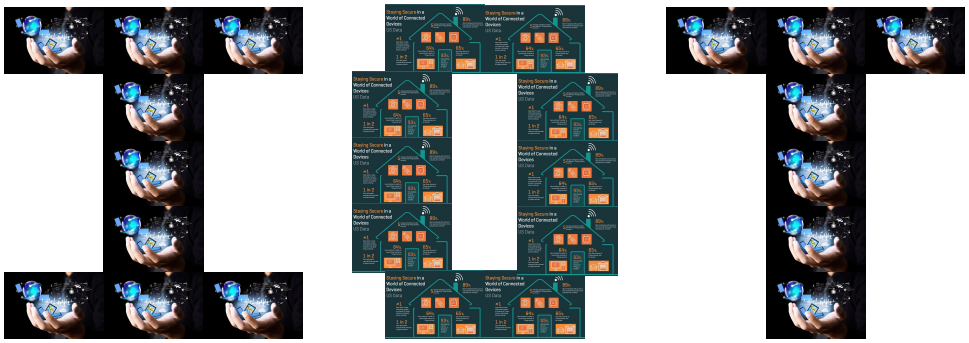
SURVEY OF TECHNOLOGIES AND SECURITY ISSUES IN



Dr. Annanda Th. RATH

PReCISE research center, Faculty of Computer Science, University of Namur, Belgium.

(September-2016)

Presentation Plan

① Introduction

② State of the art: Technologies in IoT

③ Risks and treats in IoT

④ Privacy and Data Protection Issues

⑤ Conclusion and Perspectives

Presentation Plan

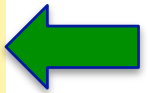
① Introduction

② State of the art: Technologies in IoT

③ Risks and treats in IoT

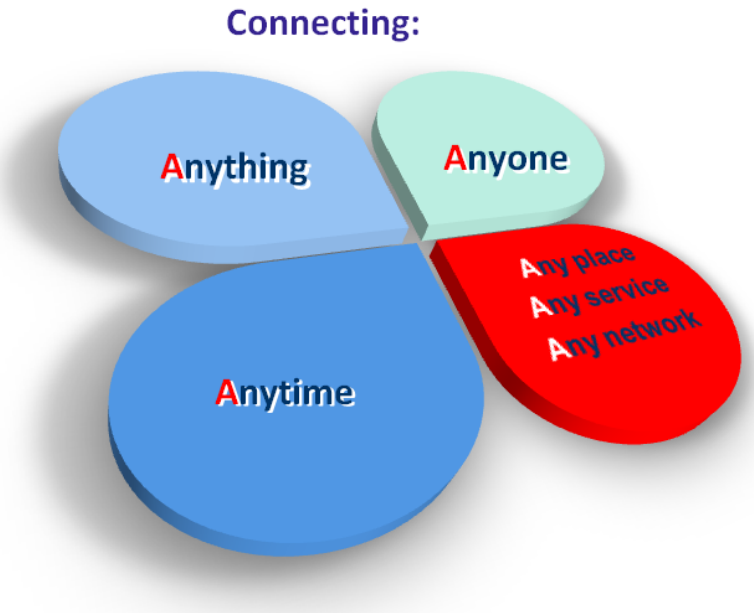
④ Privacy and Data Protection Issues

⑤ Conclusion and Perspectives



INTRODUCTION

- What is Internet of things (IoT)?
  - IoT is the networking of physical devices, vehicles, buildings and other items embedded with sensors and network connectivity that allow these objects to collect and exchange data.

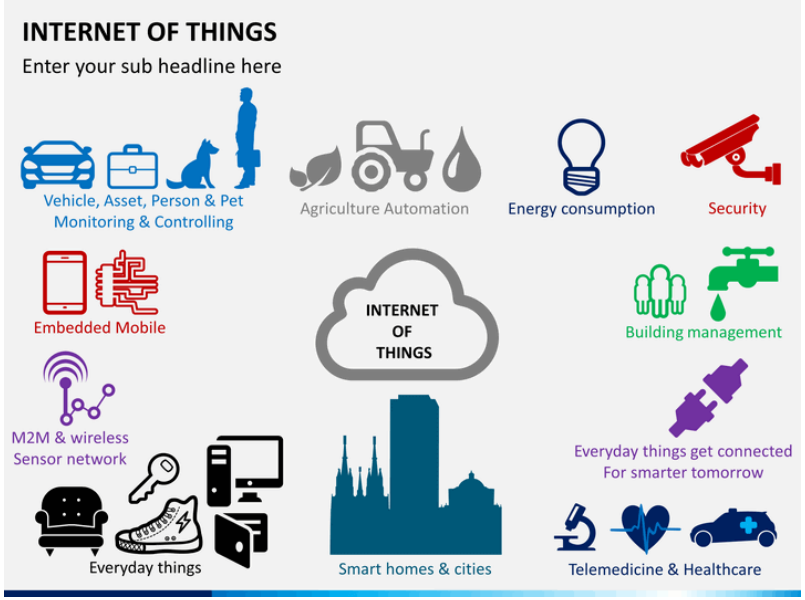


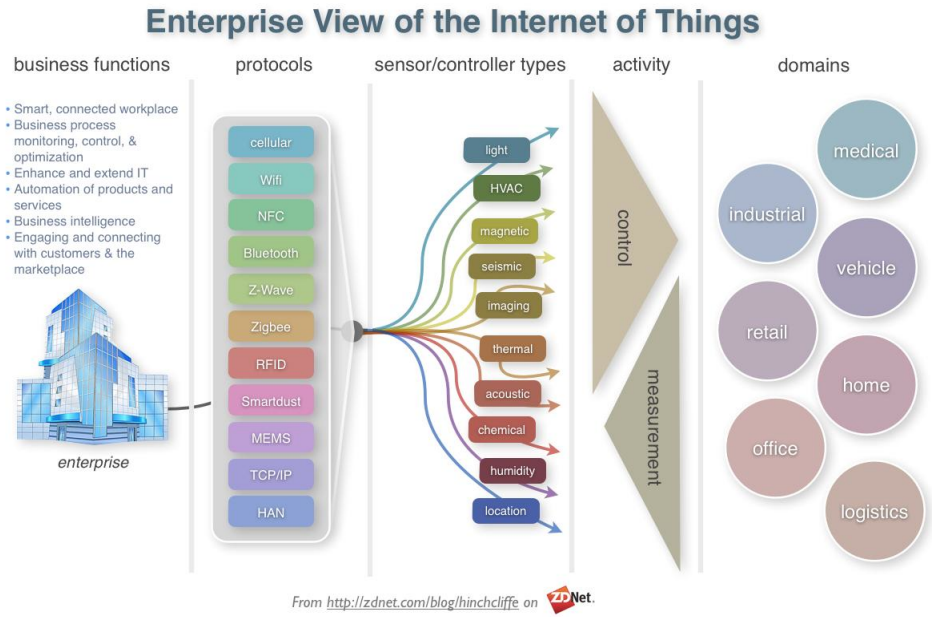
INTRODUCTION

- Why IoT is important?
  - Providing services for well-being of people
    - Smart home
    - Smart healthcare
  - Providing faster infrastructure management in large scale
    - Urban management
    - Smart city
  - Providing good and faster services to end-user
    - Promotion and advertisement
    - Agriculture
  - Enhancing Security and disaster management

INTRODUCTION

- Application domains of IoT
  - E-health and lifestyle
  - Smart home and smart city
  - Agriculture
  - Transportation
  - Security
  - Energy management

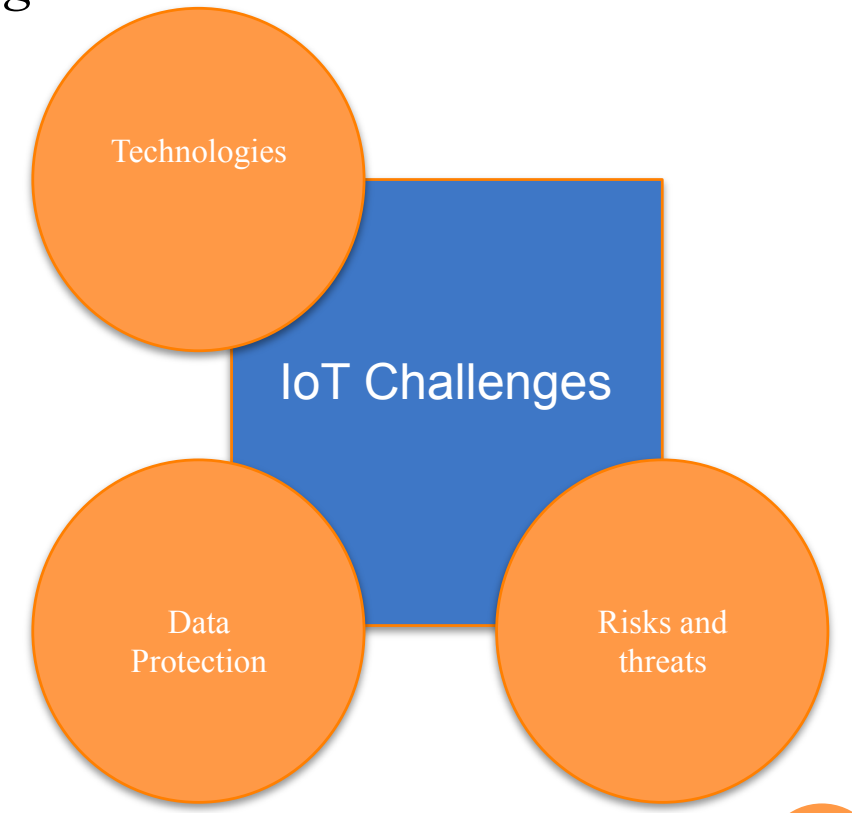




Challenges in IoT

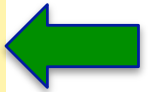
- *Since IoT works with a large number devices, the communication (connectivity) and the ability to process and protect the enormous amounts of data are the key challenges.*

- Do the existing technologies be able to address all the requirements in IoT?
- Do the existing mechanisms can be used to protect the data circulating in the IoT network?
- What are the risks and threats in IoT? Do the existing solutions used in normal network can be applied in IoT context?



Presentation Plan

① Introduction

② State of the art: Technologies in IoT 

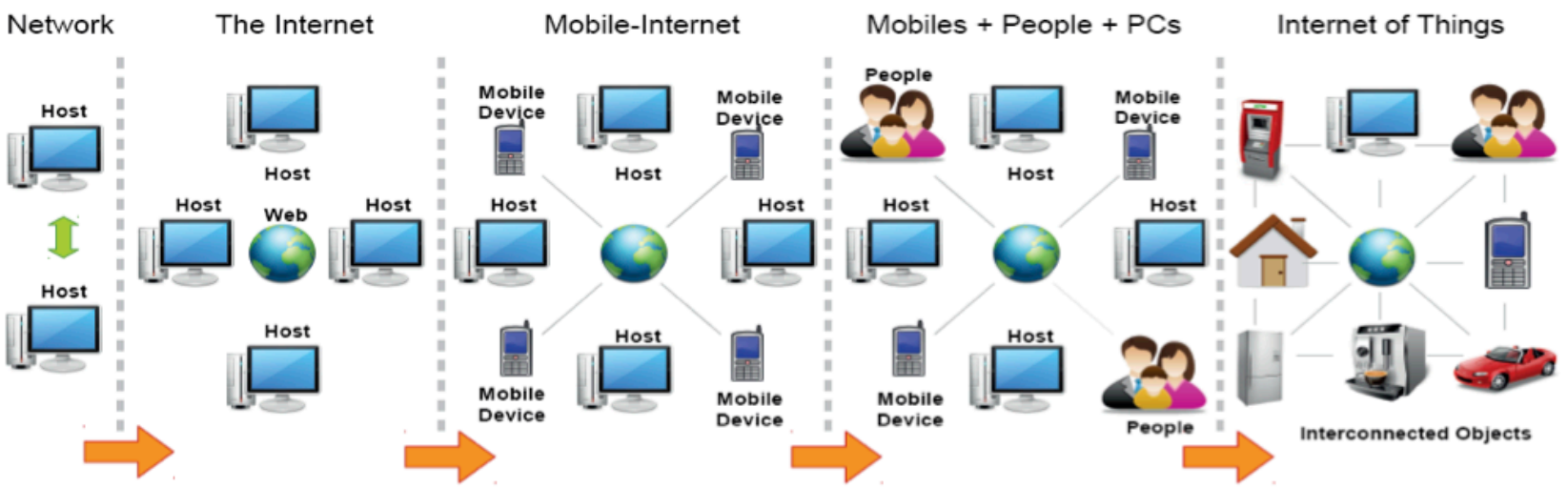
③ Risks and treats in IoT

④ Privacy and Data Protection Issues

⑤ Conclusion and Perspectives

IOT EVOLUTION

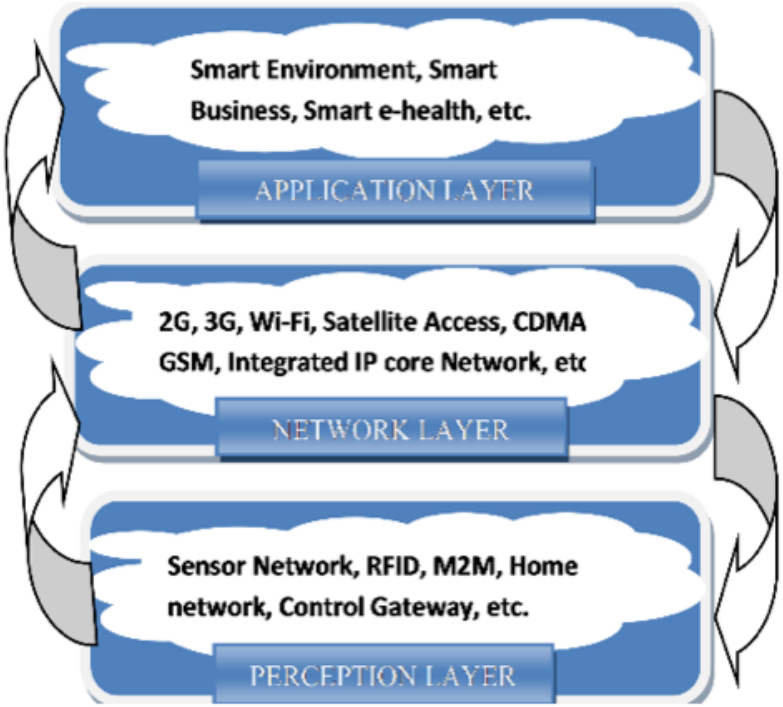
- *"The communication between computers evolves from a basic network in 1980s to Internet. Then, it comes to the era of mobile-Internet, mobile phone and finally the Internet of Things. "*



- *IoT creates a world where objects around us are connected through Internet and communicate with each other with minimum human intervention.*

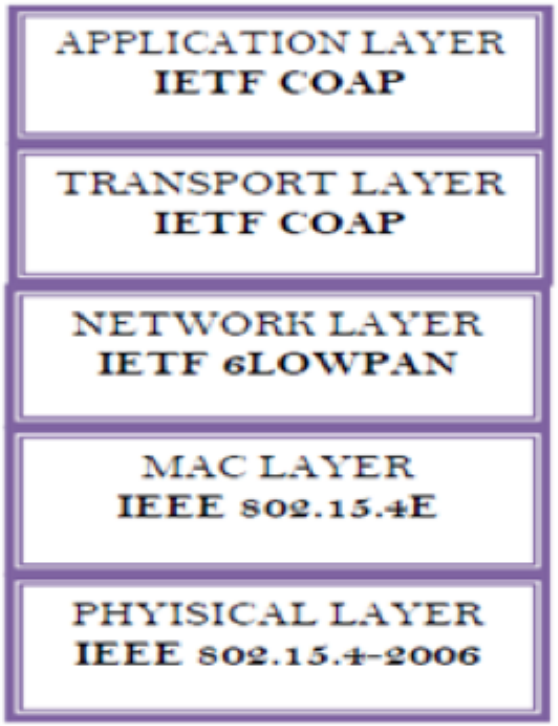
IoT ARCHITECTURE

- *"IOT architecture can be divided into three main layers. Perception layer, Network layer and and application layer"*
  - Perception layer, also known as recognition layer, gathers data/information and identifies the physical world. For example, thermal sensor gathers the temperature information.
  - Network layer, the middle layer between sensors and IoT applications, is responsible for the initial processing and broadcasting of data.
  - Application layer is the topmost layer, that supports the development of industries IoT applications.



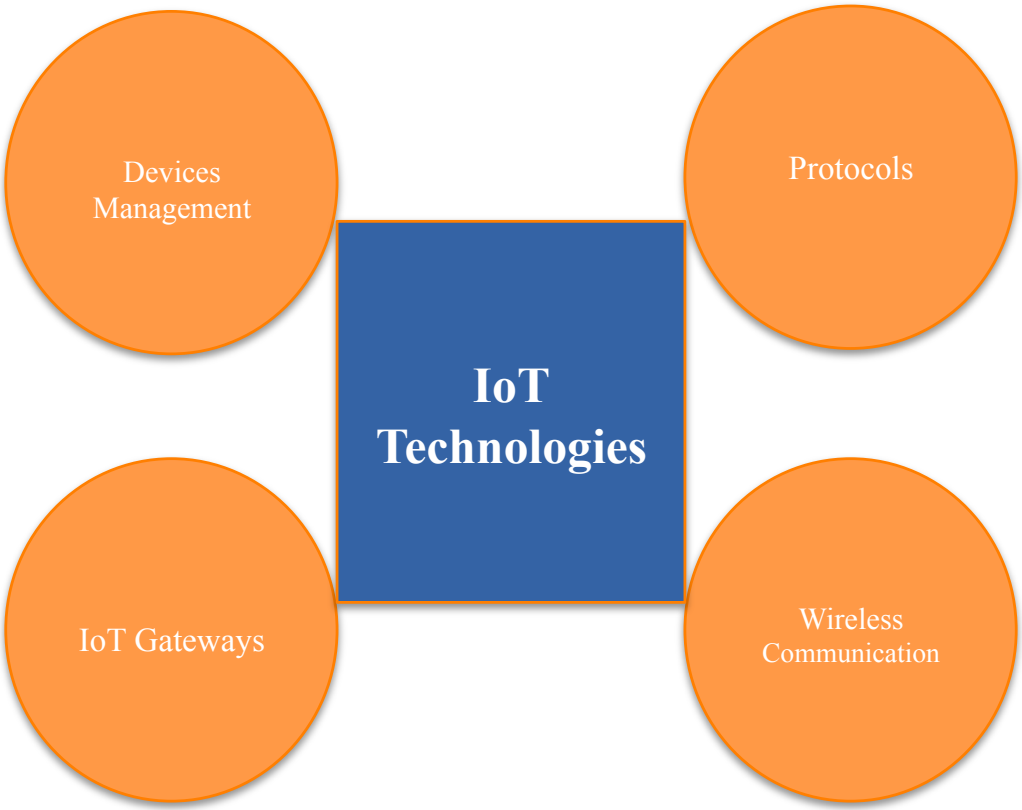
IoT PROTOCOL STACK

- *"IOT protocol stack is divided into four layers from physical layer to MAC layer, network layer, transportation layer and finally application layer."*
  - Since the large amounts of IoT applications requires only a few bit of information to be sent. It is good to look at physical layer that allows ultra low transmission rate over very narrow frequency bands with the objective of link bandwidth and power saving advantages.



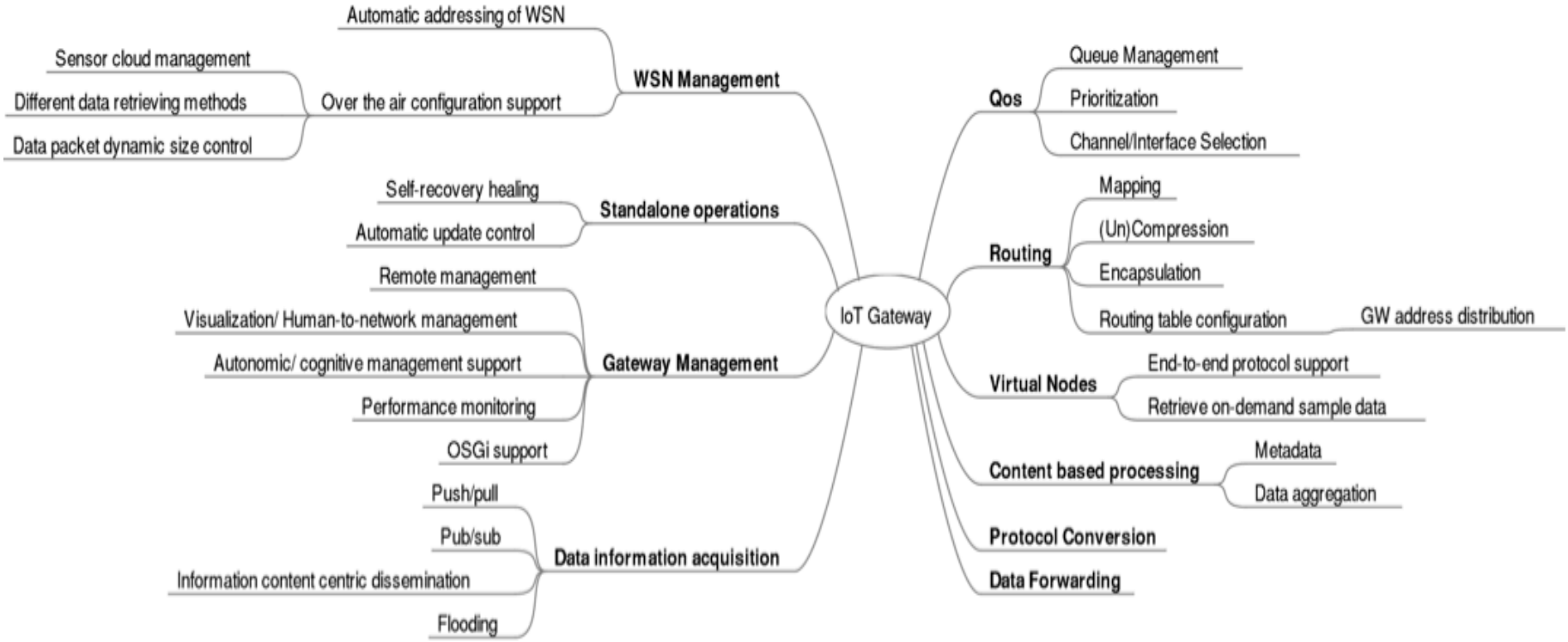
TECHNOLOGIES: IOT DEPLOYMENT

- *"To implement IoT system, we need to look at the technologies required to address some communication challenges in IoT."*



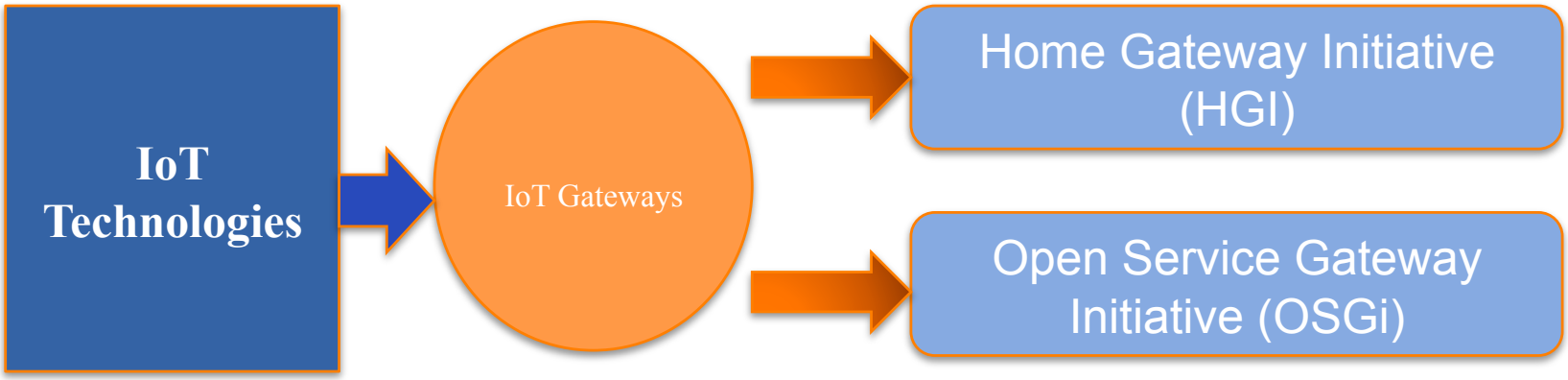
IoT Gateways

- *"IoT gateway acts as the bridge between sensors and the traditional networks, having the capabilities such as protocol conversion and device management. "*



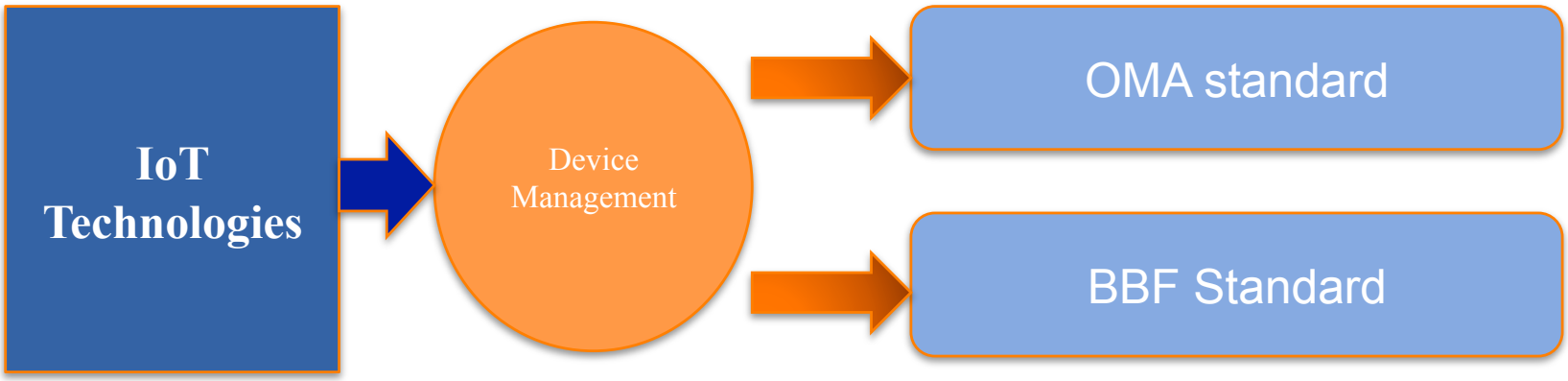
IoT Gateways: existing workgroup

- HGI develops specifications and standards for home gateway equipments for the residential market.
- OSGi is a global consortium of industry stakeholders that develop open specification to enable and promote the modular assembly of applications in Java.



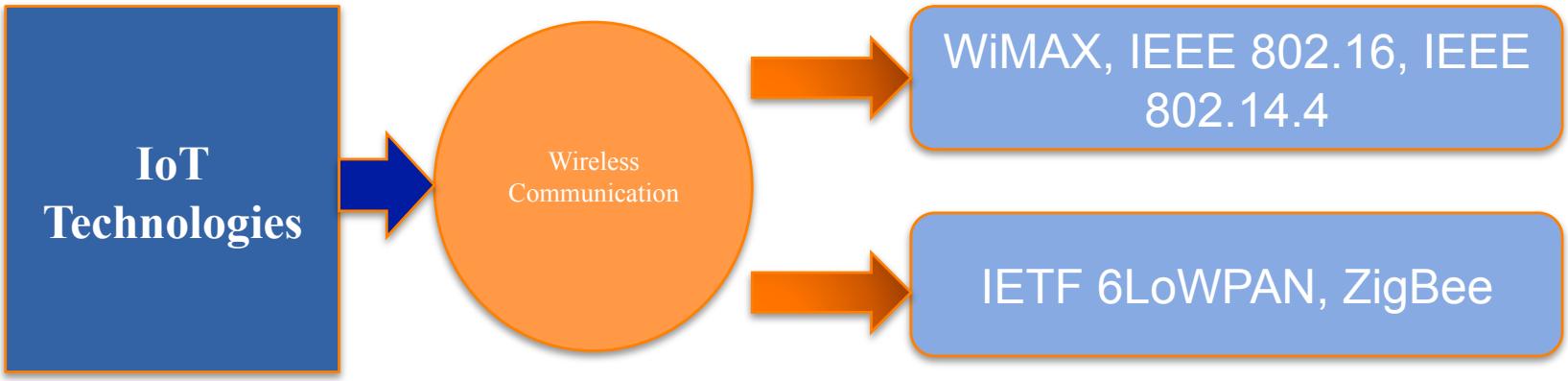
IoT Device management

- *"IoT is characterized by a large number of inter-connected devices. Thus, standardizing the device management solution is important to ensure the interoperability among devices."*
  - Device management in OMA (Open Mobile Alliance)
  - Device management in BBF (Broad Band Forum)



WIRELESS COMMUNICATION

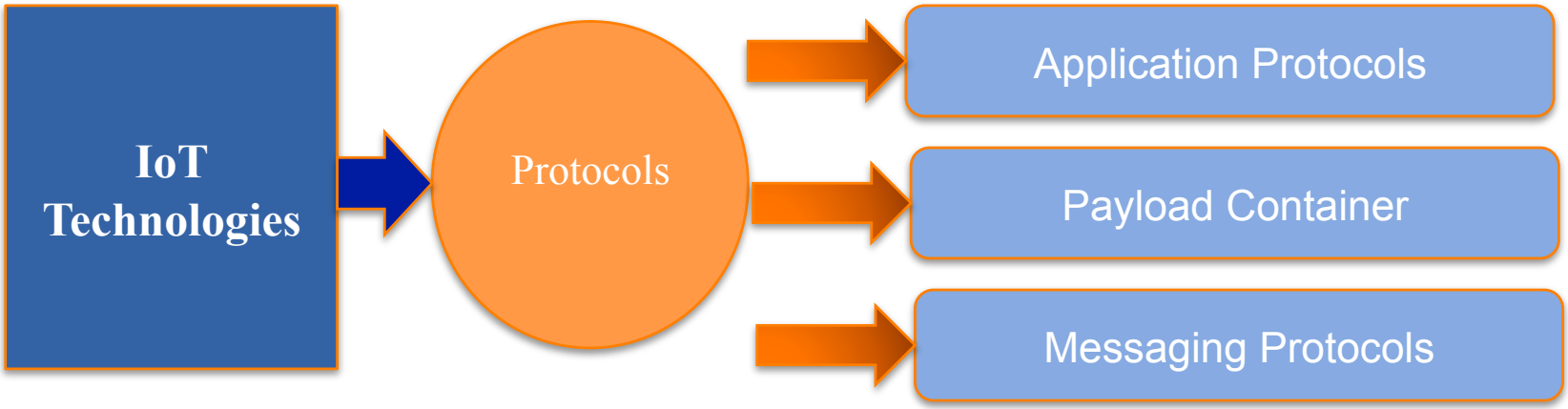
- *"Interoperability, resilience and reliability communication are the key challenges that need to be overcome in order to enable IoT." Some of existing wireless technology can be used in IoT.*
  - WiMAX and IEEE 802.16 are for PHY/MAC and the communication range is 30 km.
  - IEEE 802.15.4 is for PHY/MAC and the communication range is 1 km.
  - IETF 6LoWPAN is basically in network layer and it has the 10m communication range.
  - ZigBee is for network and upper layer, it has the communication range from 10 to 100 m.



	WiMAX/IEEE 802.16	IEEE 802.15.4	IETF 6LoWPAN	ZigBee
Layer	PHY/MAC	PHY/MAC	Network	Network and upper layers
Range	30Km	1Km	-	(see 8021.5.4)
Application	Wide Area/Industrial Automation	(see ZigBee)	Automation/Factory Environment	Monitor/Control
Power Consumption	Medium/High	Low	Low	Low

PROTOCOLS

- *"To ensure the inter-operability between different devices in IoT, the protocols for communication, data exchange and messages, are important. Three protocols are discussed below: application protocols, payload container protocols and messaging protocols.*
  - Application protocols is used to establish device-to-device data exchange. RTPS (real-time Publish-Subscribe) is a good candidate.
  - Payload container defines some basic message type and length. Simple Object Access Protocol (SOAP) and Constrained Application Protocol (CoAP) are the two well known candidates.
  - Messaging protocols defines rules and formats for exchanging message between devices in IoT. Some existing messaging protocols can be considered in IoT such as, Advanced Message Queuing Protocol (AMQP), Message Queuing Telemetry Transport (MQTT), eXtensible Messaging and Presence Protocol (XMPP) and Java Message Service (JSM).



PROTOCOLS: MESSAGING PROTOCOLS

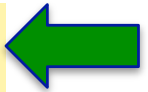
- AMQP is open standard application layer protocol for message-oriented middleware, that provides flow controlled communication with message-delivery and topic-based publish-and-subscribe messaging.
- MQTT, an OASIS standard, is an open and lightweight protocol for M2M telemetry data communication.
- XMPP, formalized by IETF, is an open XML-based protocol for near-real-time messaging.
- JSM is a part of the Java Platform Enterprise Edition, widely used for messaging technologies. It allows applications components to create, send, receive and read messages.

	AMQP	**MQTT**	**XMPP**	**JMS**
Abstraction	Pub/Sub	Pub/Sub	Pub/Sub	Pub/Sub
Architecture Style	P2P/Brokered	Brokered	P2P/Brokered	Brokered
QoS	Yes	Yes	Yes	Yes
Interoperability	Yes	Partial	Yes	No
Real-time	No	No	Near real-time	No
Transport	TCP	TCP	TCP	Not specified, typically TCP
Standard	OASIS AMQP	Proposed OASIS standard	IETF	JCP JMS standard
Licensing	Open Source and Commercially Licensed	Open Source and Commercially Licensed	Open Source and Commercially Licensed	Open Source and Commercially Licensed
Mobile Support	Yes	Yes	Yes	Dependent of the Java capabilities of the OS
Security	SASL authentication, TLS for data encryption	Simple Username/Password Authentication, SSL for data encryption	SASL authentication, TLS for data encryption	Vendor specific but typically based on SSL or TLS. Commonly used with JAAS API

Presentation Plan

① Introduction

② State of the art: Technologies in IoT

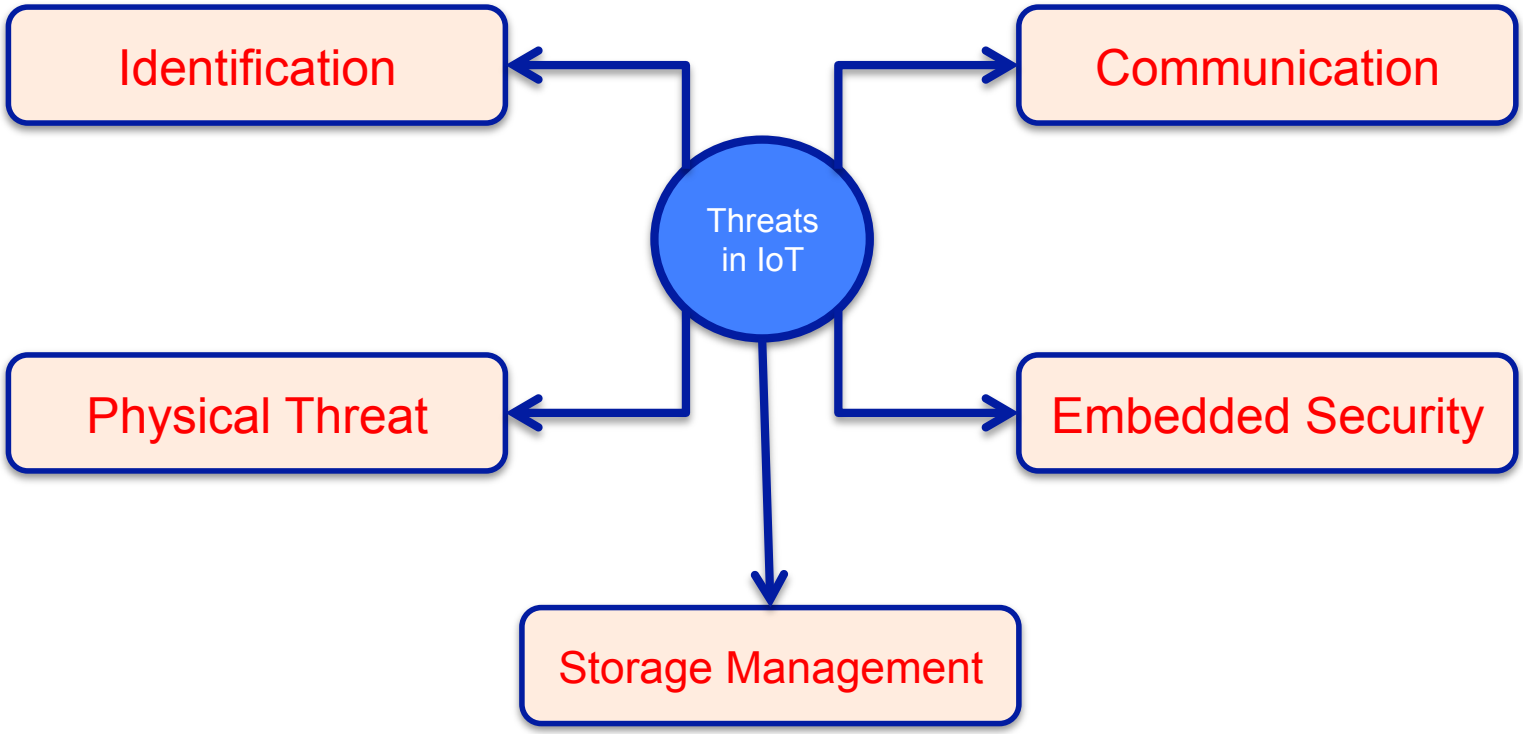
③ Risks and treats in IoT 

④ Privacy and Data Protection Issues

⑤ Conclusion and Perspectives

RISKS AND THREATS IN IOT

- *"IoT opens a new window for broader connection of smart devices, however, it also faces a new security threats and risks. IoT security is a primary management issue, which requires an effective and thorough assessment." Below are the different type of threats in IoT.*



RISKS AND THREATS IN IOT: IDENTIFICATION

- *"Identification covers determination of unique device/user/session with authentication, authorization, accounting and provisioning."*