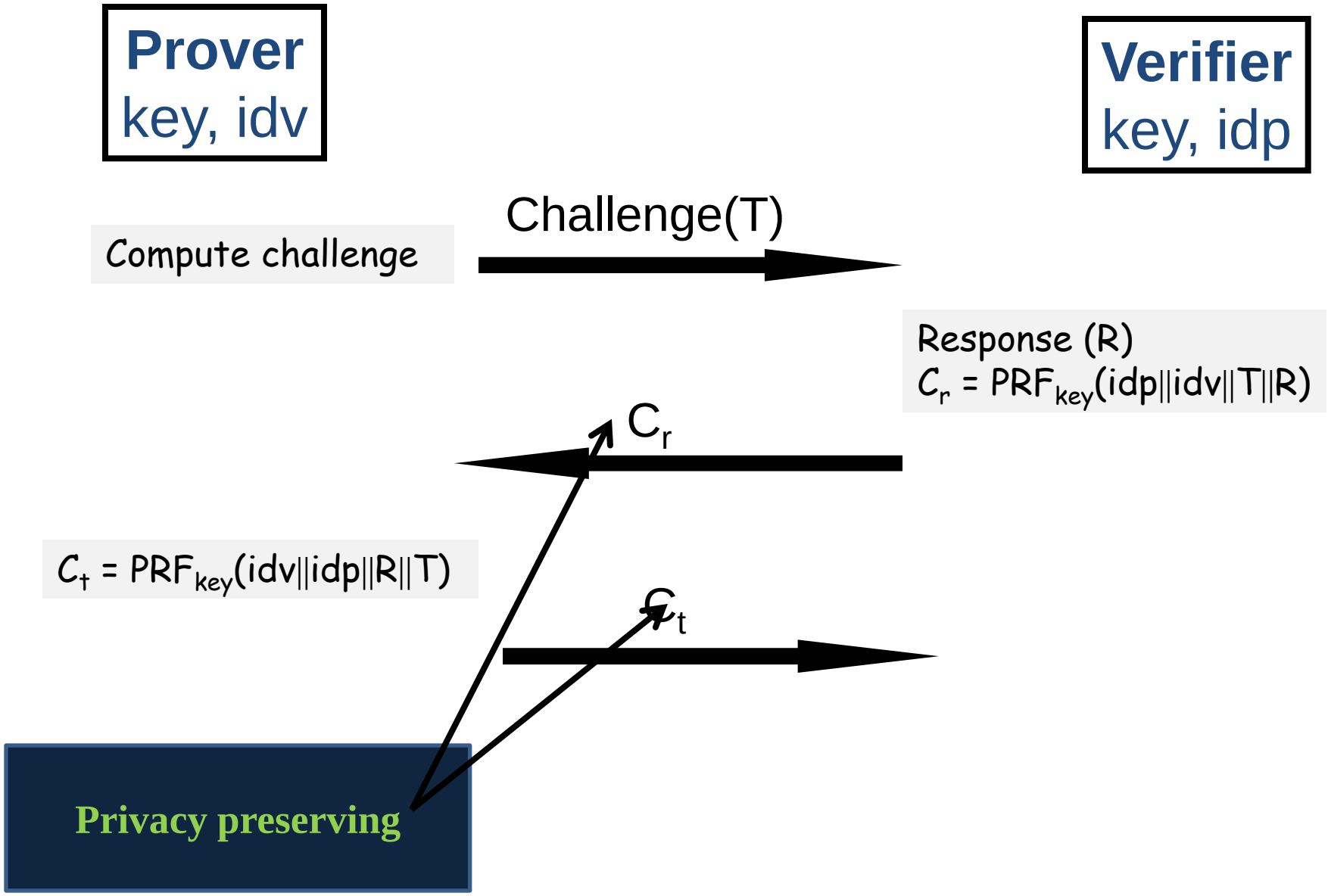
Verifier

(mutual)authentication, integrity, transient key establishment, …

- Privacy-preserved data --> avoiding link or trace.
- Authentication-preserved data --> avoiding impersonation.
- Integrity-preserved data --> avoiding data alteration.
- Confidentiality-preserved data --> avoiding unauthorized access to data

- Privacy-preserved data --> avoiding link or trace.
- Authentication-preserved data --> avoiding impersonation.
- Integrity-preserved data --> avoiding data alteration.
- Confidentiality-preserved data --> avoiding unauthorized access to data

Privacy is the goal



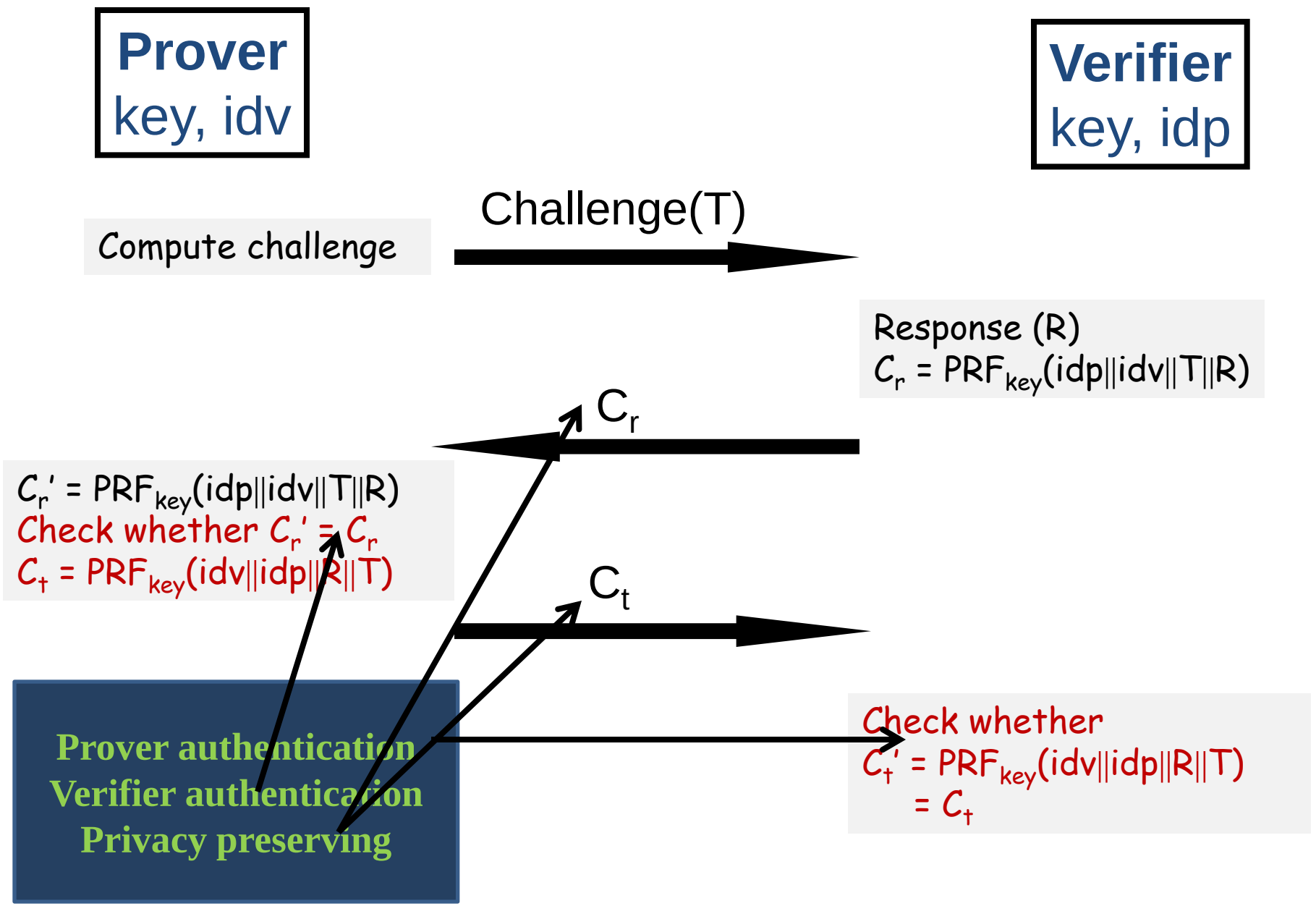
IoT scenarios/applications

- Home appliances
- Transport
- E-Governance
- Social networking
- Defense
- …

Privacy is a concern

- Privacy-preserved data --> avoiding link or tracing.
- Authentication-preserved data --> avoiding impersonation.
- Integrity-preserved data --> avoiding data alteration.
- Confidentiality-preserved data --> avoiding unauthorized access to data

Privacy, authentication are golas



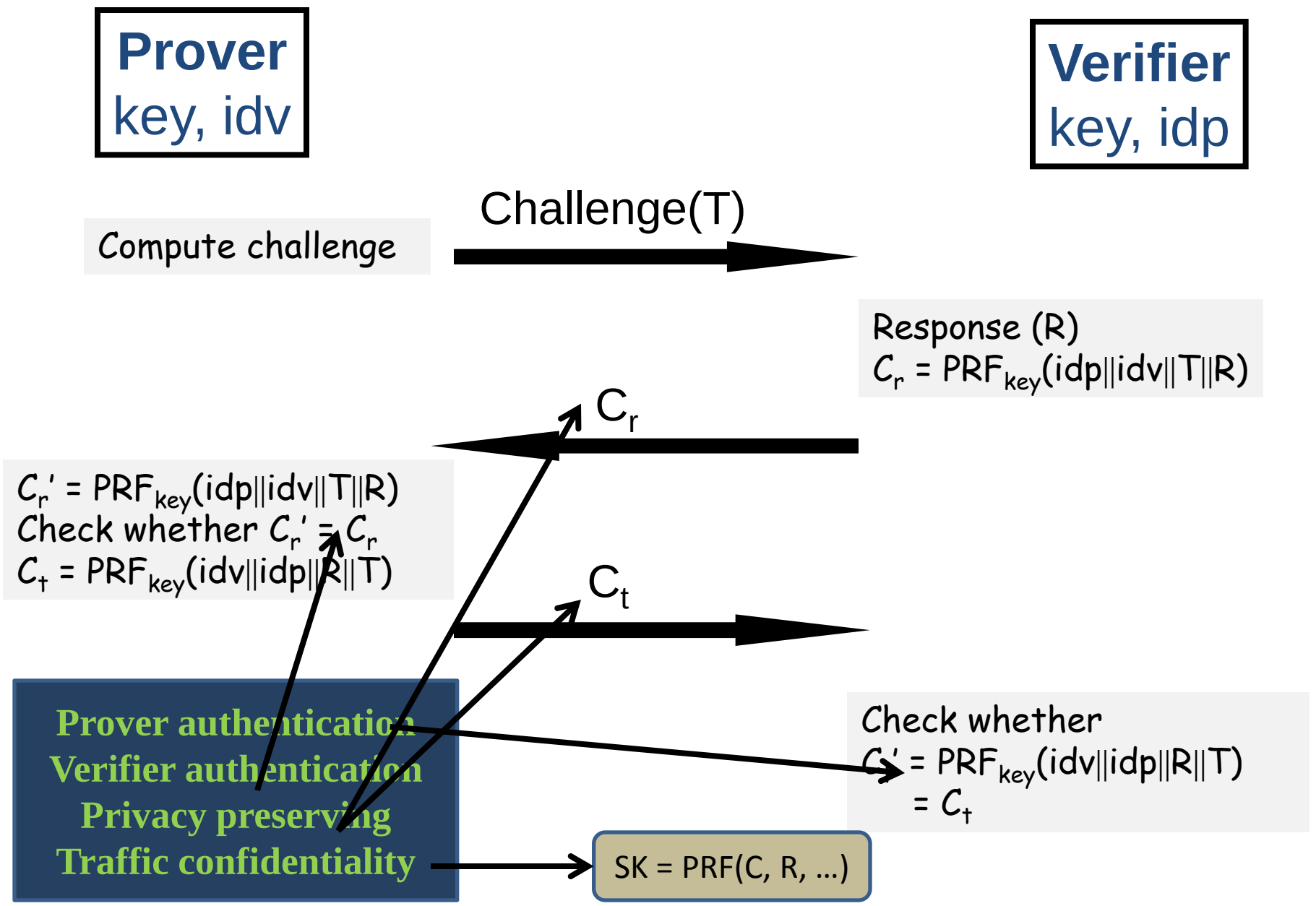
IoT scenarios/applications

- Home appliances
- Transport
- E-Governance
- Social networking
- Banking
- Enterprise systems
- Telecommunication
- Education
- Agriculture
- Defense
- …

Privacy, Authentication, Integrity matters!

- Privacy-preserved data --> avoiding link or tracing.
- Authentication-preserved data --> avoiding impersonation.
- Integrity-preserved data --> avoiding data alteration.
- Confidentiality-preserved data --> avoiding unauthorized access to data

Privacy, authentication, confidentiality



IoT scenarios/applications

- Home appliances
- Transport
- E-Governance
- Social networking
- Defense
- …

- Home appliances
- Transport
- E-Governance
- Social networking
- Defense
- Banking
- Consumer Electronics
- Telecommunication
- Smart grids
- Healthcare
- …

- Home appliances
- Transport
- E-Governance
- Social networking
- Defense
- Banking
- Consumer Electronics
- Smart Grids
- Healthcare
- …

Privacy, Authentication, Integrity, Confidentiality

Adversarial Capability

- Assume that the adversary is capable of intercepting communication between Prover and Verifier, and can inject data, alter content and delete data.

- The adversary can execute some queries like *sendProver*, *sendVerifier*, *corruptProver*.

Security of the protocol

- Correctness: legitimate Prover must be accepted.
- Soundness: fake Prover should be rejected.

Security claim

For every set of inputs the result of a real execution of the protocol with **Adversary** should not give non-negligible advantage in the security parameter of the keying material.

Security is guaranteed if the protocol is sound against a reasonably acceptable adversarial model.

Privacy of the protocol

- Learning Phase: Adversary gathers enough (T, C_t) and (R, C_r) by *sendProver* and *sendVerifier* queries with many provers. Assume that the adversary has compromised all provers except 2 provers, say P_1 and P_2.
- Challenge Phase: Challenger submits the following to the adversary:

$Exp^b_{S, A}(k)$:
1. $t_b \in_R Z_q$
2. $T_b, C_{b, real} \leftarrow SendProver_{real}(., x_b)$
3. Return $P_{b, real}$

$Exp^b_{S, A}(k)$:
1. $t_b \in_R Z_q$
2. $T_b, C_{b, random} \leftarrow SendProver_{random}(., x_b)$
3. Return $P_{b, random}$

Adversary's task is to guess whether
$P_{b,t} \in \{P_1, P_2\}$, where $t \in \{real, random\}$.

Privacy claim

For every set of inputs the result of a real execution of the protocol with **Adversary** is computationally indistinguishable from the result of a random execution with **Adversary**.

Privacy is guaranteed if the adversary cannot distinguish with which one of two provers, he is interacting through a large set of gathered queries.

Finally, Efficiency is equally important

Gate Equivalent (GE), a standard measurement unit

Example: On a constraint chip the implementation of:
- the ECDSA takes roughly 10000 GE
- the AES encryption takes roughly 3600 GE
- the hash algorithm SHA-1 takes roughly 8120 GE
- the EC point multiplication takes roughly 1000 GE

With this, the cost of the protocol discussed here would be:

- for privacy-preserving feature ~ 5600 GE at each side.
- for privacy, authentication-preserving feature ~ 9200 GE at each side.
- for privacy, authentication, confidentiality-preserving feature ~ 11200 GE.

Courtesy: D. M. Hein, J. Wolkerstorfer, and N. Felber. ECC is ready for RFID - a proof in silicon. In proc. of International Workshop on Selected Areas in Cryptography, LNCS 5381, Springer, pp. 401–413, 2009.

Conclusions

- The reality of IoT is not far, around the corner.
  - enormous scope, challenges, and opportunities

- Internet along with high speed mobile communication would become communication backbone for IoT infrastructure.

- Manufacturers, service providers need to agree on a set of solutions based on functional and financial goals.

Conclusions

- **Security and privacy issues need more emphasis on constrained environments** (traditional solution may not work!)
  - **Lightweight crypto primitive**
  - **Proxy security, data ownership, trust, …**
  - **Denial of service, lock/unlock service, destroying data,…**

- Finally, regulatory issues, political factors have to be resolved.

Thanks!