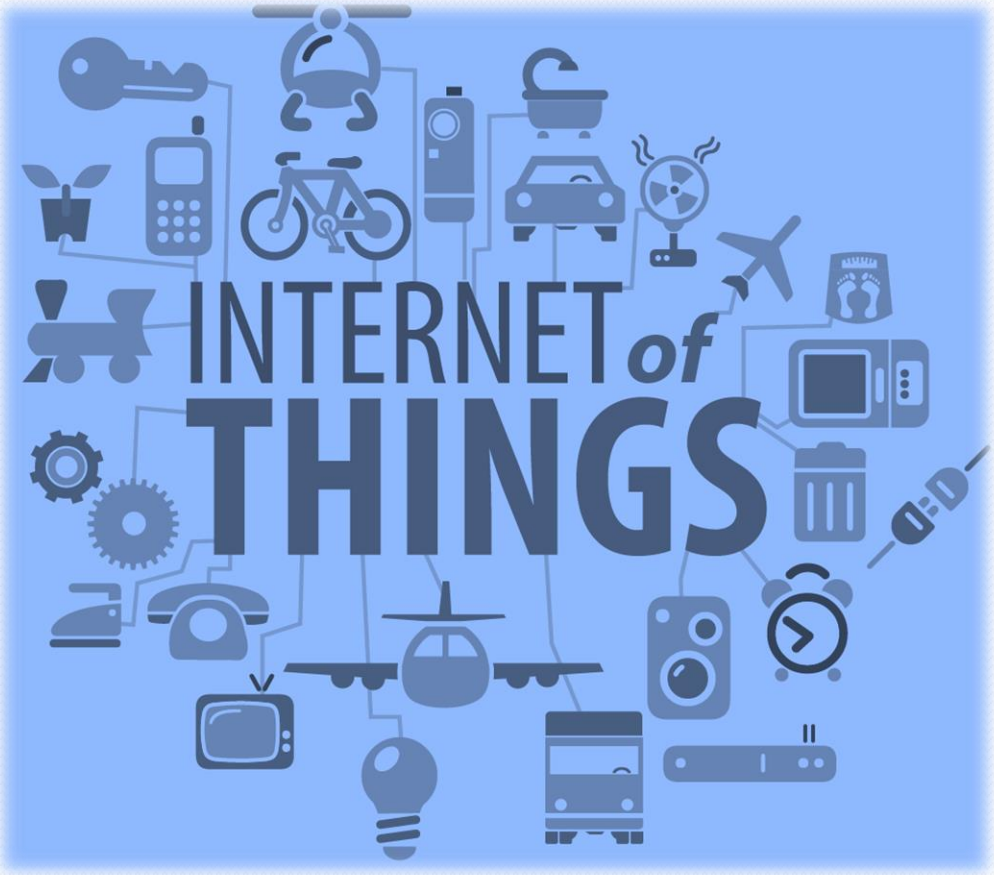
Internet of Things (IoT)

Fatih ABUT

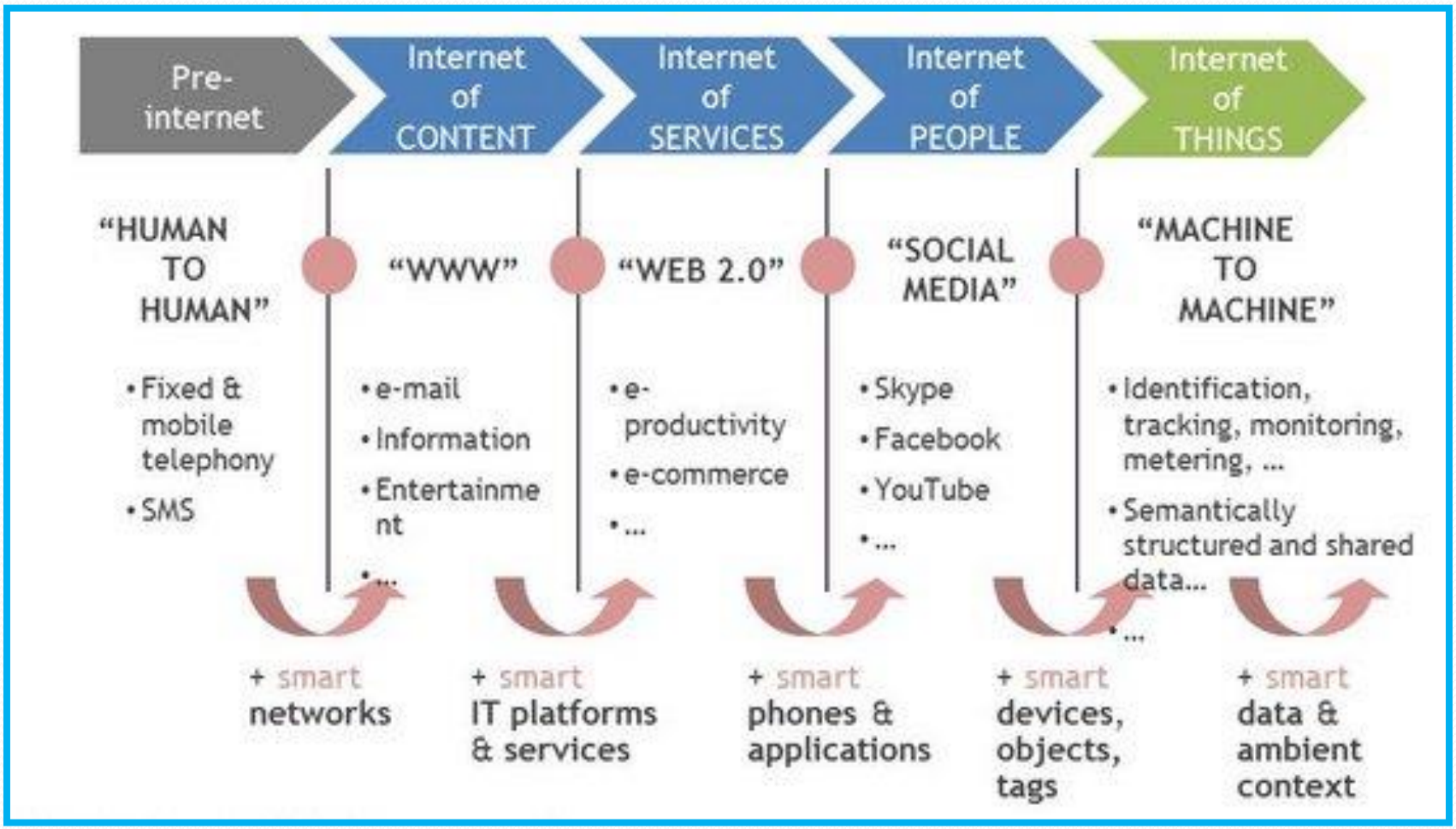
Department of Computer Engineering
Çukurova University, Adana, TURKEY

December 2020

What is IoT?



Evolution of IoT

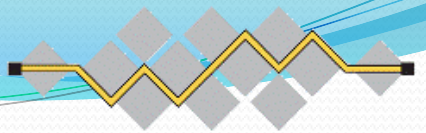


IoT is…. (According to EU)

- A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities

IoT is…. (According to ITU)

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 [ITU-T Y.2060]



IoT is…. (According to IETF)

IoT is a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols

IoT is…. (According to IEEE)

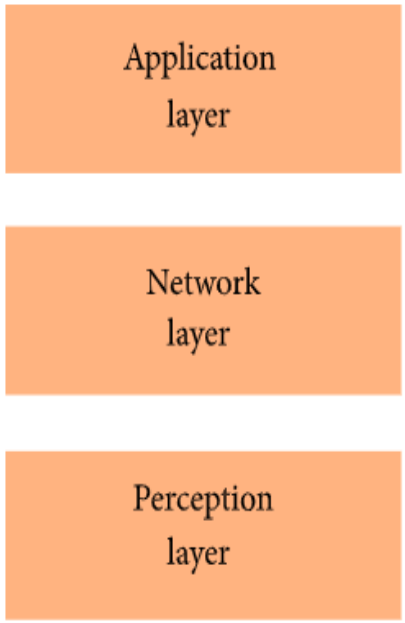
A network of items each embedded with sensors which are connected to the Internet.

IoT is…. (According to Wikipedia)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

Architecture of IOT

- The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
- The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
- The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed.

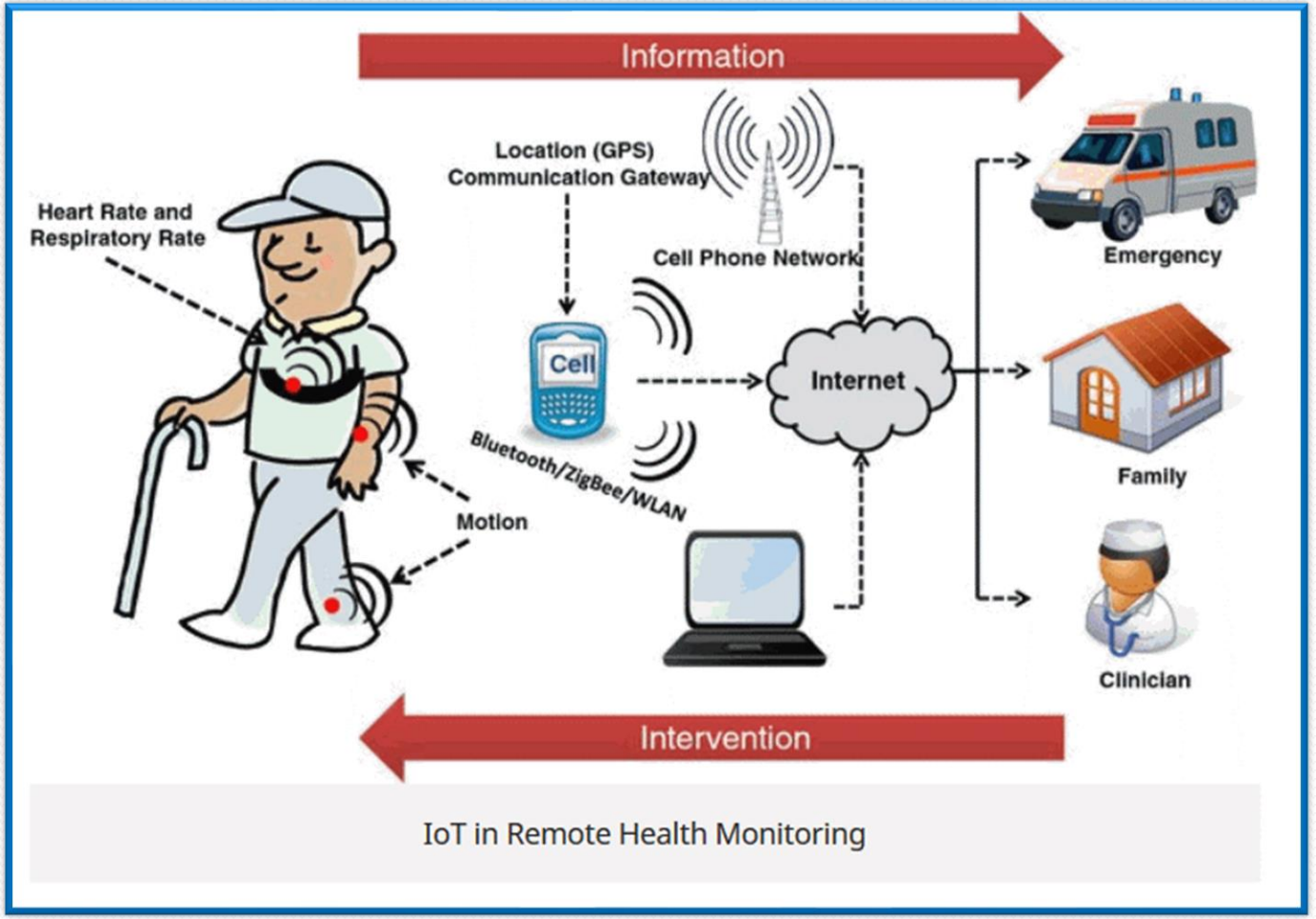


The application layer is responsible for data formatting and presentation. The application layer in the Internet is typically based on HTTP. However, HTTP is not suitable in resource constrained environments. Many alternate protocols have been developed for IoT environments such as CoAP (Constrained Application Protocol) and MQTT (Message Queue Telemetry Transport).

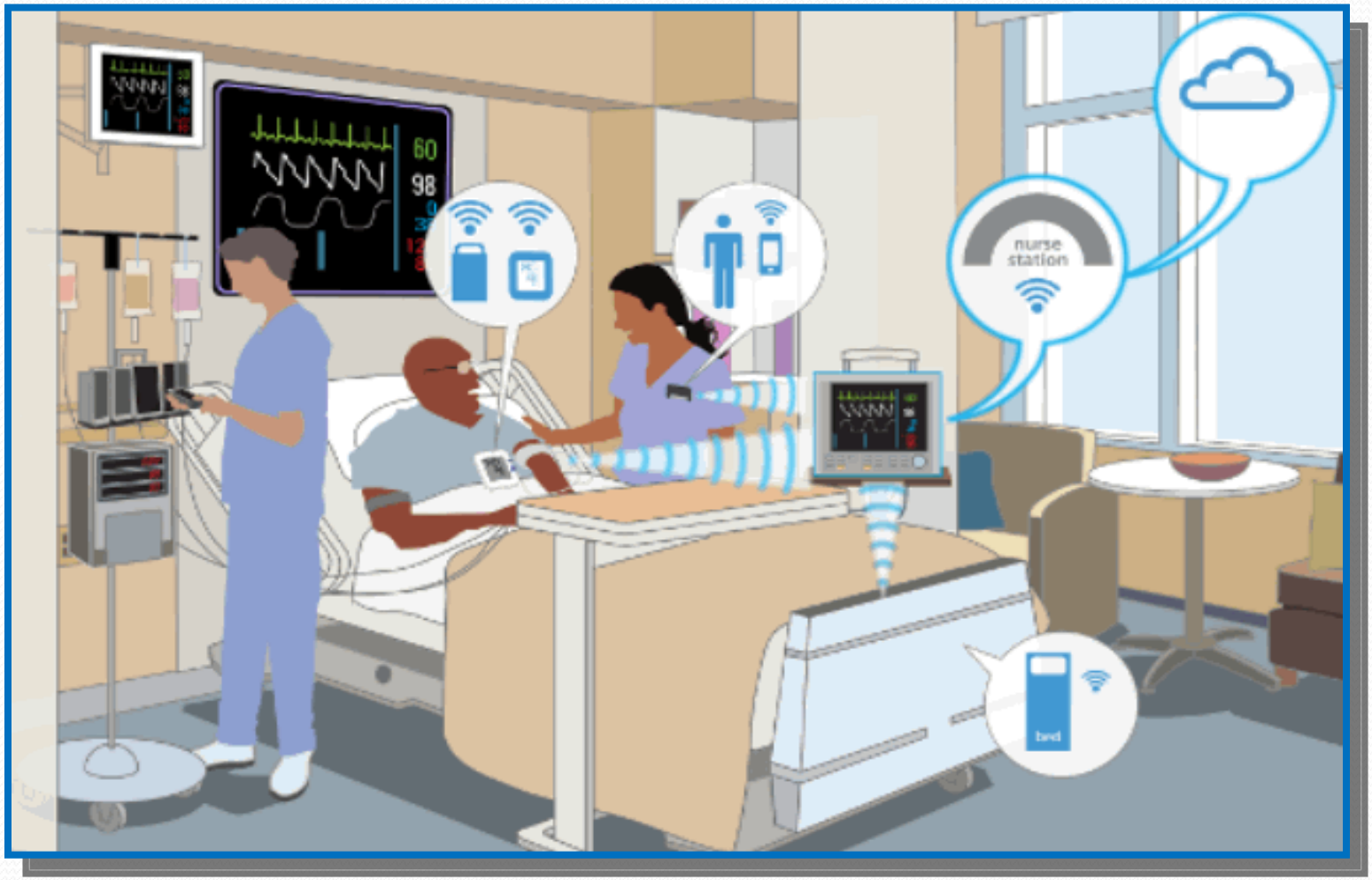
Examples of IoT Applications

- The IoT is bringing about new generation of applications such as smart
  - factories, cities, and homes,
  - grids and power plants,
  - automotive and transportation,
  - aerospace and aviation,
  - healthcare,
  - education and
  - agriculture, to name just a few.

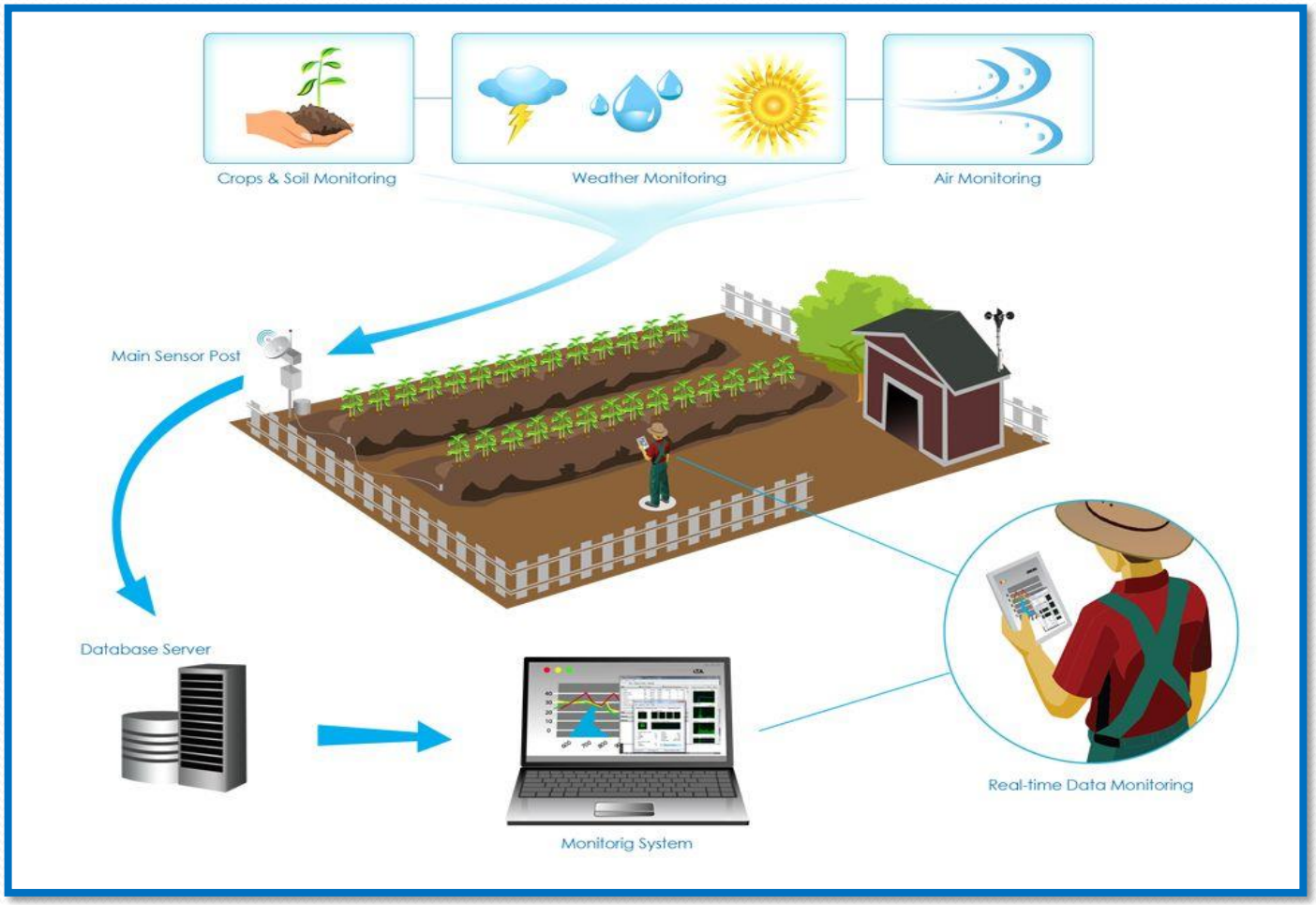
IoT in Health



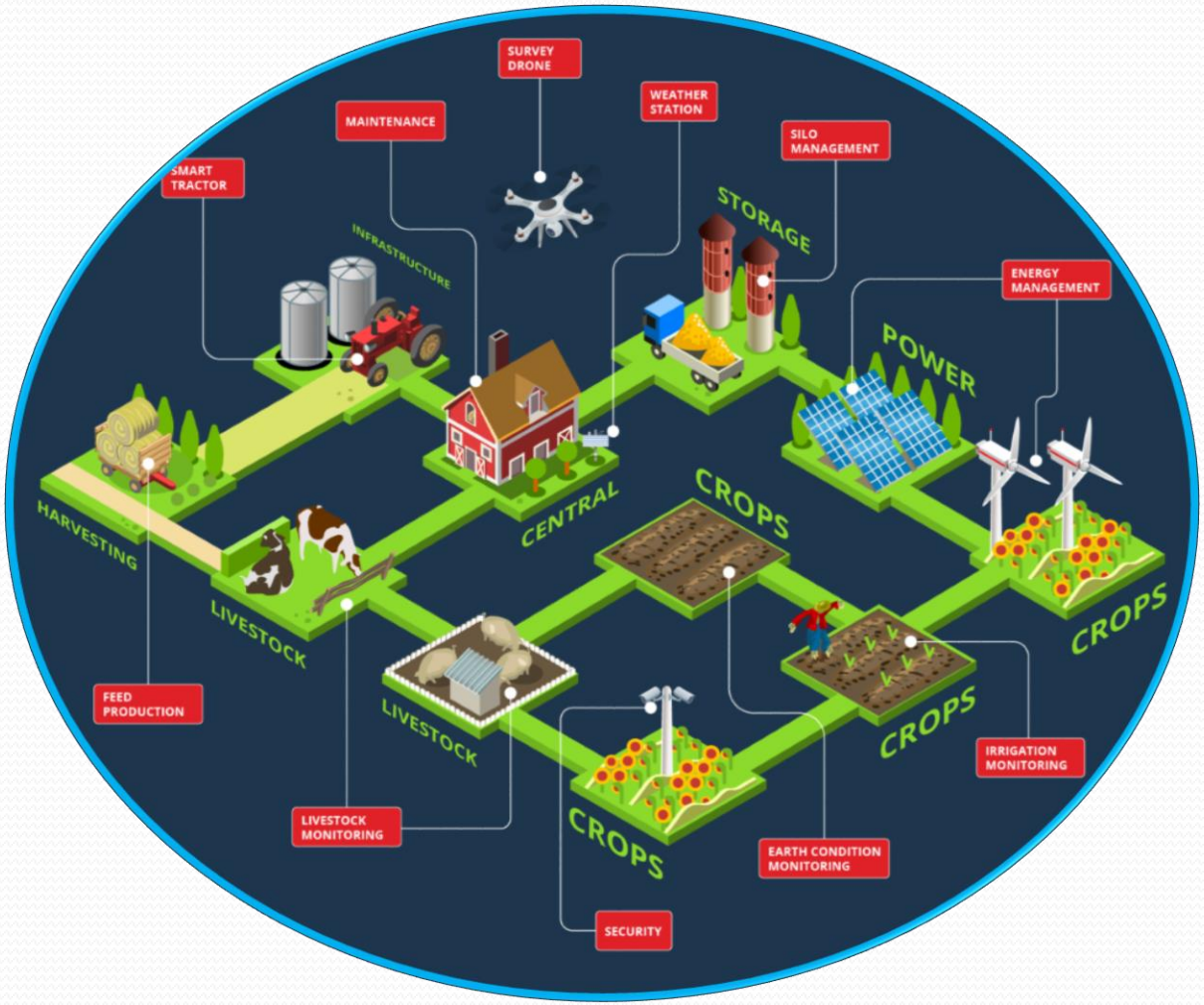
IoT in Health



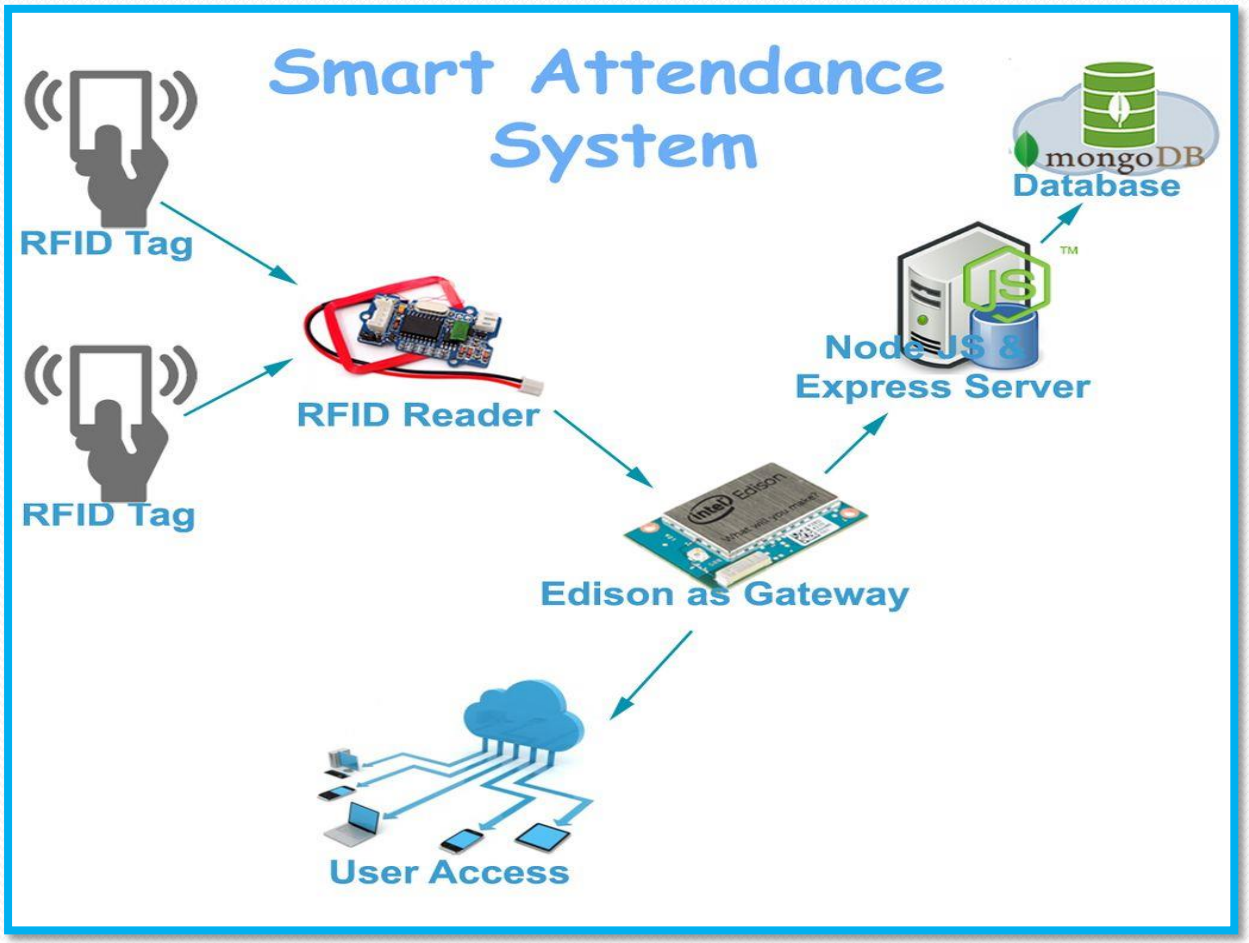
IoT in Agriculture



IoT in Agriculture



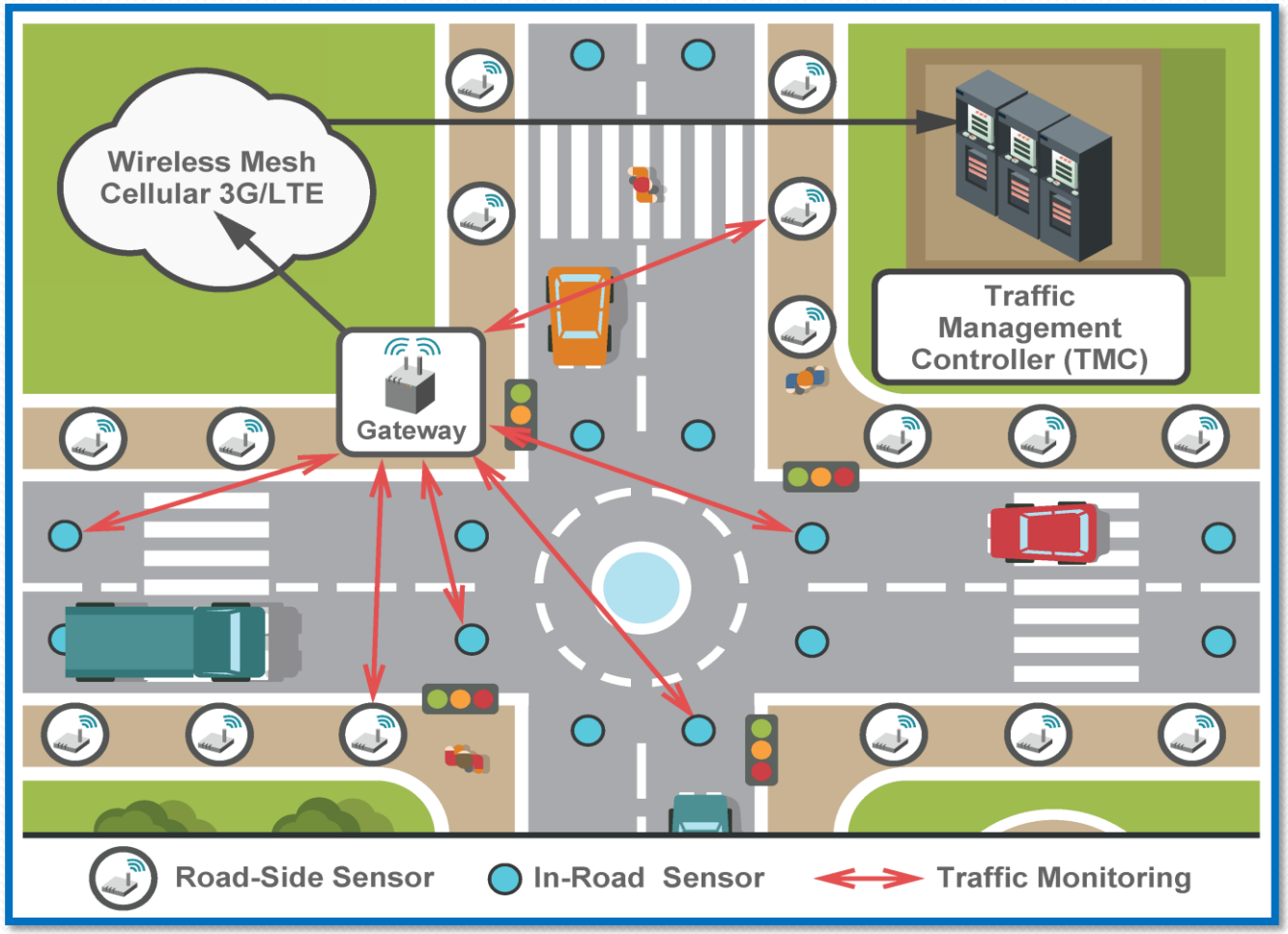
IoT in Education



IoT in Education

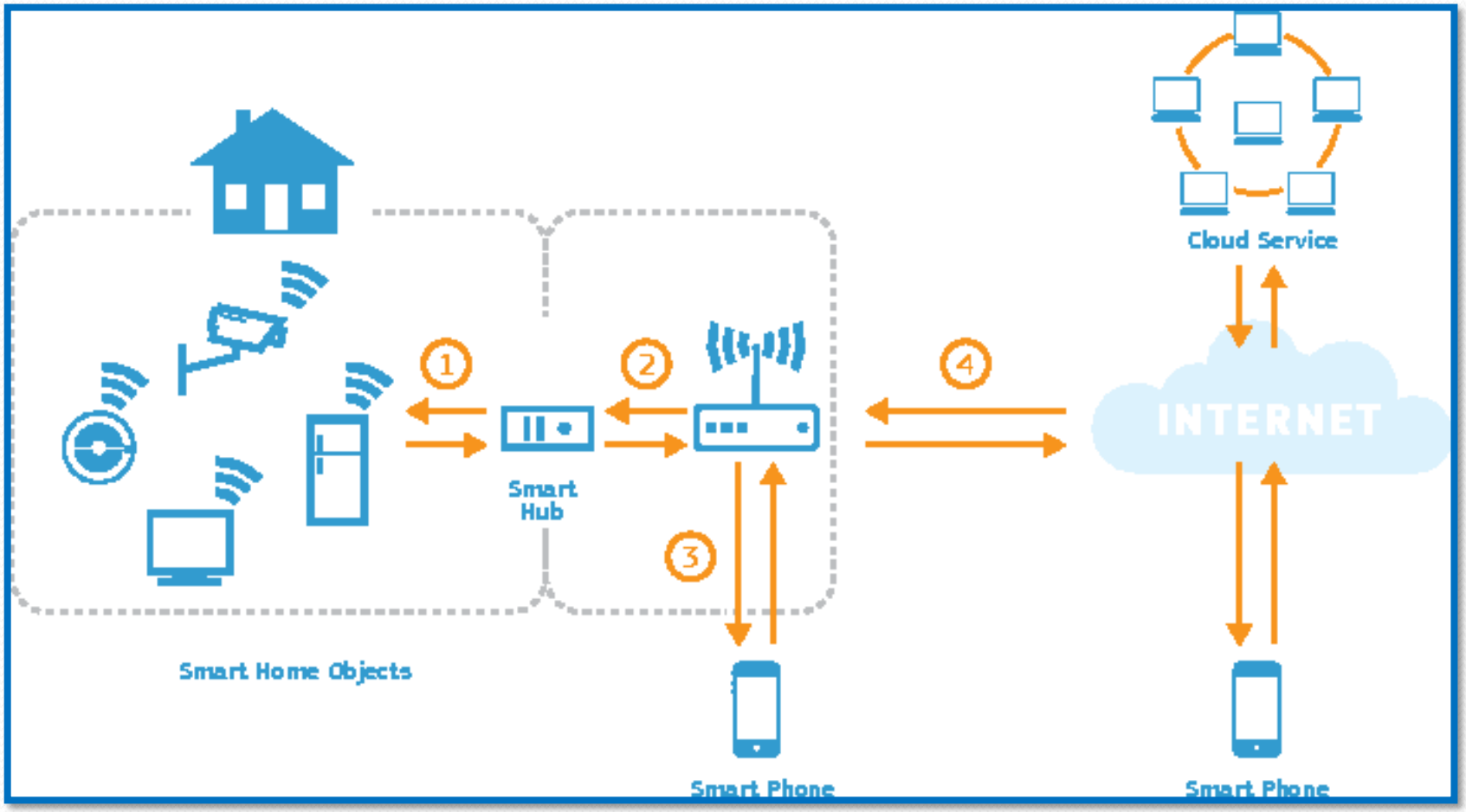
IoT in Traffic

IoT in Traffic



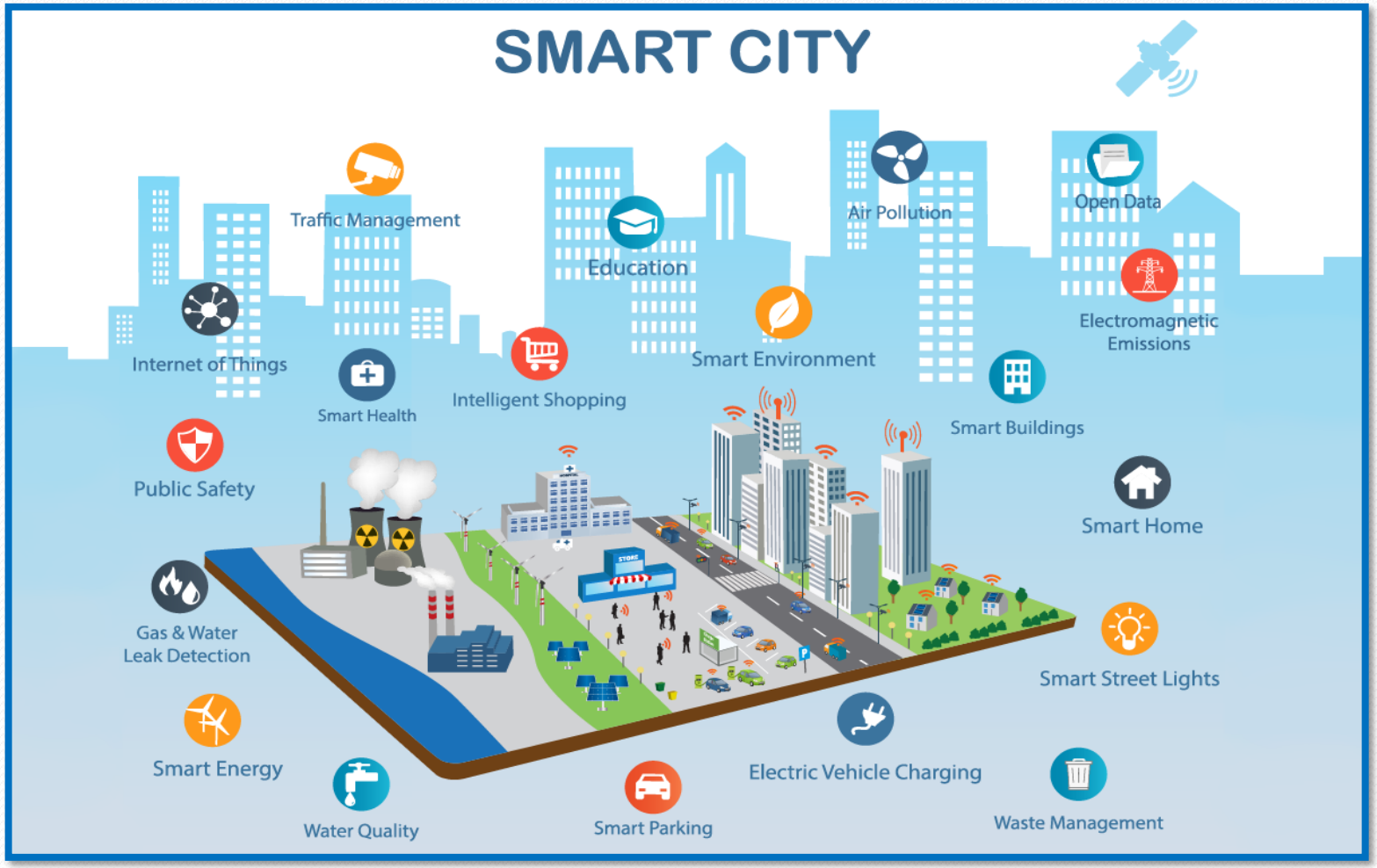
IoT in Smart Home

IoT in Smart Home

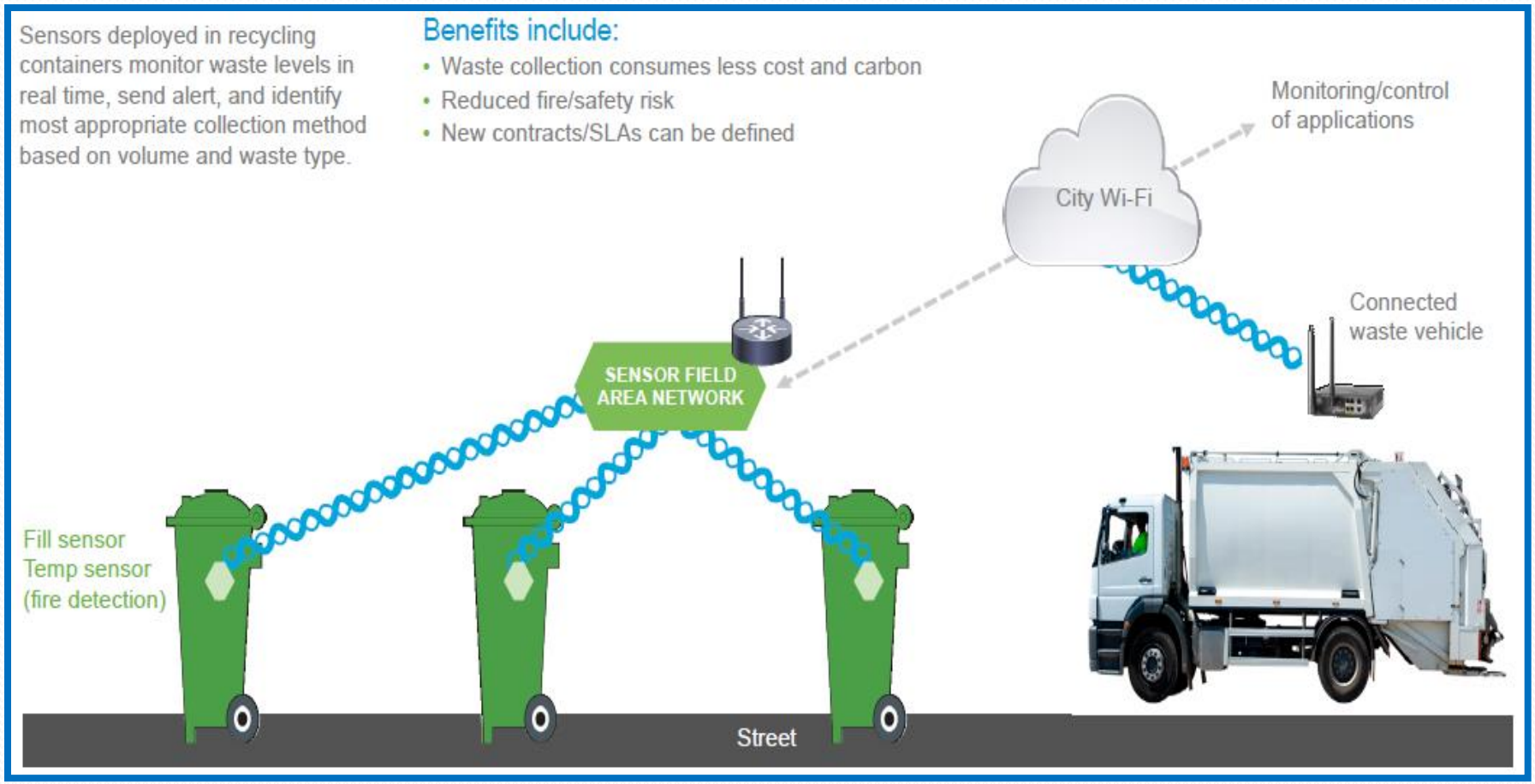


IoT in Retails

IoT in Smart Cities



IoT Based Waste Collection

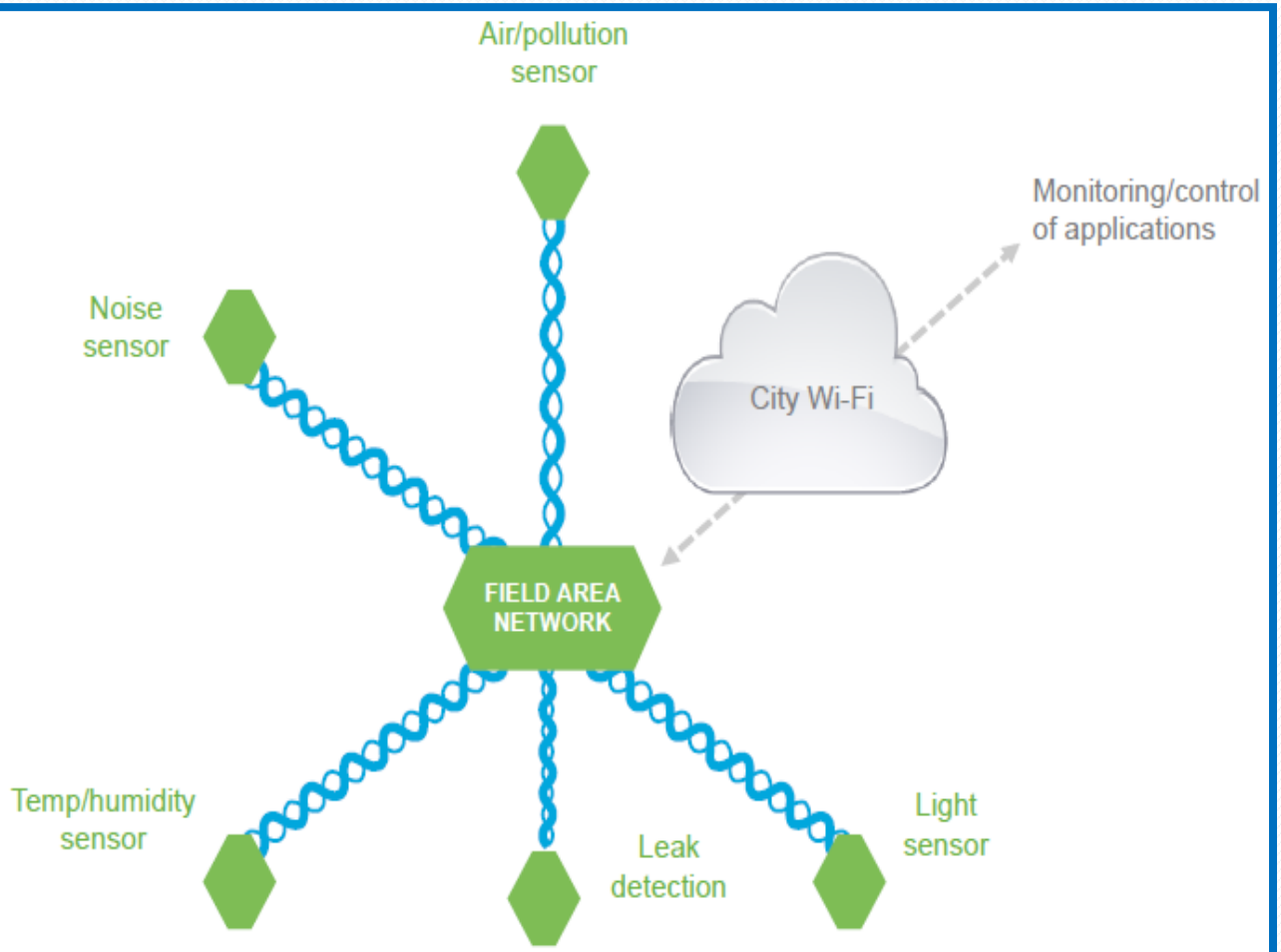


IoT Based Pollution Control

Installation of environment sensors:
air, light, humidity, noise, etc.

Benefits include:

- Leverages parking sensor infrastructure
- Provides valuable data for improving analytics applications and forecasting



IoT Application Layer Protocols

- Due to **constrained**
  - energy,
  - computation,
  - memory,
  - hardware resources, and
  - communication capacities

of these physical IoT devices, **a new generation of protocols and algorithms** are being developed and standardized -> CoAP with default CoAP CC and CoCoA

Why Not HTTP?

- Because HTTP requires connection as it runs on TCP, and HTTP is document centric.

- But in IOT all we want to send is small data, not documents, so HTTP generates a problem which is low data rate and high energy consumption (3-step handshake), while CoAP is a connectionless as it runs on UDP, and it is meant for M2M communication by design.

CoAP (RFC7252)

- The Constrained Application Protocol (CoAP) has been designed by the Internet Engineering Task Force (IETF) for the needs of IoT application layer communication.
- The CoAP is a specialized web transfer protocol for use with these constrained physical devices.
- There are various types of CoAP Messages
  - Confirmable Message (CON)
  - Non-confirmable Message (NCON)
  - Acknowledgement Message (ACK)
  - Reset Message (RST)

Some CoAP Message Types

- Confirmable Message (CON)
  - Some messages require an acknowledgement. These messages are called "Confirmable". When no packets are lost, each Confirmable message elicits exactly one return message of type Acknowledgement or type Reset.
- Non-confirmable Message (NCON)
  - Some other messages do not require an acknowledgement.
- Acknowledgement Message (ACK)
  - An Acknowledgement message acknowledges that a specific Confirmable message arrived.

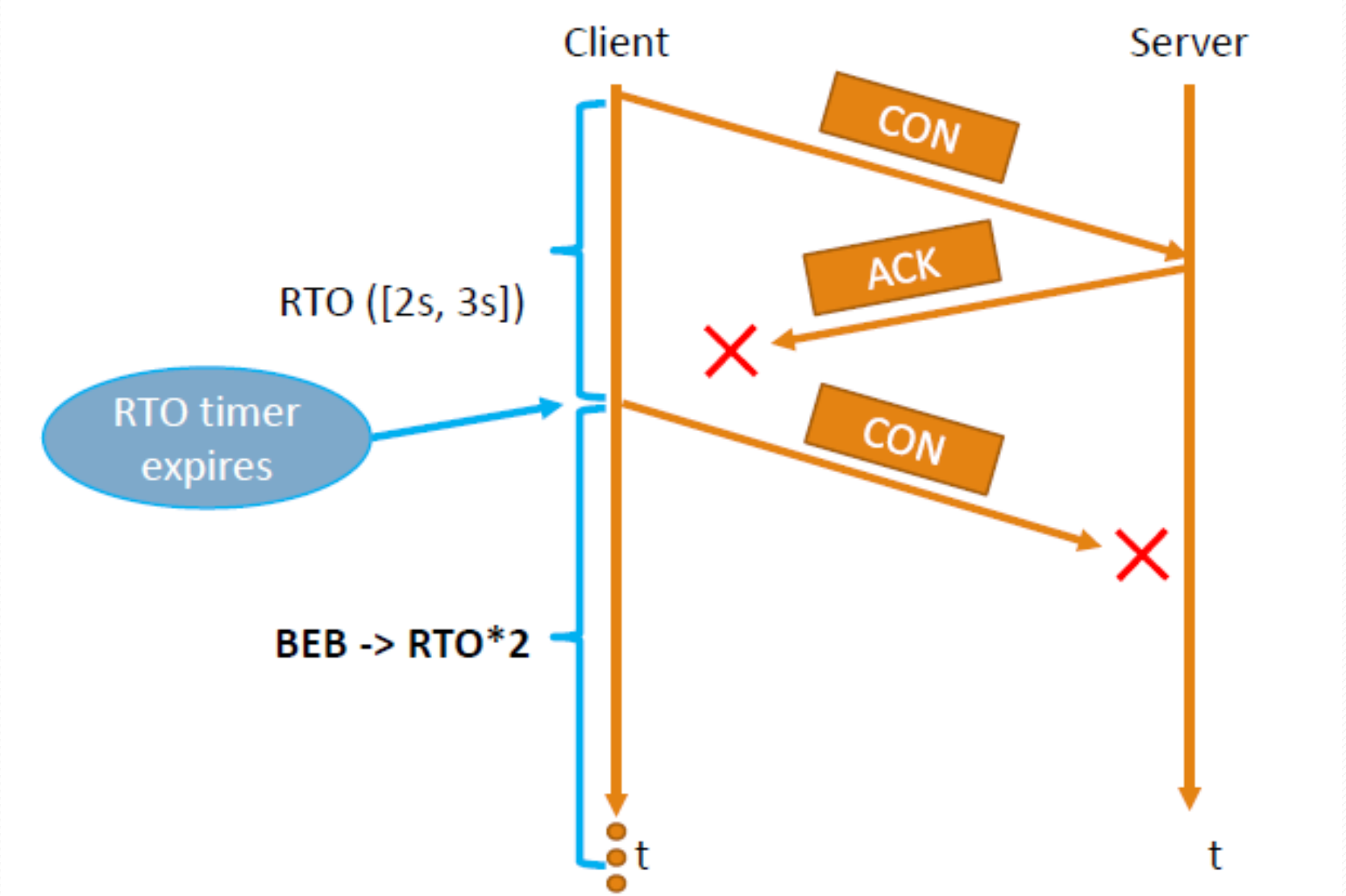
Congestion in IoT networks

- CoAP is based **on UDP** to better fit the requirements of constrained physical devices.
  - UDP is a very simple and light-weight transport layer protocol that does not handle congestion within the network.

- The phenomenon of congestion in IoT networks is also a major problem.
  - When the queuing and storing capacities of physical devices forming the IoT network are exceeded or generated traffic within IoT network gets close to the network capacity, network congestion is inevitably observed.
  - Typical effect of network congestion results with queuing delay and packet loss.
  - Congestion decreases the network utilization. This is known as congestive collapse.
  - Congestion control and avoidance (CCA) mechanisms are required to avoid congestive collapse.

Default CoAP Congestion Control (CC)

- Thus, the core CoAP specification offers a basic conservative default CoAP congestion control (CC) mechanism based on retransmission timeout (RTO) with binary exponential backoff (BEB).
-
- The sender retransmits the Confirmable message at exponentially increasing intervals, until it receives an acknowledgement (or Reset message) or runs out of attempts. [RFC7252]


Client
Server
CON
ACK
RTO ([2s, 3s])
RTO timer expires
CON
BEB -> RTO*2
t
t

Default CoAP CC

- **CONSERVATIVE**
  - Default CoAP CC is insensitive to network conditions.

- THUS,
- «Further congestion control optimizations and considerations are expected in the future, …»

[RFC7252]

CoAP Congestion Control Advanced (CoCoA)

- For each destination endpoint, CoCoA maintains two RTO estimators:
  - The strong RTO estimator gathers RTT information (RTT_{strong}) by measuring only when no retransmissions occurred.
  - The weak RTO estimator, which takes RTT values from retransmitted requests (RTT_{weak}) using the time between sending the initial request and obtaining the reply.

- The following formulas apply when obtaining a new RTT measurement (RTT_{X_new}), where RTTVAR is the round-trip time variation and X stands for strong or weak accordingly:

  - $RTTVAR_X = (1-\beta) \times RTTVAR_X + \beta \times \left|RTT_X - RTT_{X\_new}\right|$

  - $RTT_X = (1-\alpha) \times RTT_X + \alpha \times RTT_{X\_new}$

    $\beta = {}^1/_8 \quad , \alpha = {}^1/_4$

  - $RTO_X = RTT_X + K_X \times RTTVAR_X$

    $K_{strong} = 4 \quad , K_{weak} = 1$

  - $RTO_{overall} = \gamma_X \times RTO_X + (1-\gamma_X) \times RTO_{overall}$

    $\gamma_{strong} = 0.5, \gamma_{weak} = 0.25$

- $RTO_{overall}$ is then used to determine the initial RTO (RTO_{init}) of CON transmission

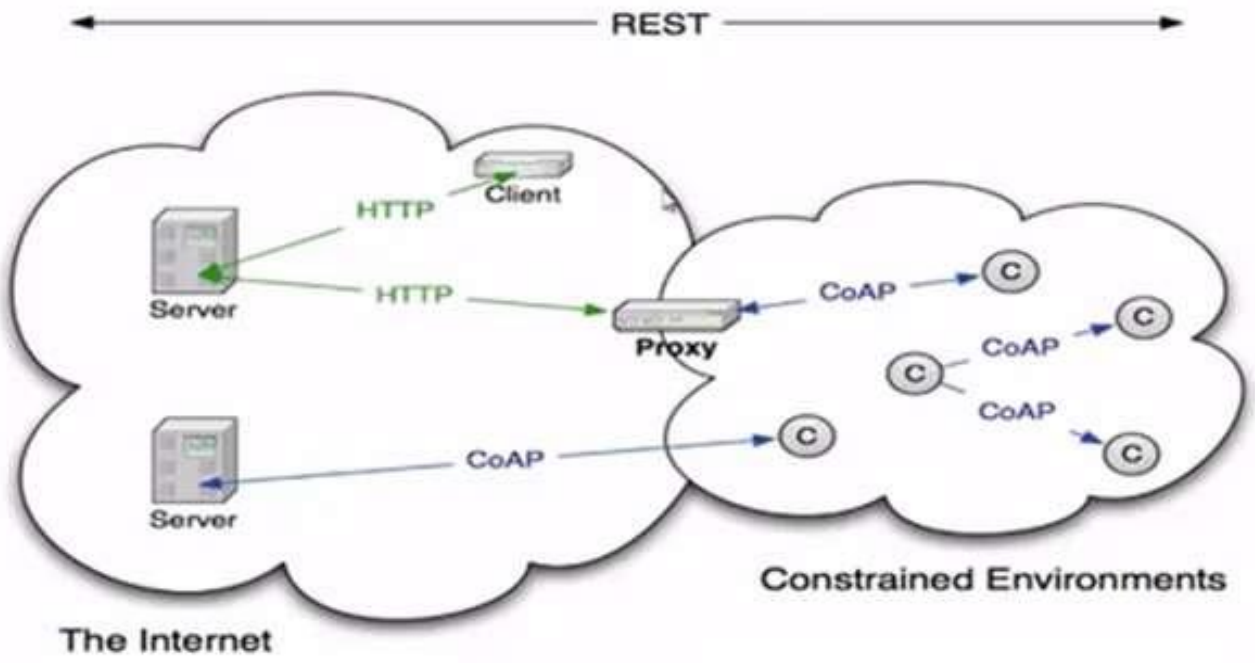
VARIABLE BACKOFF FACTOR (VBF)

- The introduction of the VBF is an important change to the backoff behavior used by default CoAP CC and CoCoA, replacing the BEB applied to retransmissions. Instead of doubling the previous RTO value ($RTO_{previous}$) to obtain the RTO applied to the next retransmission (RTO_{new}), it is multiplied by a variable factor:
  - $RTO_{new} = RTO_{previous} \times VBF$

$$VBF(RTO_{init}) = \begin{cases} 3, & RTO_{init} < 1s \\ 2, & 1s \leq RTO_{init} \leq 3s \\ 1.5, & RTO_{init} > 3s \end{cases}$$

URI Scheme of COAP

- COAP similar to HTTP. Just like URI scheme for HTTP, COAP have URI scheme also written like coap:// .



CoAP Architecture

Some Challenges of IoT

- Privacy
- Interoperability
- Security
- Quality of Service
- Data Encryption and Key Management
- Network Issues (Traffic Congestion)