Cloud Computing (CS60118)

(Spring 2020-2021)

Communication and Networking Technologies

Dr. Sudip Misra
Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/
Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Contents

- Communication Technologies
  - IEEE 802.15.4
  - 6LoWPAN
  - RFID
  - Zigbee
  - Wireless HART
  - Bluetooth
- Networking Technologies
  - MQTT
  - CoAP
  - XMPP

Introduction

- The most important and commonly used communication protocols in IoTs and cloud computing are:

  --6LoWPAN, Zigbee, IEEE 802.15.4, Wireless HART, Z-Wave, ISA 100, NFC, RFID, and Bluetooth

IEEE 802.15.4

Features of IEEE 802.15.4

- IEEE 802.15.4 is the technical standard for low-rate wireless personal area networks
- Developed primarily for low-data-rate applications and extended-life low-power-consumption uses.
- IEEE 802.15.4 employs only the first two layers (PHY, MAC) in addition with the logical link control (LLC) and service-specific convergence sublayer (SSCS) to communicate with all upper layers.
- Operates in the ISM radio band.
- The goal of IEEE 802.15.4 is to render a base format to which the upper layers (layers 3 through 7) could add other protocols and features.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

Features of IEEE 802.15.4

- IEEE 802.15.4 utilizes direct sequence spread spectrum (DSSS) modulation.
- High tolerance to noise and interference and offers link reliability improvement mechanisms.
- The low-speed versions of IEEE 802.15.4 use Binary Phase Shift Keying (BPSK), whereas the high data-rate versions use offset-quadrature phase-shift keying (O-QPSK).Uses CSMA-CA for channel access.
- Multiplexing feature enables multiple devices to access the same channel without interference at different times.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

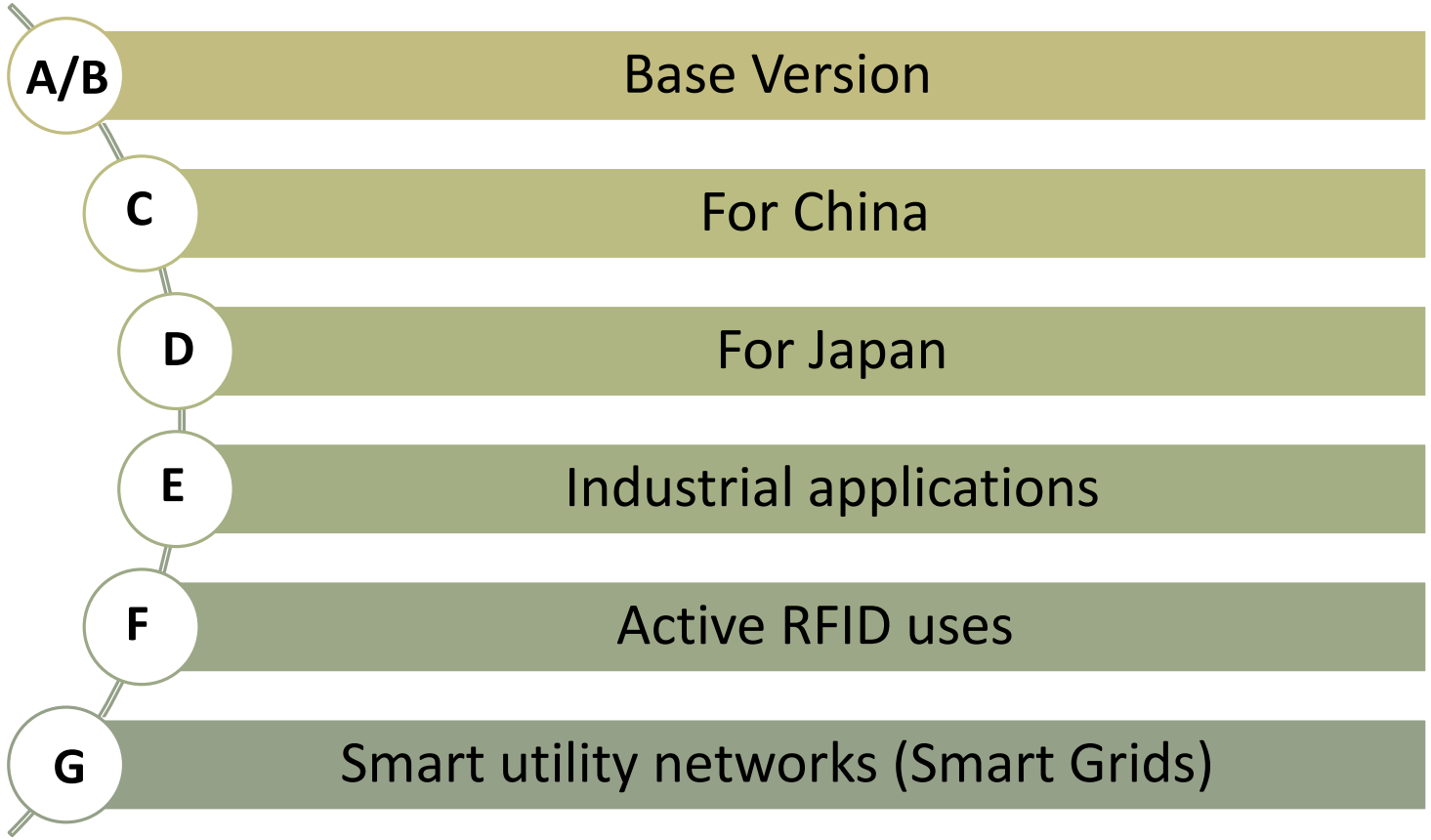
Features of IEEE 802.15.4

- Short packets are transmitted infrequently for a very low duty cycle (<1%) to minimize power consumption.
- The minimum power level defined is –3 dBm or 0.5 mW.
- Under the best conditions the transmission range can reach up to 1000 meters.
- Standard transmission range is 10 to 75 meters.
- The nature of the transmission path is mostly line of sight (LOS).
- 802.15.4 defines two topologies:
  - a basic star
  - a basic peer-to-peer (P2P)

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

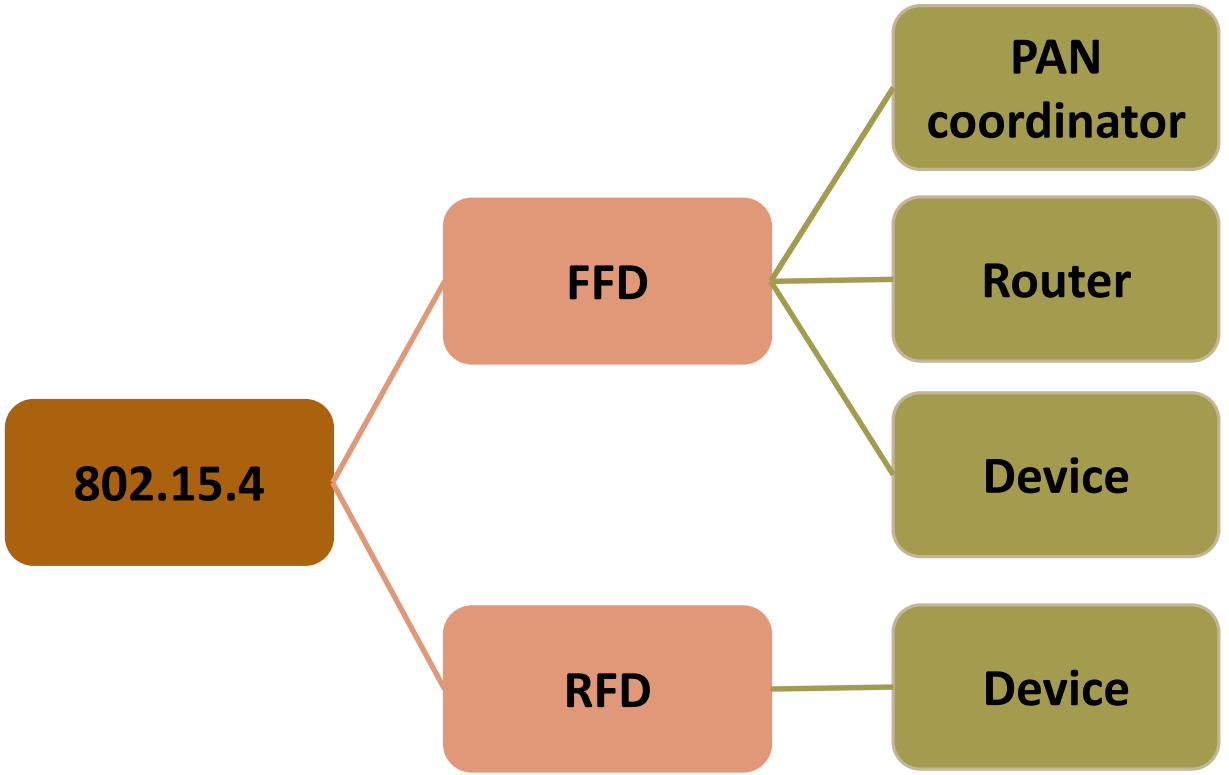
IEEE 802.15.4 Layered diagram

IEEE 802.15.4 Variants

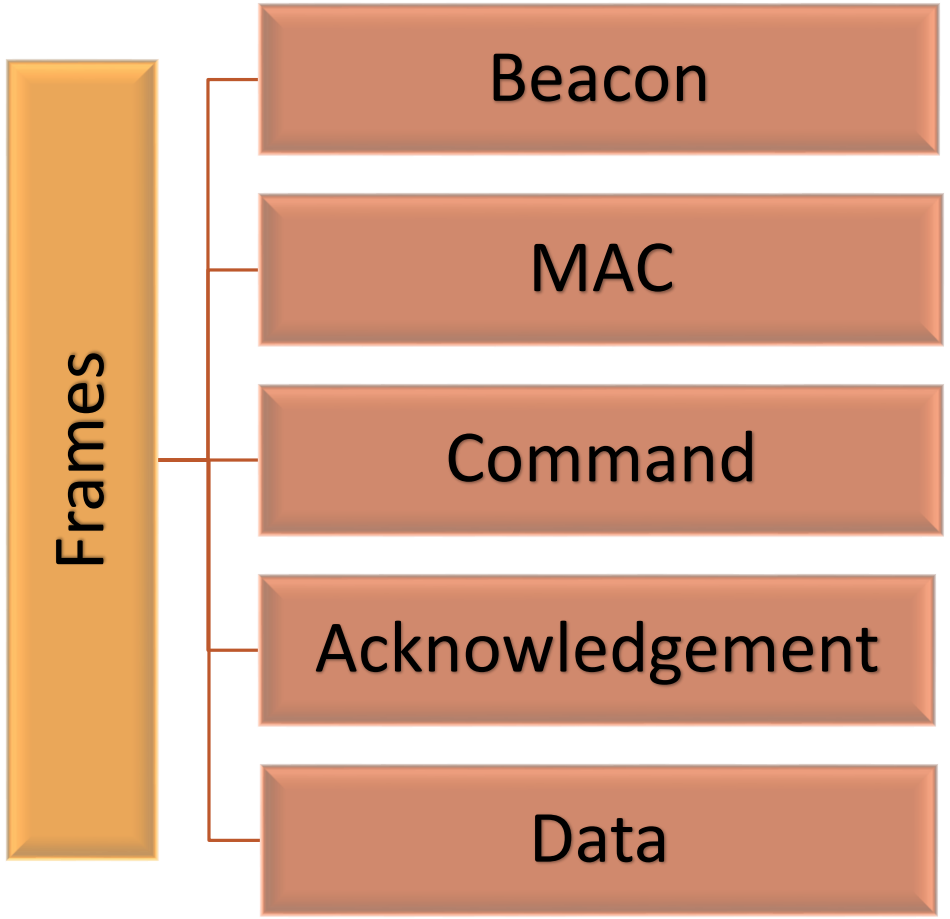


IEEE 802.15.4 Types

- Full Function Device (FFD)
  - Can communicate with all types of devices
  - Supports full protocol
- Reduced Function Device (RFD)
  - Can only communicate with an FFD
  - Reduces power consumption
  - Minimum CPU/RAM required

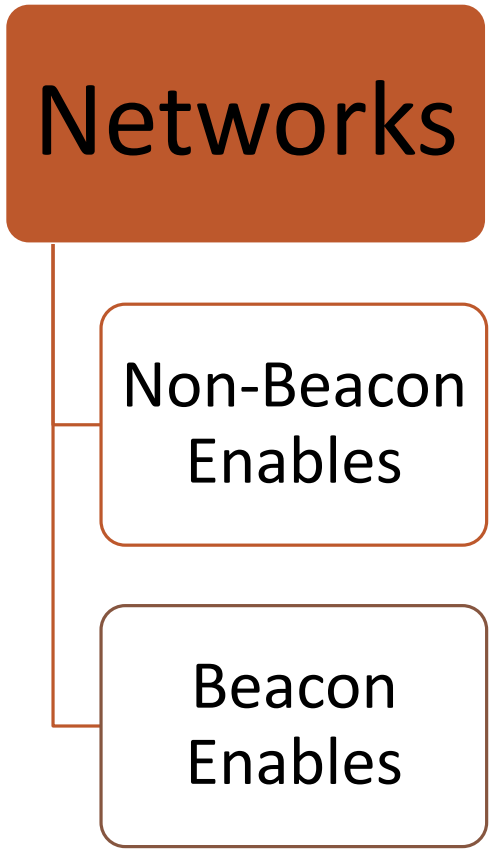


IEEE 802.15.4 Frames



Beacon Enabled Networks

- Beacon messages are transmitted periodically.
- Data-frames are transmitted through Slotted CSMA/CA with a superframe structure which the PAN coordinator manages.
- Beacons are used to synchronize & associate nodes with the coordinator.
- Operational scope crosses the whole network.



Non-Beacon Enabled Networks

- Data-frames are transmitted through un-slotted CSMA/CA (ContentionBased)
- Beacons are used for only link-layer discovery.
- Both source and destination IDs are required.
- All protocol addressing must stick to mesh configurations as IEEE 802.15.4 is primarily a mesh protocol.
- Communications amongst nodes are de-centralized.

6LoWPAN

Introduction

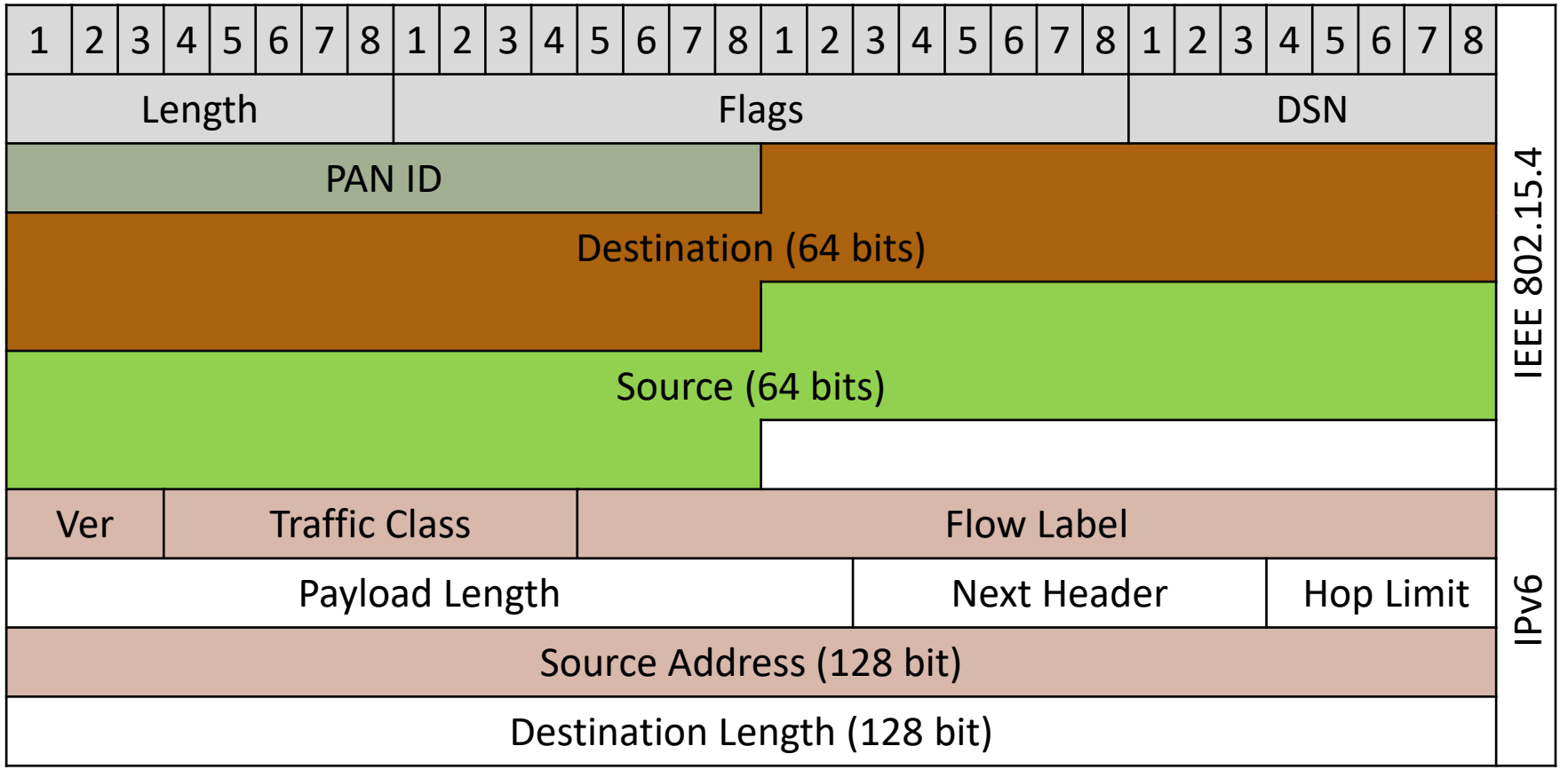
- Acronym for Low-power Wireless Personal Area Networks (LoWPAN) over IPv6.
- Especially designed for low-power devices by adopting a compressed IPv6 protocol to minimize resource consumption
- Allows small low-power devices with limited processing capability to communicate wirelessly through an Internet protocol.
- It was created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

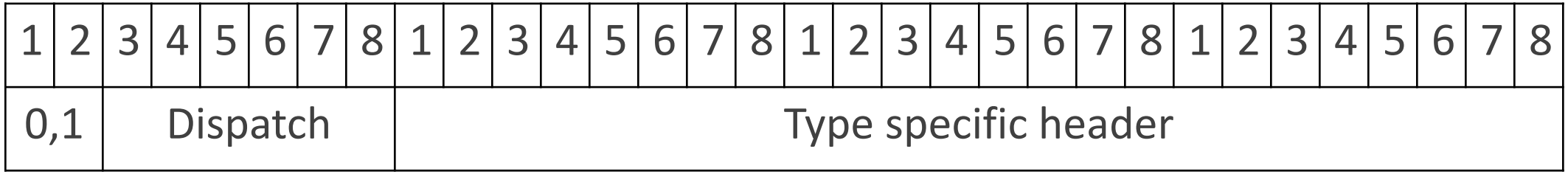
Features of 6LoWPAN

- Small packet size with low bandwidth (250/40/20 kbps) and low power (battery operated)
- Addressing:
  - 64-bit extended
  - 16-bit short addressing: unique within the PAN [IEEE802.15.4].
- Supports star and mesh topology
- Relatively low cost

6LowPAN Packet Format



Header Type: Dispatch Header



- 0,1:
  - Dispatch Type Identifier
- Dispatch:
  - 6-bit
  - Identifies the type of the subsequent header.
- Type-specific header
  - A header determined by the Dispatch Header.

Header Type: Mesh Addressing Header

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0,1		O	F	Hops Left				originator address												Final address											

- O:
  - 0 if the Originator Address is an IEEE extended 64 bit address
  - 1 if it is a short 16-bit addresses.
- F:
  - 0 if the Final Destination Address is an IEEE extended 64 bit
  - 1 if it is a short 16-bit addresses.
- Hops Left:
  - Decremented by each forwarding node before forwarding the packet to its next hop
  - The packet is not forwarded any further if Hops Left becomes 0.

Header Type: Fragmentation Header

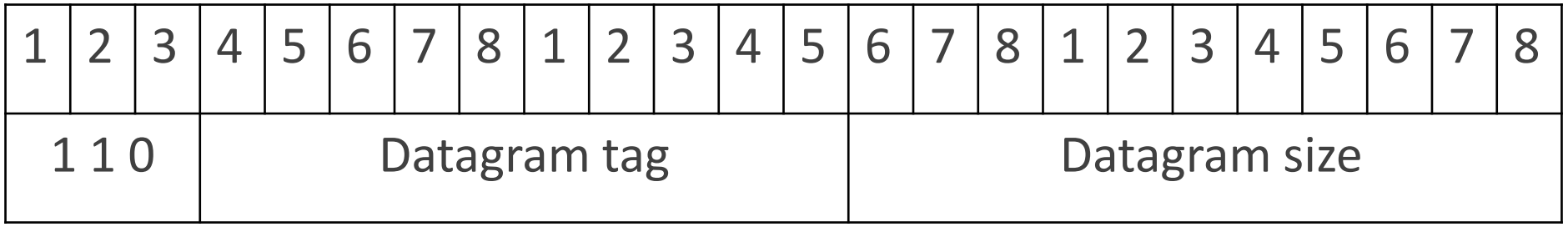


Figure: First Fragment

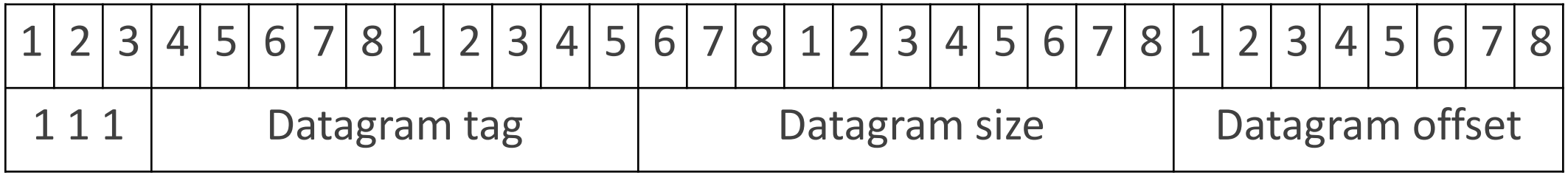


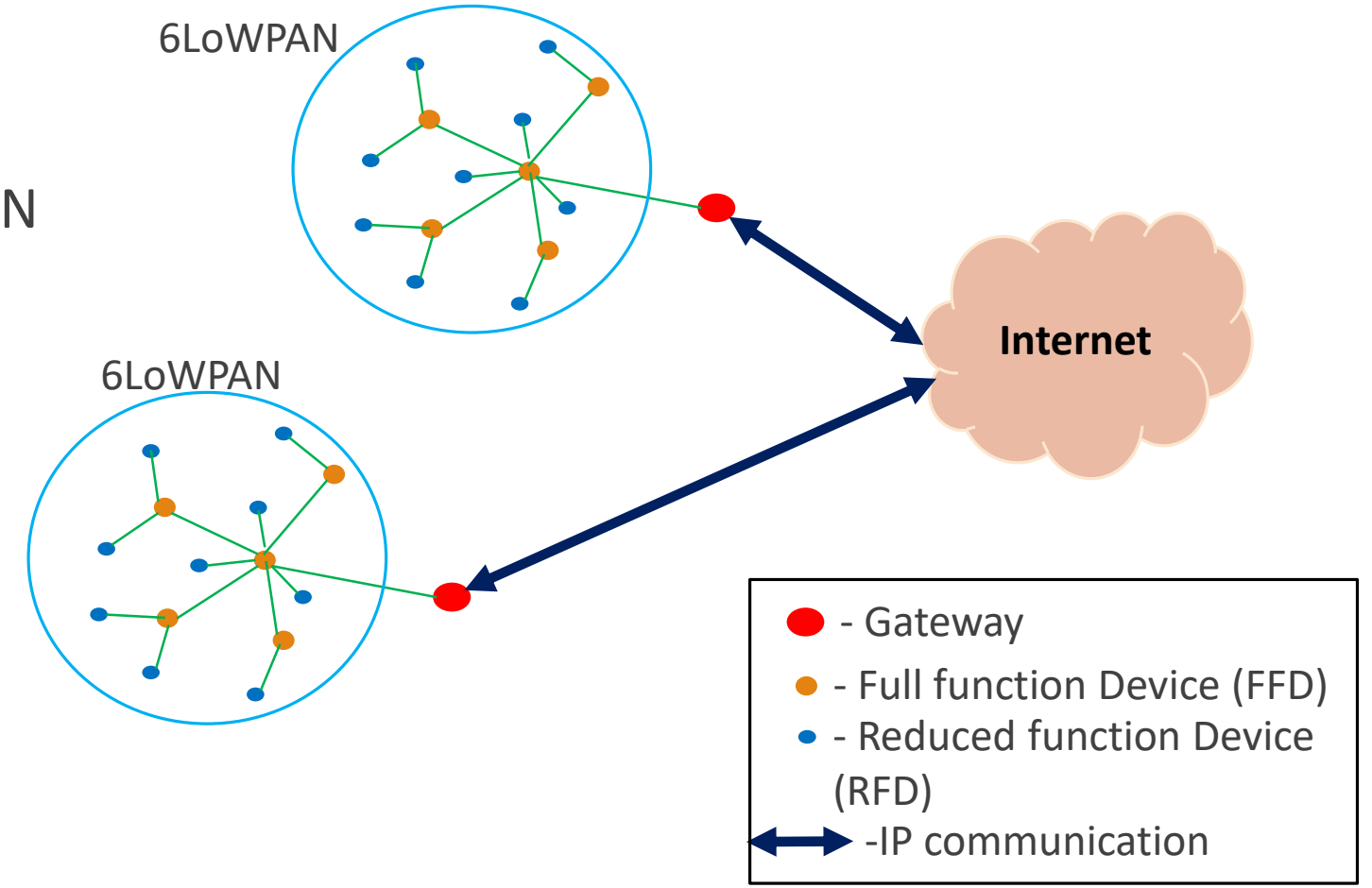
Figure: Subsequent Fragment

Header Type: Fragmentation Header

- Datagram tag:
  - Same value for all link fragments of a payload.
  - The sender increments datagram tag for successive, fragmented datagrams.
  - 10 bits long.
- Datagram size:
  - 11 bit long
  - Same value for all link fragments of an IP payload datagram.
- Datagram offset:
  - present only in the second and subsequent link fragments
  - 8 bits long.

6LoWPAN Routing

- Mesh routing within the PAN.
- Routing between IP and the PAN domain
- Routing protocols in use:
  - LOADng
  - RPL
  - HiLow



LOADng Routing

- Simplified on-demand routing protocol based on Ad-hoc On-demand Distance Vector (AODV), which is extended for use in IoT.
- Basic operations of LOADng are:
  - **Generation of Route Requests (RREQs)** by originator to discover a route to a destination
  - **Forwarding of RREQs** until they reach the destination LOADng Router
  - **Generation of Route Replies (RREPs)** after recieving RREQ from the destination to the originator

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)*. IETF. I-D draft-clausen-lln-loadng-14

LOADng Routing

- If a route is broken, a **Route Error (RERR)** message will be sent back to the originator to inform the originator about the route breakage.
- **Optimized flooding** is supported to reduce the overhead created by RREQ generation and flooding.
- Only the destination is authorized to respond to an RREQ.
- Intermediate LOADng Routers are strictly forbidden from replying to any RREQs, even if they have any active routes to the destination.
- RREQ/RREP messages created by a LOADng Router has a unique, monotonically increasing sequence number.

RPL Routing

- Routing protocol for lossy and low power networks.
- Handles routing topology employing low rate beaconing.
- Detection inconsistencies increase beaconing rate (if a node or link in a route is broken).
- The datagram itself constitutes Routing information.
- Proactive: Maintaining routing topology.
- Reactive: Resolving routing inconsistencies.
- RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

RPL Routing

- RPL supports confidentiality and integrity of a message, Data-Path Validation, and Loop Detection.
- Routing optimization objectives of RPL comprise:
  - minimizing energy
  - minimizing latency
  - satisfying constraints (w.r.t node power, bandwidth.)
- RPL operations need bidirectional links, and in some LLN cases, those links may show asymmetric nature.
- It is necessary to substantiate the reachability of a router before it is used as a parent.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

RFID

Introduction

- Radio-frequency identification
- An RFID system comprises a radio transponder, a radio receiver and a transmitter.
- Slightly similar to barcodes.
- Digitally encoded data in RFID tags can be read by a reader. The reader read data from tags and store in a database.
- Unlike barcodes and QR codes, RFID tag data can be read outside the line-of-sight

Source: "How does RFID work?" AB&R (Online)

Features RFID

- Each RFID tag comprises an integrated circuit and an antenna.
- RFID tags are often covered with a protective material to act as a shield against various environmental effects.
- Tags can be passive or active.
- Passive RFID tags are more widely used.
- Passive tags are powered by the RFID reader's interrogating radio waves before they can transmit information
- Active tags have their own power supply, and therefore, the reader can read them from hundreds of meters apart

Source: "How does RFID work?" AB&R (Online)

RFID Types

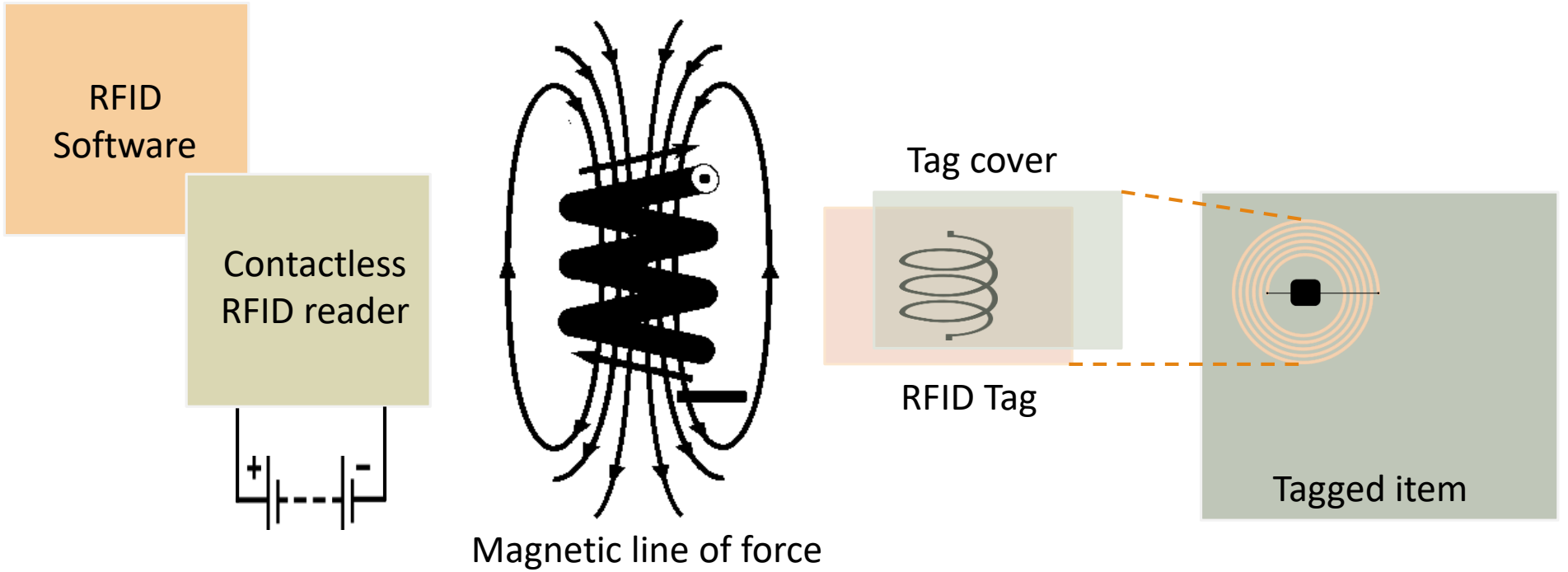
- Passive Reader Active Tag (PRAT)
- Active Reader Passive Tag (ARPT)
- Active Reader Active Tag (ARAT)

Working Principle

- Derived from Automatic Identification and Data Capture (AIDC)technology.
- AIDC is the method that automatically identifies objects, collects data about the objects, and stores them directly into computer systems with little or no human intervention.
- QR codes, bar codes, RFID, biometrics, magnetic stripes, optical character recognition (OCR), smart cards, and voice recognition are considered as part of AIDC.
- RFID uses radio waves to perform AIDC functions.
- An RFID system's main components are:-- an RFID tag or smart label, an RFID reader, and an antenna.

Source: "How does RFID work?" AB&R (Online)

Working Diagram



Applications

- Inventory management
- Asset tracking
- Controlling access to restricted areas
- Locating lost airport baggage
- Timing sporting events
- Supply chain management
- Counterfeit prevention
- Tracking of persons and animals
- Toll collection and contactless payment

Source: "How does RFID work?" AB&R (Online)