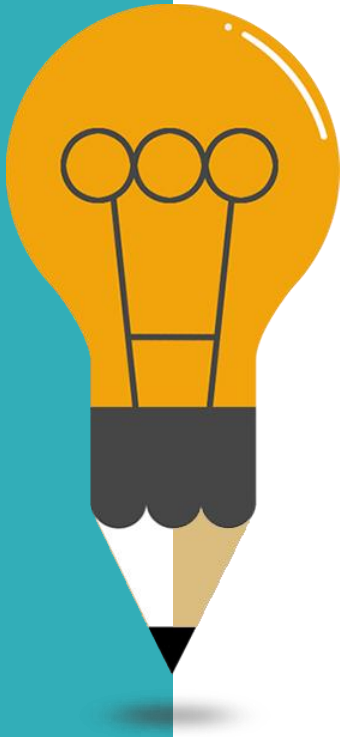
RFID: Technology and Applications

Jin Zhang

Department of Computer Science and Engineering

Southern University of Science and Technology



Outline

01 **Overview of RFID**

Reader-Tag; Potential applications

02 **RFID Technology Internals**

RF communications
Reader/Tag protocols
Middleware architecture

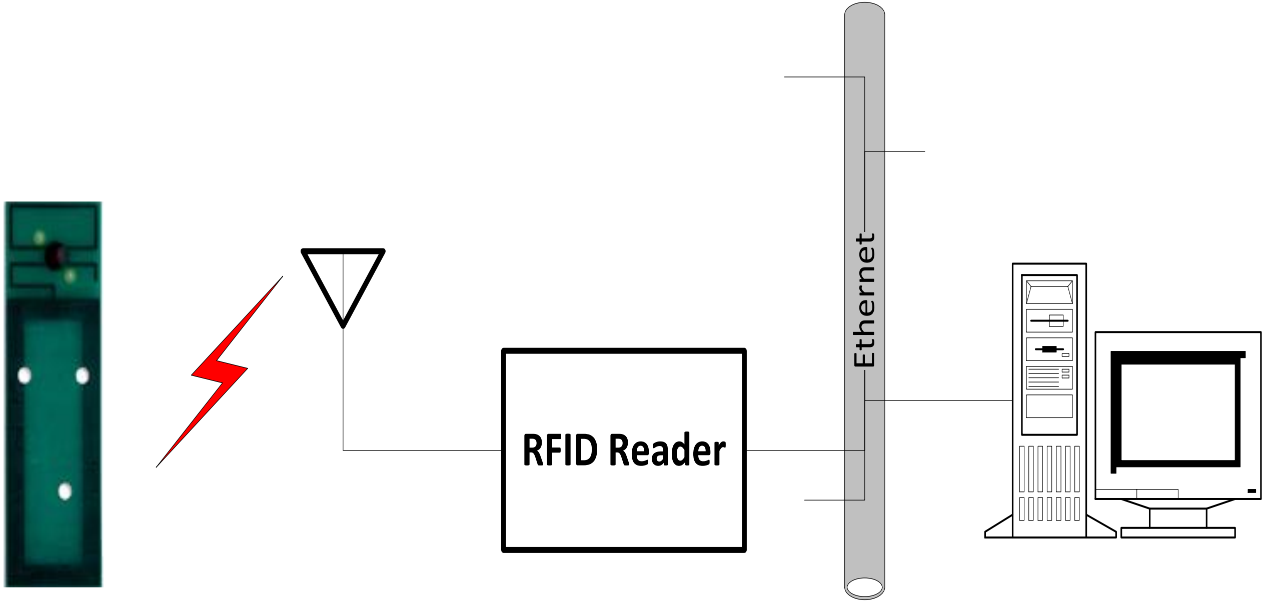
03 **Security and Privacy**

04 **Conclusion**

What is RFID?

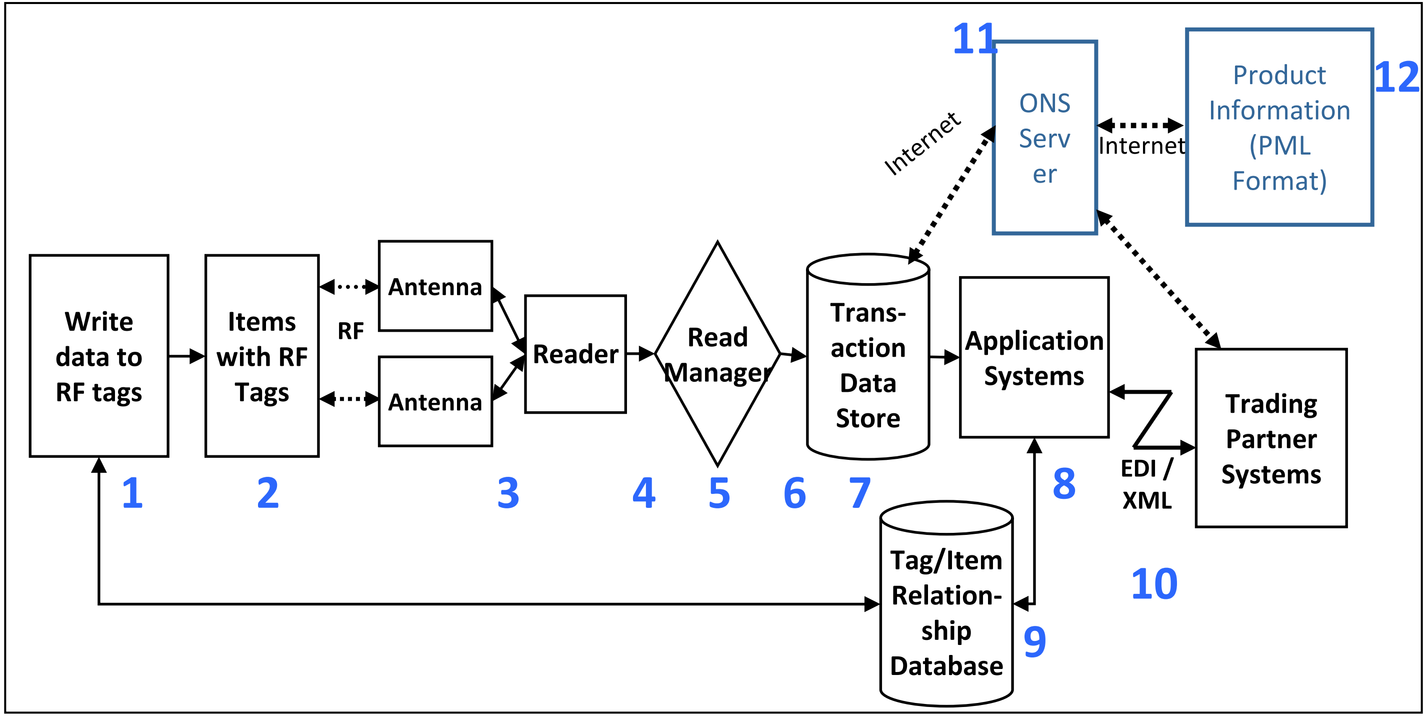
- RFID = Radio Frequency IDentification
- An ADC (Automated Data Collection) technology that:
  - Uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track
  - Is fast and does not require physical sight or contact between reader/scanner and the tagged item
  - Performs the operation using low cost components
  - Attempts to provide unique identification and backend integration that allows for wide range of applications
- Other ADC technologies: Bar codes, OCR

RFID System Components



RFID Tag RF Antenna Network Workstation

RFID Systems: Logical View

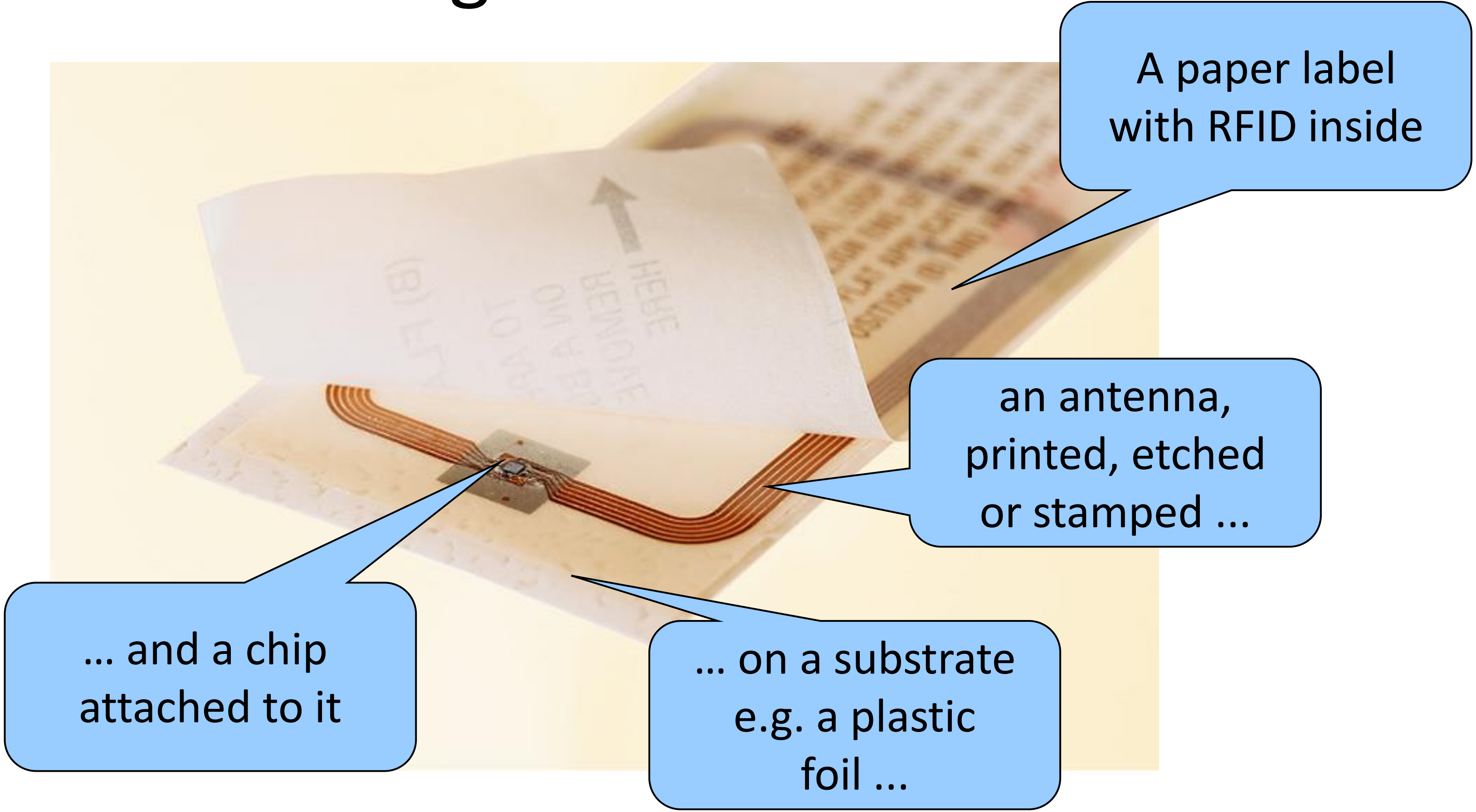


Tag Interfaces

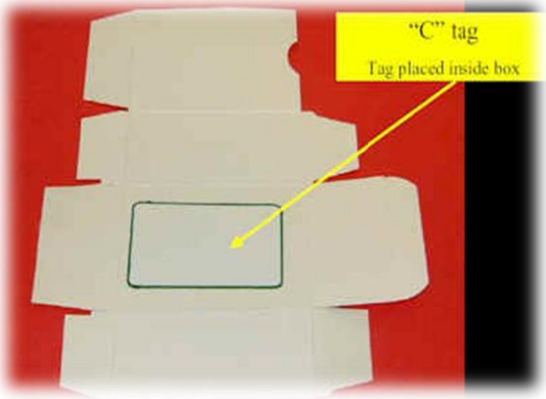
RFID Middleware

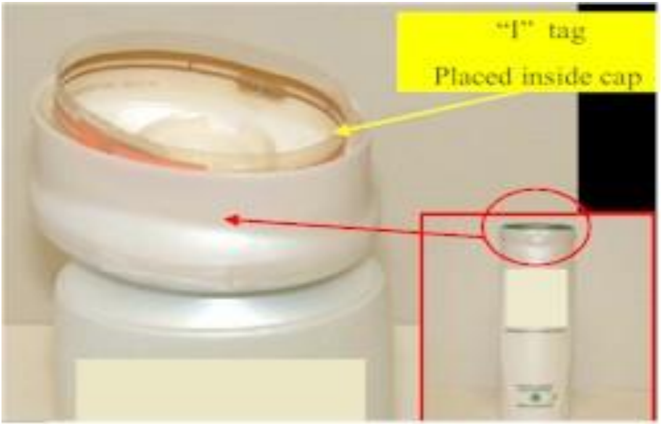
Other Systems

RFID Tags: Smart Labels



Some RFID Tags

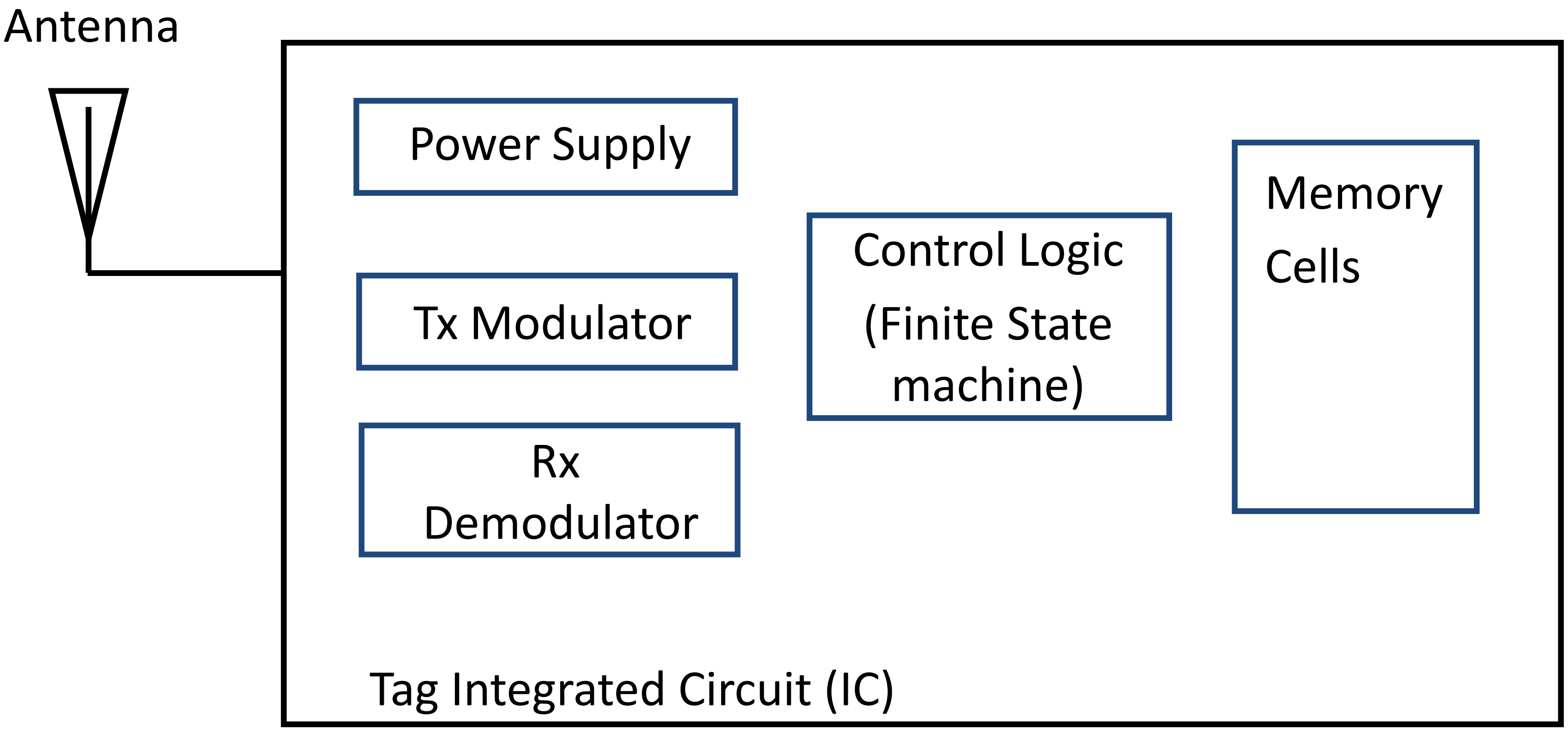




RFID Tags

- Tags can be attached to almost anything:
  - Items, cases or pallets of products, high value goods
  - Vehicles, assets, livestock or personnel
- **Passive Tags**
  - Do not require power – Draws from Interrogator Field
  - Lower storage capacities (few bits to 1 KB)
  - Shorter read ranges (4 inches to 15 feet)
  - Usually Write-Once-Read-Many/Read-Only tags
  - Cost around 25 cents to few dollars
- **Active Tags**
  - Battery powered
  - Higher storage capacities (512 KB)
  - Longer read range (300 feet)
  - Typically can be re-written by RF Interrogators
  - Cost around 50 to 250 dollars

Tag Block Diagram



RFID Tag Memory

- Read-only tags
  - Tag ID is assigned at the factory during manufacturing
    - Can never be changed
    - No additional data can be assigned to the tag
- Write once, read many (WORM) tags
  - Data written once, e.g., during packing or manufacturing
    - Tag is locked once data is written
    - Similar to a compact disc or DVD
- Read/Write
  - Tag data can be changed over time
    - Part or all of the data section can be locked

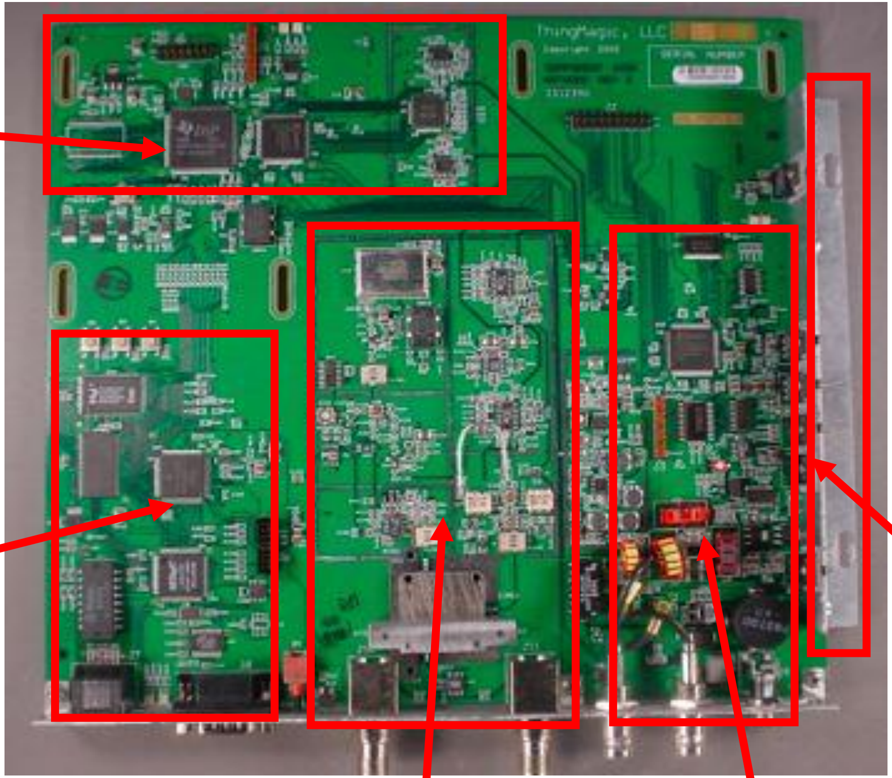
RFID Readers

- Reader functions:
  - Remotely power tags
  - Establish a bidirectional data link
  - Inventory tags, filter results
  - Communicate with networked server(s)
  - Can read 100-300 tags per second
- Readers (interrogators) can be at a fixed point such as
  - Entrance/exit
  - Point of sale
- Readers can also be mobile/hand-held

Some RFID Readers

Reader Anatomy

Digital Signal Processor (DSP)



Network Processor

915MHz Radio

13.56MHz Radio

Power Supply

RFID Advantages over Bar-Codes

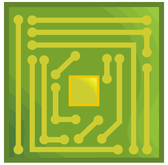
- No line of sight required for reading
- Multiple items can be read with a single scan

- Each tag can carry a lot of data (read/write)
- Individual items identified and not just the category

- Passive tags have a virtually unlimited lifetime
- Active tags can be read from great distances

- Can be combined with barcode technology

"Smart labels": EPC (Electronic Product Code) tags

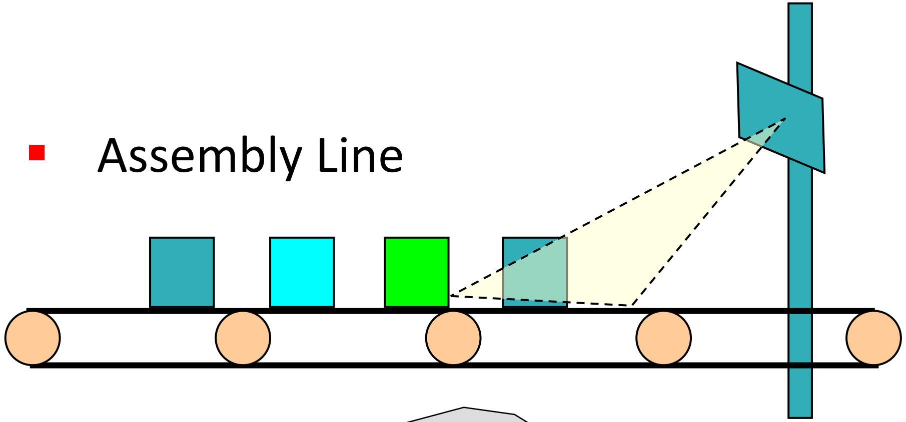
Barcode	EPC tag
	
Line-of-sight	**Radio contact**
Specifies object type	**Uniquely specifies object**

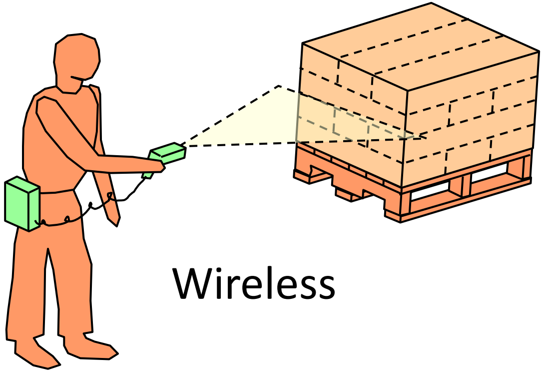
Fast, automated scanning

Provides pointer to database entry for every object, i.e., unique, detailed history

RFID Application Points

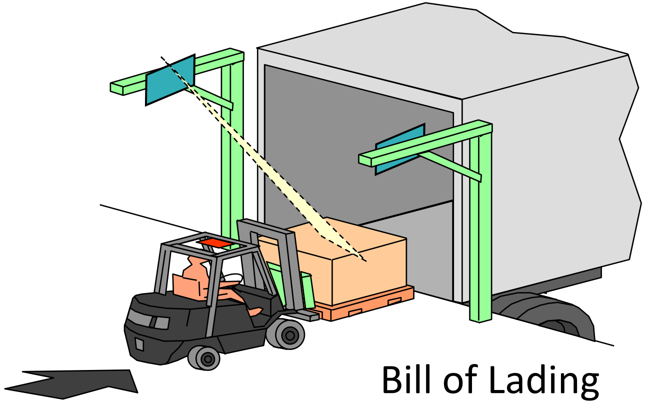
- Assembly Line





Wireless

- Handheld Applications



Bill of Lading
Material Tracking

- Shipping Portals

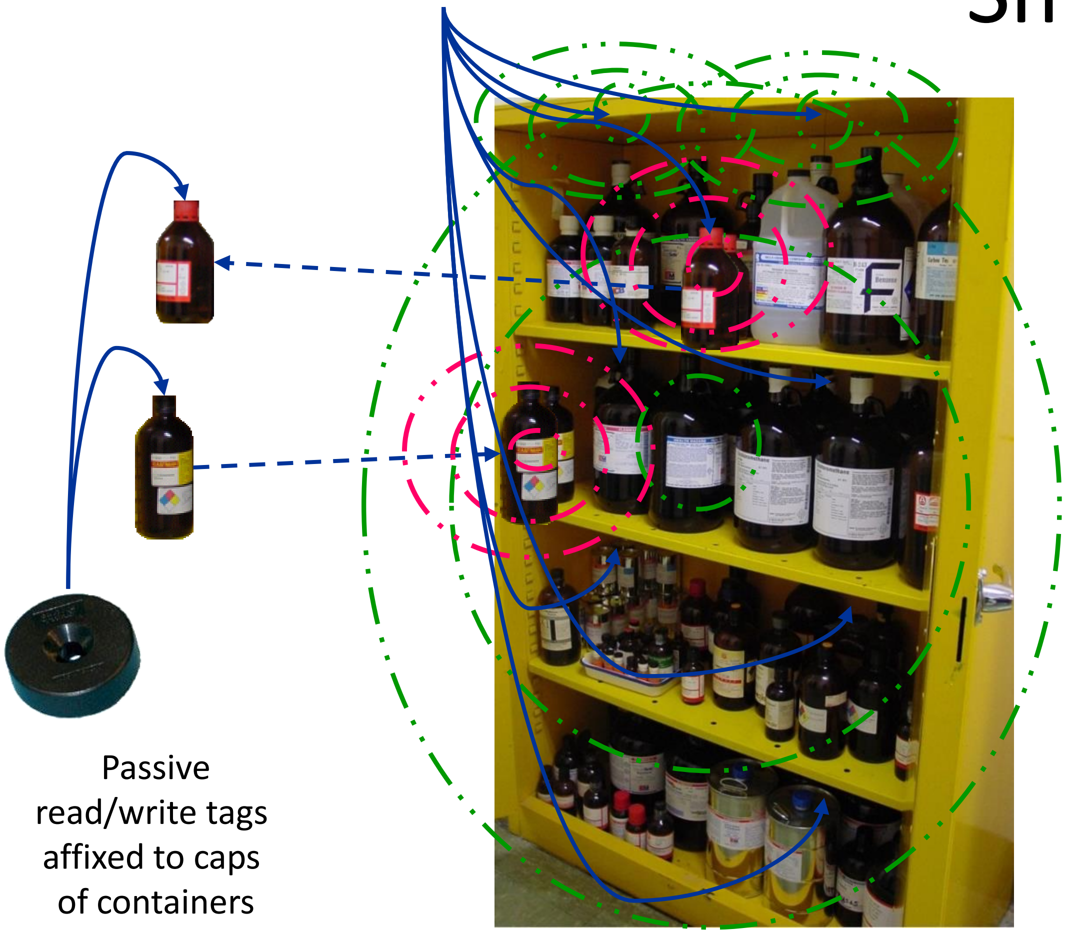
RFID Applications

- Manufacturing and Processing
  - Inventory and production process monitoring
  - Warehouse order fulfillment
- Supply Chain Management
  - Inventory tracking systems
  - Logistics management
- Retail
  - Inventory control and customer insight
  - Auto checkout with reverse logistics
- Security
  - Access control
  - Counterfeiting and Theft control/prevention
- Location Tracking
  - Traffic movement control and parking management
  - Wildlife/Livestock monitoring and tracking

Smart Groceries

- Add an RFID tag to all items in the grocery
- As the cart leaves the store, it passes through an RFID transceiver
- The cart is rung up in seconds

Smart Cabinet



1. Tagged item is removed from or placed in "Smart Cabinet"
2. "Smart Cabinet" periodically interrogates to assess inventory
3. Server/Database is updated to reflect item's disposition
4. Designated individuals are notified regarding items that need attention (cabinet and shelf location, action required)

Smart Fridge

- Recognizes what's been put in it
- Recognizes when things are removed
- Creates automatic shopping lists
- Notifies you when things are past their expiration

- Shows you the recipes that most closely match what is available

Smart Groceries Enhanced

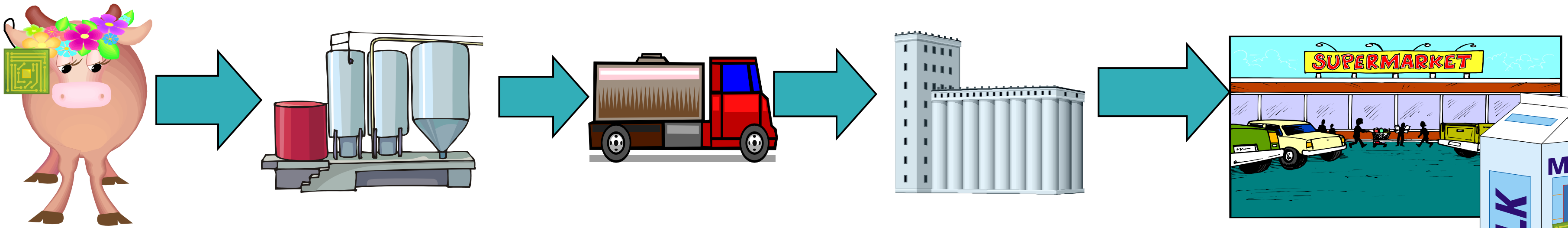
- Track products through their entire lifetime

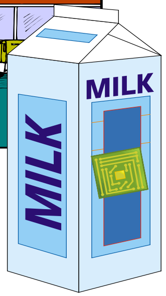
Some More Smart Applications

- “Smart” appliances:
  - Closets that advice on style depending on clothes available
  - Ovens that know recipes to cook pre-packaged food
- “Smart” products:
  - Clothing, appliances, CDs, etc. tagged for store returns
- “Smart” paper:
  - Airline tickets that indicate your location in the airport
- “Smart” currency:
  - Anti-counterfeiting and tracking

- “Smart” people ??

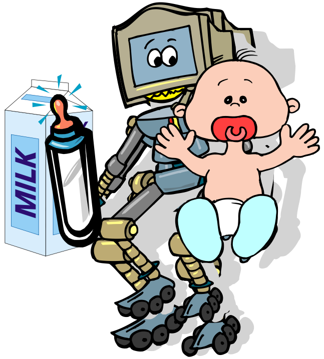
2030: Week in the Life of a Milk Carton

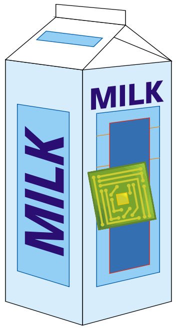




- 30 April: RFID-tagged cow 'Bessie' produces milk
- 30 April: Milk transferred to RFID-tagged tank
  - Cow identity and milking time recorded in tank-tag database
- 1 May: RFID portal on truck records loading of refrigeration tanks
  - (Truck also has active RFID (+GPS) to track geographical location and RFID transponder to pay tolls)
- 2 May: Chemical-treatment record written to database record for milk barrel
  - Bessie's herd recorded to have consumed bitter grass; compensatory sugars added
- 3 May: Milk packaged in RFID-tagged carton; milk pedigree recorded in database associated with cart on tag
- 4 May: RFID portal at supermarket loading dock records arrival of carton
- 5 May: 'Smart' shelf records arrival of carton in customer area
- 5 May 0930h: 'Smart' shelf records removal of milk
- 5 May 0953h: Point-of-sale terminal records sale of milk (to Alice)

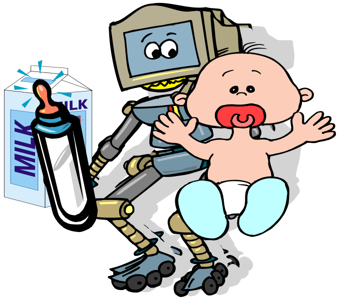
2030: Week in the Life of a Milk Carton

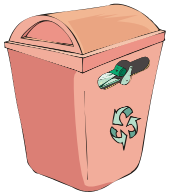


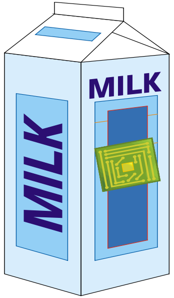


- 6 May 0953h: Supermarket transfers tag ownership to Alice’s smart home
- 6 May 1103h: Alice’s refrigerator records arrival of milk
- 6 May 1405h: Alice’s refrigerator records removal of milk; refrigerator looks up database-recorded pedigree and displays: “*Woodstock, Vermont, Grade A, light pasturization, artisanal, USDA organic, breed: Jersey, genetic design #81726*”
- 6 May 1807h: Alice’s ‘smart’ home warns domestic robot that milk has been left out of refrigerator for more than four hours
- 6 May 1809h: Alice’s refrigerator records replacement of milk
- 7 May 0530h: Domestic robot uses RFID tag to locate milk in refrigerator; refills baby bottle

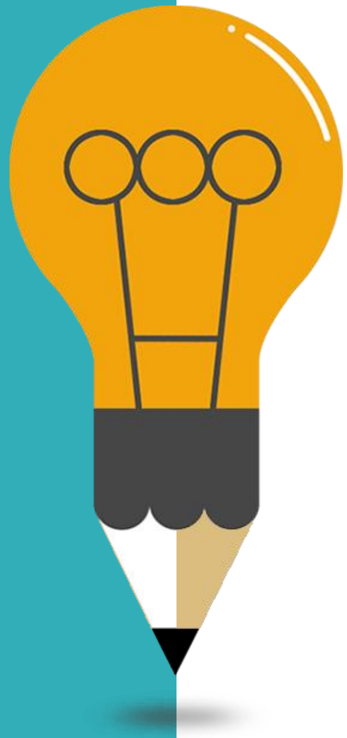
2030: Week in the Life of a Milk Carton







- 7 May 0530h: Domestic robot uses RFID tag to locate milk in refrigerator; refills baby bottle
- 7 May 0531h: Robot discards carton; ‘Smart’ refrigerator notes absence of milk; transfers order to Alice’s PDA/phone/portable server grocery list
- 7 May 2357h: Recycling center scans RFID tag on carton; directs carton to paper-brick recycling substation



Outline

01 **Overview of RFID**

Reader-Tag; Potential applications

02 **RFID Technology Internals**

RF communications

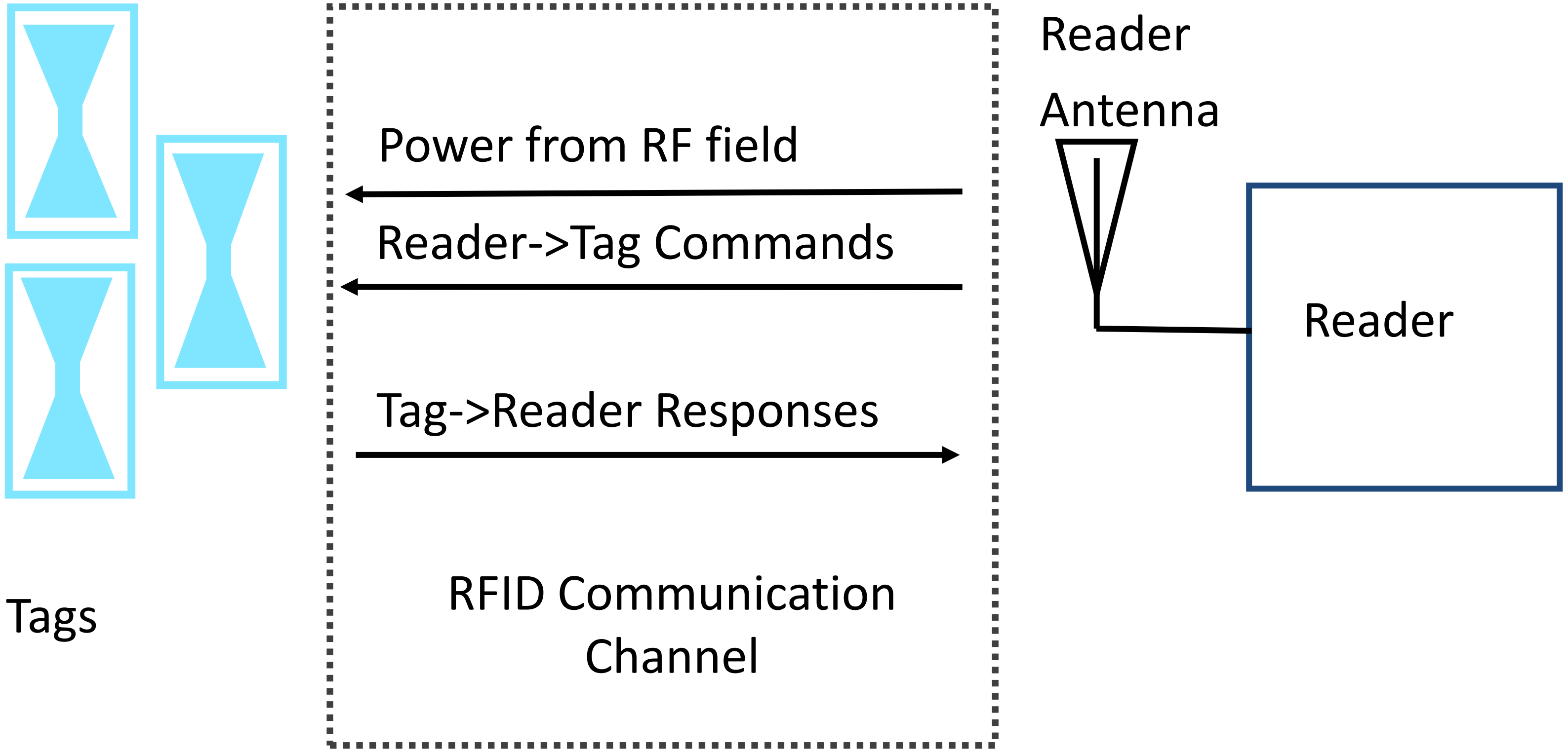
Reader/Tag protocols

Middleware architecture

03 **Security and Privacy**

04 **Conclusion**

RFID Communications



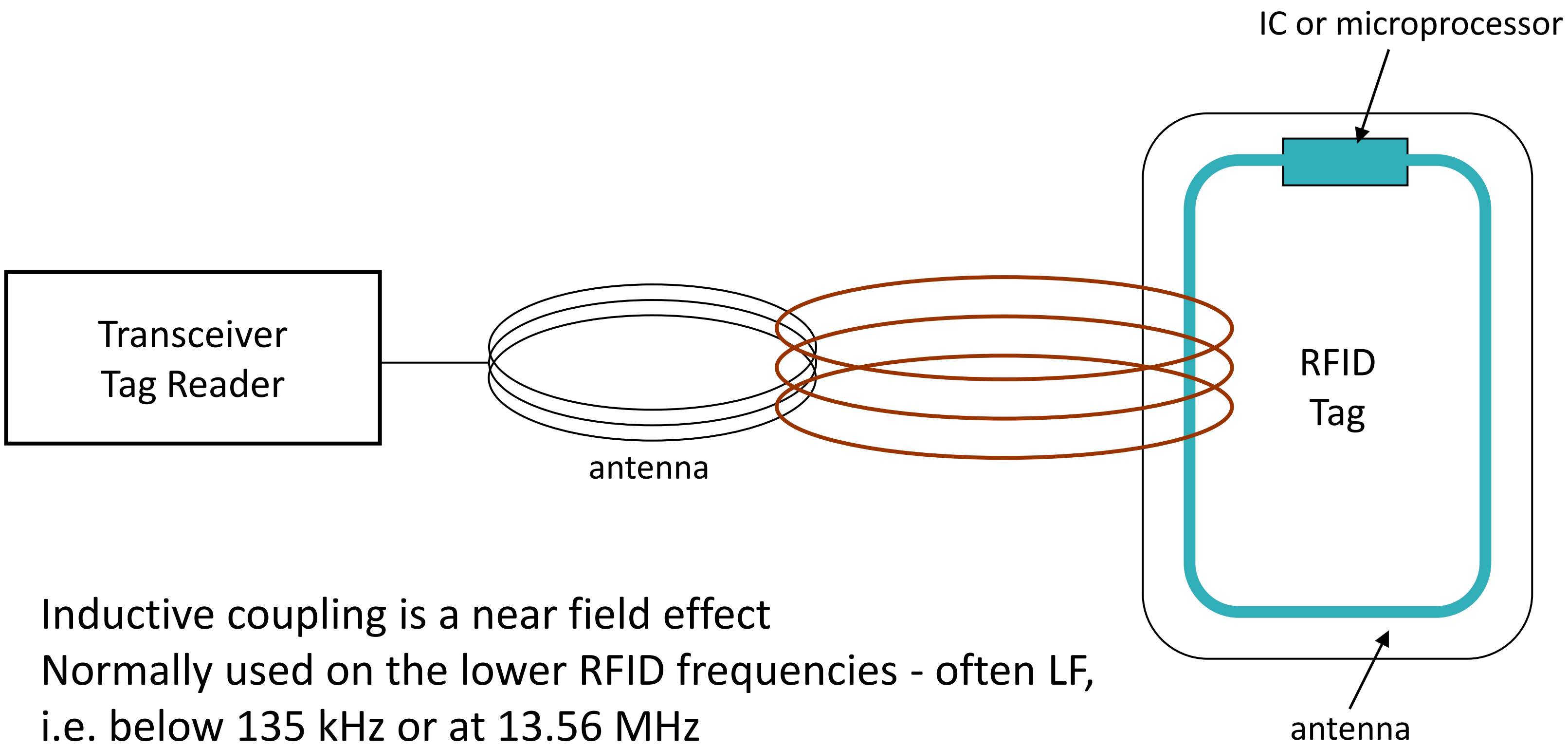
RFID Communication

- Host manages Reader(s) and issues Commands

- Reader and tag communicate via RF signal
- Carrier signal generated by the reader
- Carrier signal sent out through the antennas
- Carrier signal hits tag(s)
- Tag receives and modifies carrier signal
  - "sends back" modulated signal (Passive Backscatter – also referred to as "field disturbance device")
- Antennas receive the modulated signal and send them to the Reader

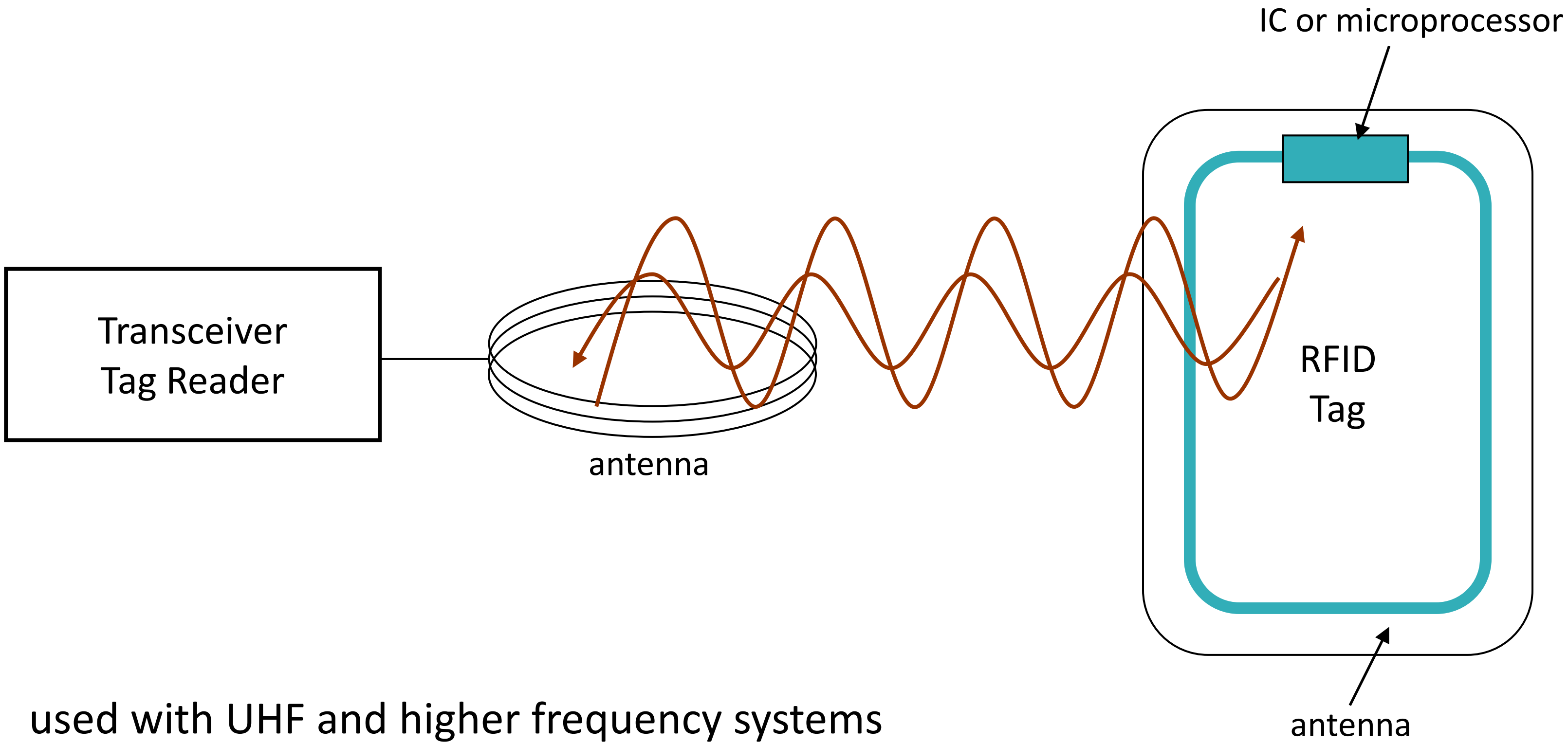
- Reader decodes the data
- Results returned to the host application

Antenna Fields: Inductive Coupling



- Inductive coupling is a near field effect
- Normally used on the lower RFID frequencies - often LF, i.e. below 135 kHz or at 13.56 MHz

Antenna Fields: Propagation Coupling

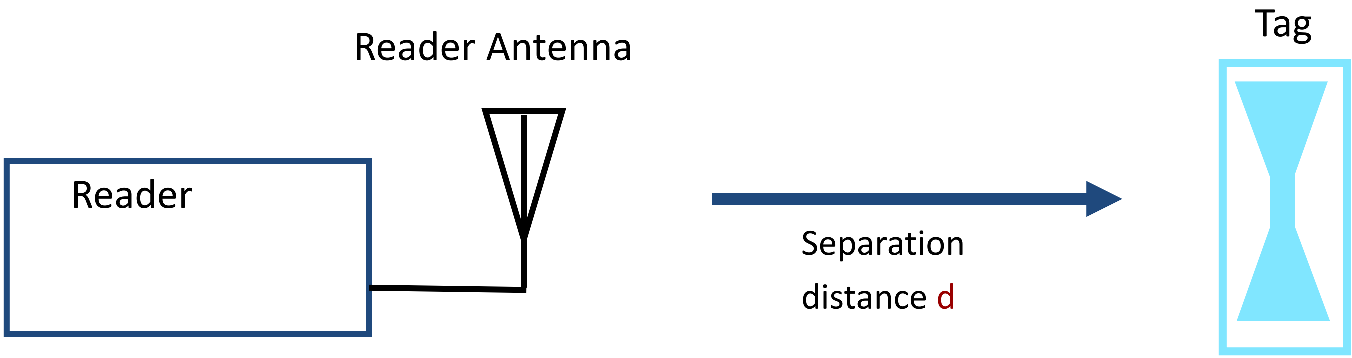


used with UHF and higher frequency systems

Operational Frequencies

Frequency Ranges	LF 125 KHz	HF 13.56 MHz	UHF 868 - 915 MHz	Microwave 2.45 GHz & 5.8 GHz
Typical Max Read Range (Passive Tags)	Shortest 1”-12”	Short 2”-24”	Medium 1’-10’	Longest 1’-15’
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling	Active tags with integral battery or passive tags using capacitive storage, E-field coupling
Data Rate	Slower	Moderate	Fast	Faster
Ability to read near metal or wet surfaces	Better	Moderate	Poor	Worse
Applications	Access Control & Security Identifying widgets through manufacturing processes or in harsh environments Ranch animal identification Employee IDs	Library books Laundry identification Access Control Employee IDs	supply chain tracking Highway toll Tags	Highway toll Tags Identification of private vehicle fleets in/out of a yard or facility Asset tracking

Reader->Tag Power Transfer



Q: If a reader transmits Pr watts, how much power Pt does the tag receive at a separation distance d?

A: It depends-

UHF (915MHz) : Far field propagation : $Pt \propto 1/d^2$

HF (13.56MHz) : Inductive coupling : $Pt \propto 1/d^6$

Limiting Factors for Passive RFID

1. Reader transmitter power Pr (Gov't. limited)
2. Reader receiver sensitivity Sr
3. Reader antenna gain Gr (Gov't. limited)

4. Tag antenna gain Gt (Size limited)
5. Power required at tag Pt (Silicon process limited)
6. Tag modulator efficiency Et

Implications

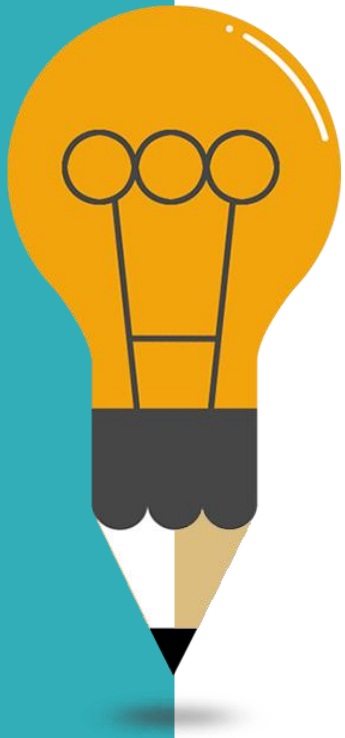
- Since $Pt \propto 1/d^2$, doubling read range requires 4X the transmitter power
- Larger antennas can help, but at the expense of larger physical size because $G\{t,r\} \propto Area$
- More advanced CMOS process technology will help by reducing Pt

- At large distances, reader sensitivity limitations dominate

RF Effects of Common Materials

Material	Effect(s) on RF signal
Cardboard	Absorption (moisture) Detuning (dielectric)
Conductive liquids (shampoo)	Absorption
Plastics	Detuning (dielectric)
Metals	Reflection
Groups of cans	Complex effects (lenses, filters) Reflection
Human body / animals	Absorption, Detuning, Reflection

Outline



01 **Overview of RFID**

Reader-Tag; Potential applications

02 **RFID Technology Internals**

RF communications

Reader/Tag protocols

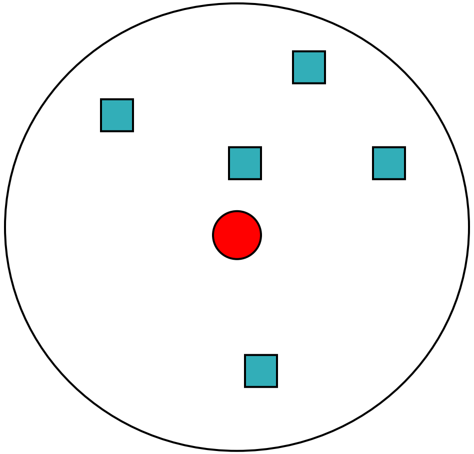
Middleware architecture

03 **Security and Privacy**

04 **Conclusion**

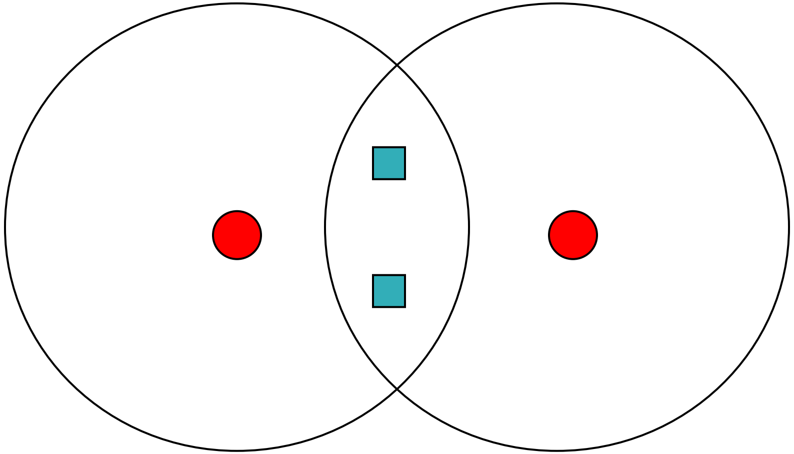
Reader Collision Problem

Tag collision



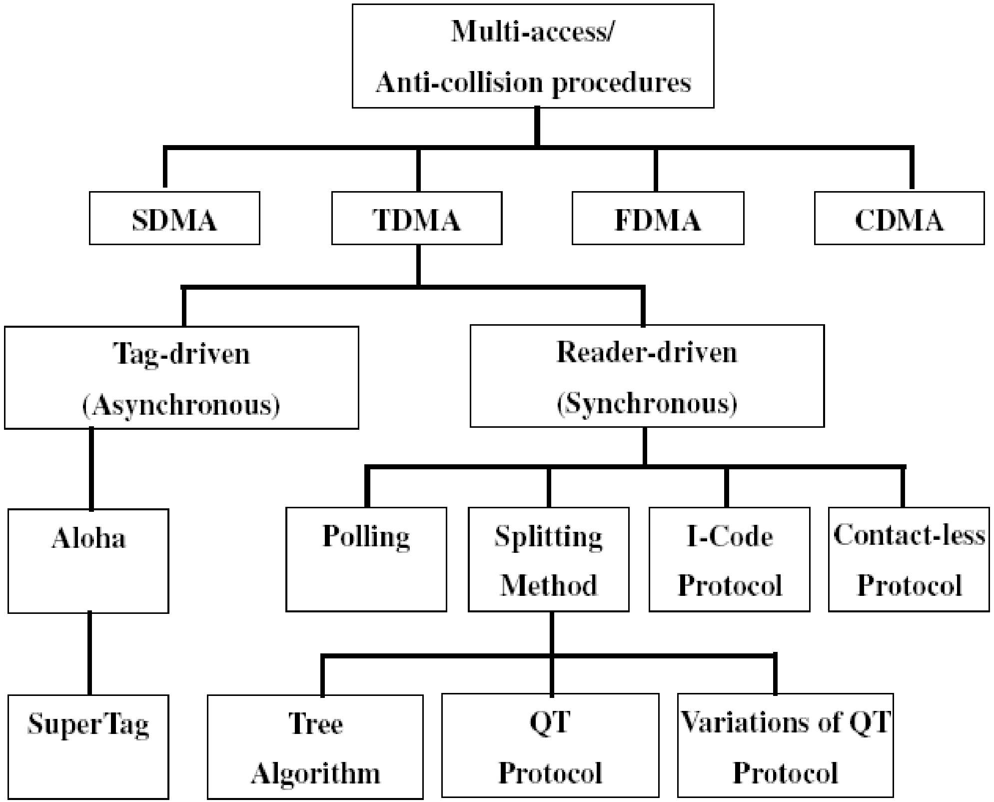
Probability-based
Deterministic-based (Prefix-based)

Reader collision



Centralized
Distributed

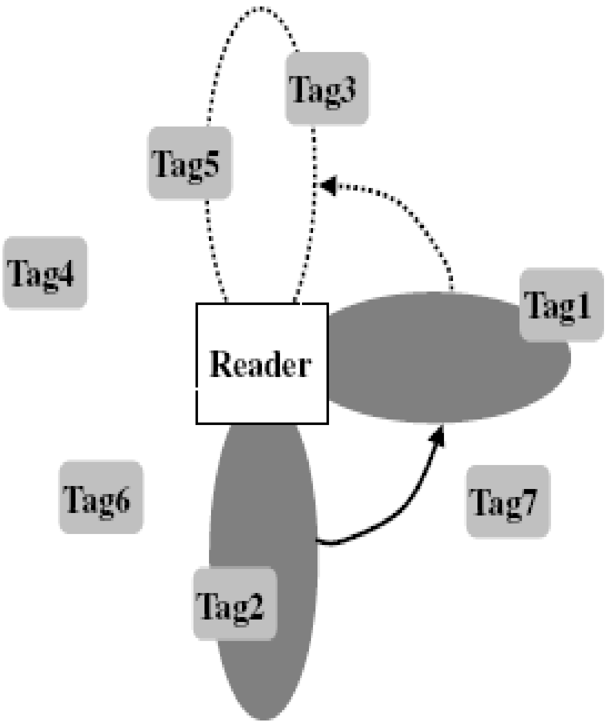
Taxonomy of Tag Anti-Collision Protocols



by Dong-Her Shih et. al., published in Computer Communications, 2006

SDMA

- SDMA (Space Division Multiple Access)
  - Reuse a certain resource, such as channel capacity in spatially separated area
    - Reduce the reading range of readers and forms as an array in space
    - Electronically controlled directional antenna
    - Various tags can be distinguished by their angular positions

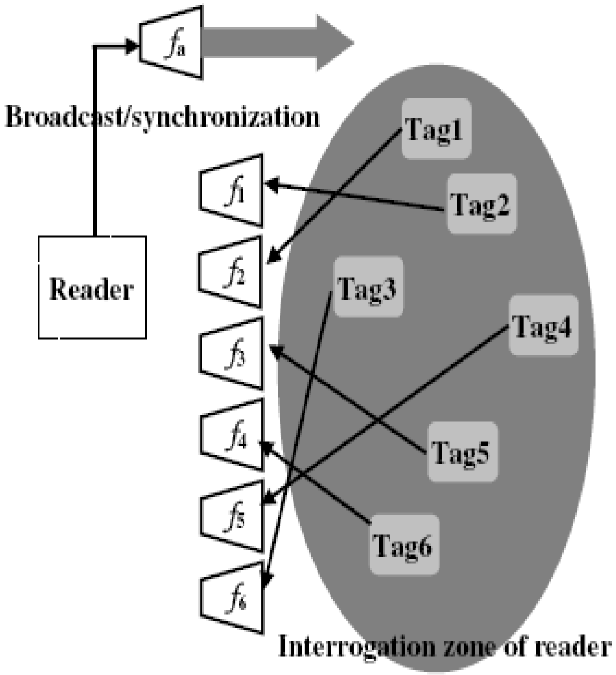


Disadvantage: the relatively high implementation cost of the complicated antenna system

FDMA

- FDMA (Frequency Division Multiple Access)
  - Several transmission channels on various carrier frequencies are simultaneously available
  - Tags respond on one of several frequencies

Disadvantage: the relatively high cost of the readers, since a dedicated receiver must be provided for every reception channel



CDMA

- CDMA (Code Division Multiple Access)
  - Too complicate and too computationally intense for RFID tags as well
  - CDMA uses spread spectrum modulation techniques based on pseudo random codes, to spread the data over the entire spectrum

TDMA

- TDMA (Time Division Multiple Access)
  - The largest group of RFID anti-collision protocols
  - Tag driven (tag talk first, TTF)
    - Tag transmits as it is ready
    - Aloha
    - SuperTags
      - Tags keep retransmit ID with random interval until reader acknowledges
    - Tag-driven procedures are naturally very slow and inflexible
  - Reader driven (reader talk first, RTF)
    - Polling, splitting, I-code, contactless

Slotted ALOHA

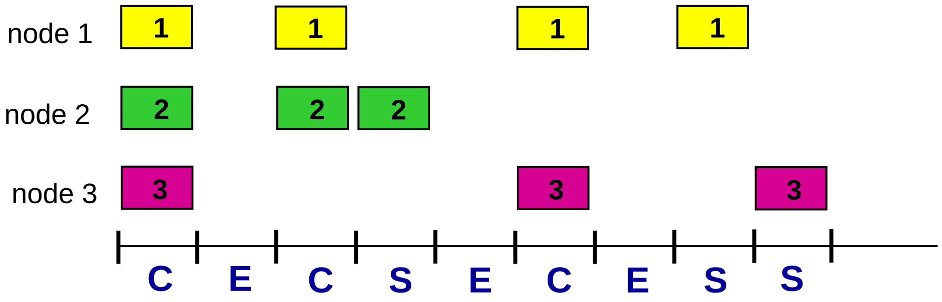
assumptions:

- all frames same size
- time divided into equal size slots (time to transmit 1 frame)
- nodes start to transmit only slot beginning
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision

operation:

- when node obtains fresh frame, transmits in next slot
  - *if no collision:* node can send new frame in next slot
  - *if collision:* node retransmits its frame in each subsequent slot with prob. p until success

Slotted ALOHA



Pros:

- single active node can co ntinuously transmit at ful l rate of channel
- highly decentralized: only slots in nodes need to b e in sync
- simple

Cons:

- collisions, wasting slots
- idle slots
- nodes may be able to de tect collision in less than time to transmit packet
- clock synchronization

Slotted ALOHA: efficiency

efficiency: long-run fraction of successful slots (many nodes, all with many frames to send)

- *suppose:* N nodes with many frames to send, each transmits in slot with probability p
- prob that given node has success in a slot $= p(1-p)^{N-1}$
- prob that *any* node has a success $= Np(1-p)^{N-1}$

- max efficiency: find p^* that maximizes $Np(1-p)^{N-1}$
- for many nodes, take limit of $Np^*(1-p^*)^{N-1}$ as N goes to infinity, gives:

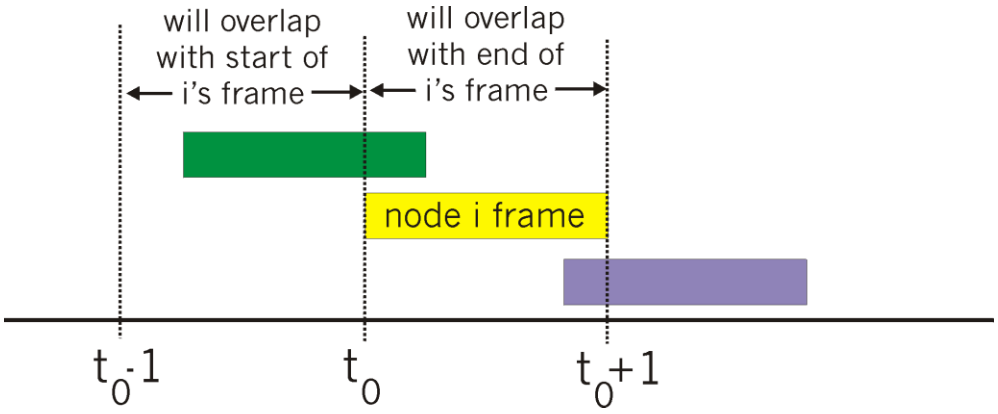
max efficiency = 1/e = .37

at best: channel used for useful transmissions 37% of time!

!

Pure (unslotted) ALOHA

- unslotted Aloha: simpler, no synchronization
- when frame first arrives
  - transmit immediately
- collision probability increases:
  - frame sent at t0 collides with other frames sent in [t0-1,t0+1]



Pure ALOHA efficiency

P(success by given node) = P(node transmits) $\cdot$

P(no other node transmits in $[t_0-1,t_0]$ $\cdot$

P(no other node transmits in $[t_0-1,t_0]$

$$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$$

$$= p \cdot (1-p)^{2(N-1)}$$

… choosing optimum p and then letting $n \rightarrow \infty$

$$= 1/(2e) = .18$$

even *worse* than slotted Aloha!

Polling

- Polling
  - Master node invites the slave nodes to transmit data in turn
  - Reader must have the complete knowledge (database) of tags
  - Reader interrogates the RFID tags by polling ‘‘whose serial number starts with a 1 in the first position?’’
  - Those tags meet this test reply “yes” while others remain
  - Similar question about the next digit in their binary serial number continues
  - Slow, inflexible

Splitting

- Splitting or tree-search
  - Nodes transmit packets in time slots, if there is more than one node transmitting in a time slot then a collision occurs at the receiver
  - Collision resolution split the set of colliding nodes into two subsets
    - Nodes in the first subset transmit in the first time slot. Nodes in the other subset wait until the collision between the first subset of nodes is completely resolved
    - If the first subset of nodes encounters another collision, then further splitting takes place
    - This is done recursively till all the collisions have been resolved
    - Once all the collisions in the first subset of nodes are resolved, then a similar procedure is followed for the second subset

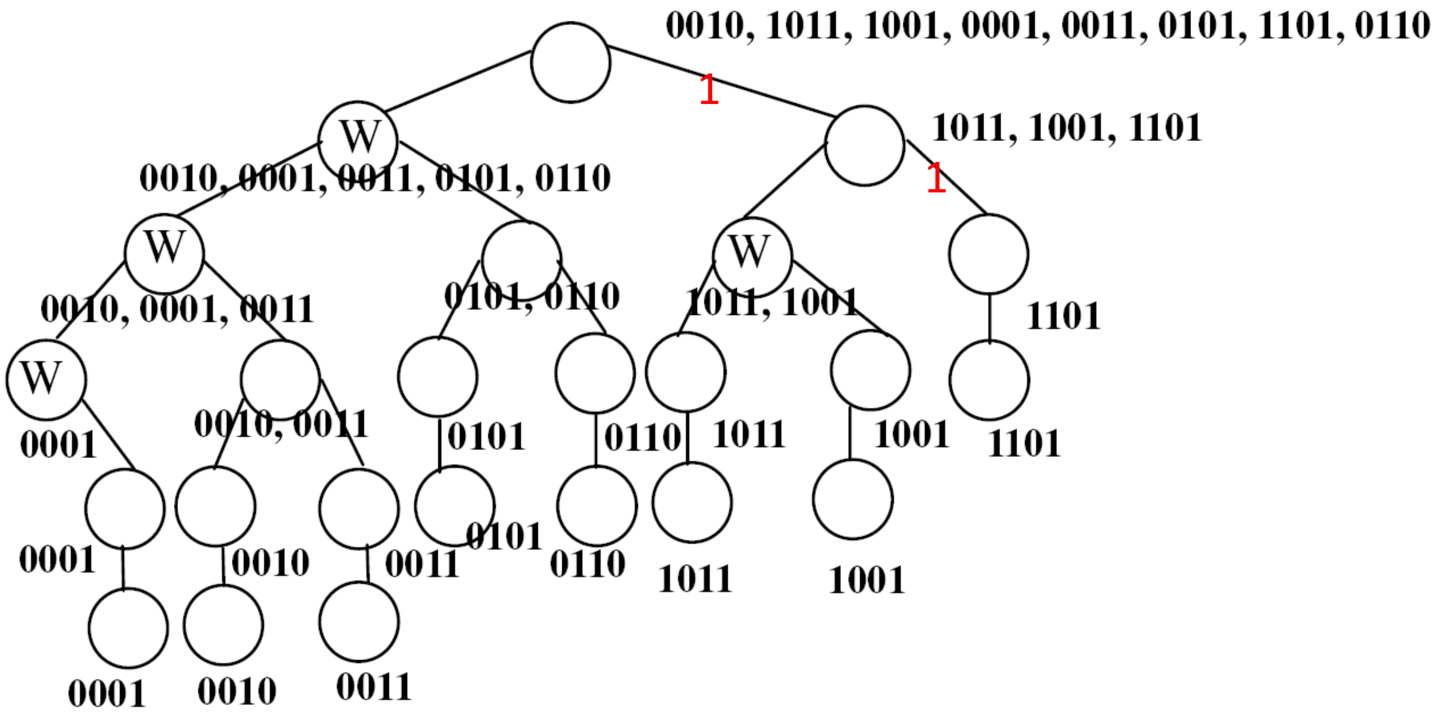
Splitting

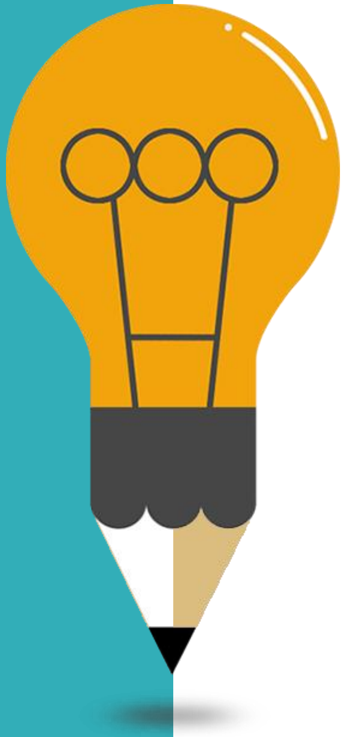
- Tree algorithm
  - Based on binary search tree algorithm
  - Each collided tag generates a random number by flipping an unbiased B-sided coin (splitting the colliding tags into B disjoint subsets)
    - B = 2, each collided tag would generate a number 0 or 1
  - The reader always sends a feedback informing the tags whether 0 packet, 1 packet, or more than 1 packet is transmitted in the previous slot
  - Each tag needs to keep track of its position in the binary tree according to the reader’s feedback

Contact-less

- Contact-less
  - Is based on the tree splitting methodology to identify one bit of the ID in every arbitration step
  - The tag uses the modulation scheme which identifies “0” in the specified bit position with 00ZZ (Z stands for no modulation) and “1” as “ZZ00”
    - In this way, the reader can recognize the responses from all the tags and divide the unidentified tags into 2 groups
      - One had *0*’s in the requested bit position and the other had *1*’s. This is termed as the *BitVal* step

Contact-less





Outline

01 Overview of RFID
Reader-Tag; Potential applications

02 RFID Technology Internals
RF communications
Reader/Tag protocols
Middleware architecture

03 Security and Privacy

04 Conclusion

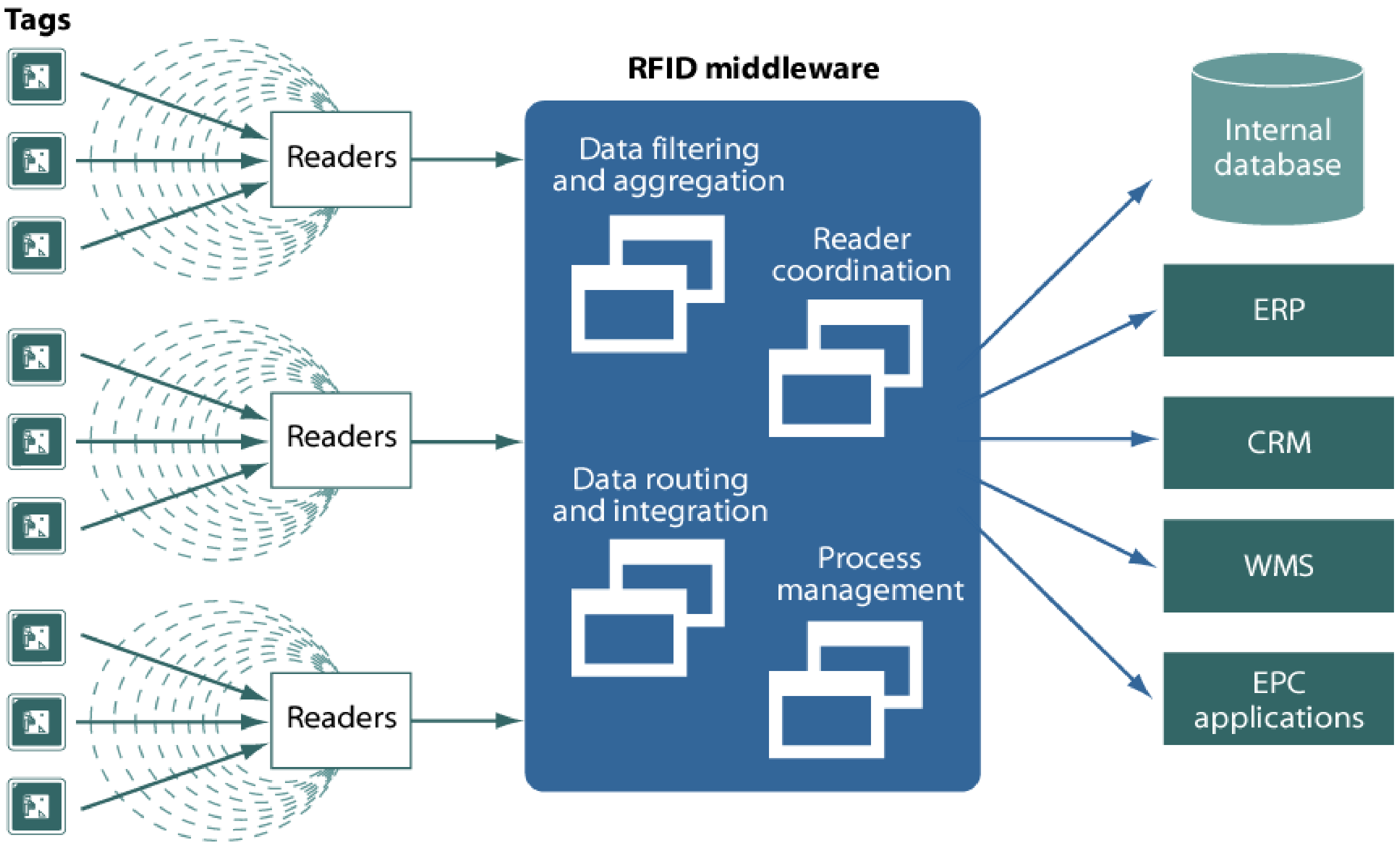
How Much Data?

Consider a supermarket chain implementing RFID:

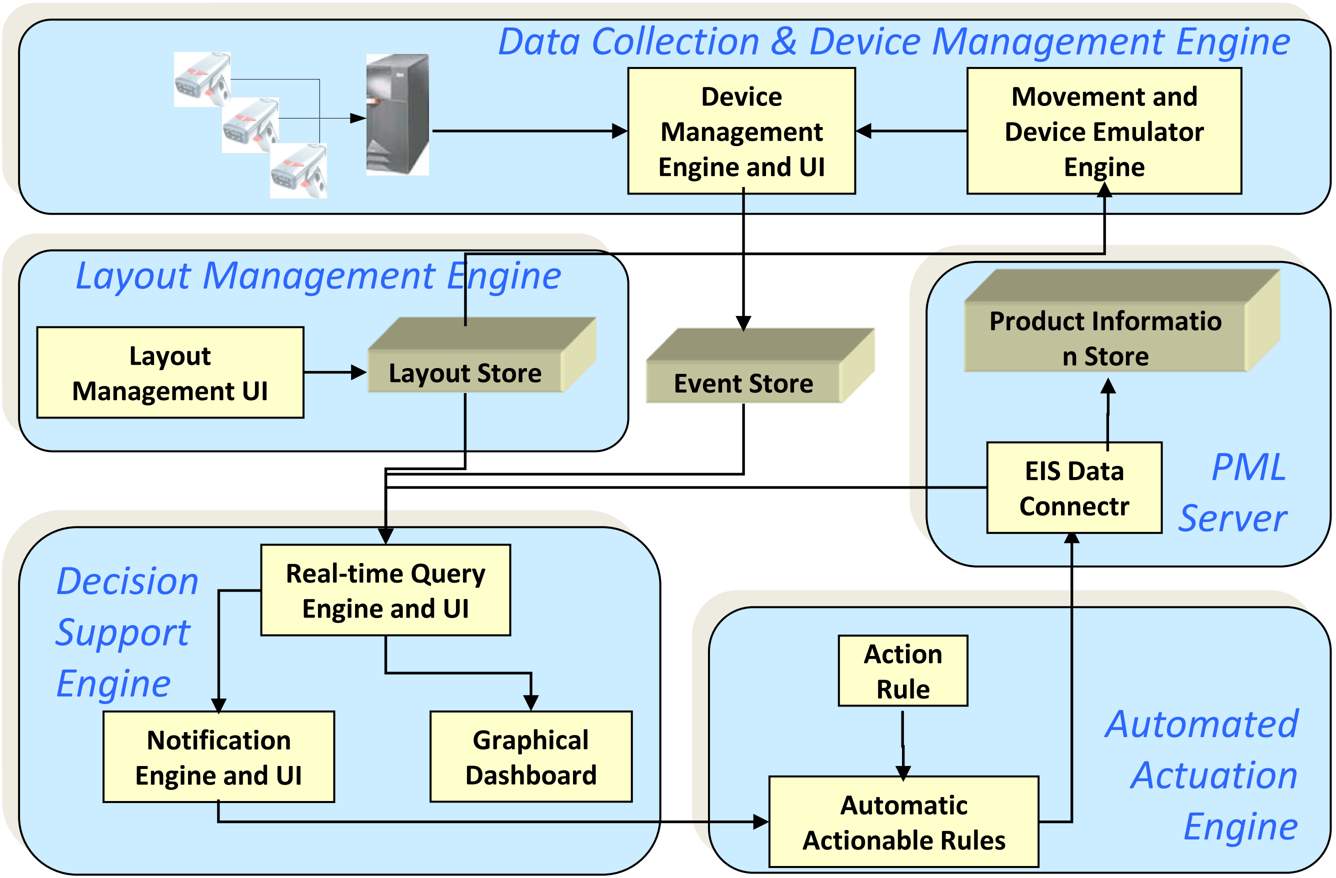
- 12 bytes EPC + Reader ID + Time = 18 bytes per tag
- Average number of tags in a neighborhood store = 700,000
- Data generated per second = 12.6 GB
- Data generated per day = 544 TB
- Assuming 50 stores in the chain,
    - data generated per day = 2720 TB

- Stanford Linear Accelerator Center generates 500 TB

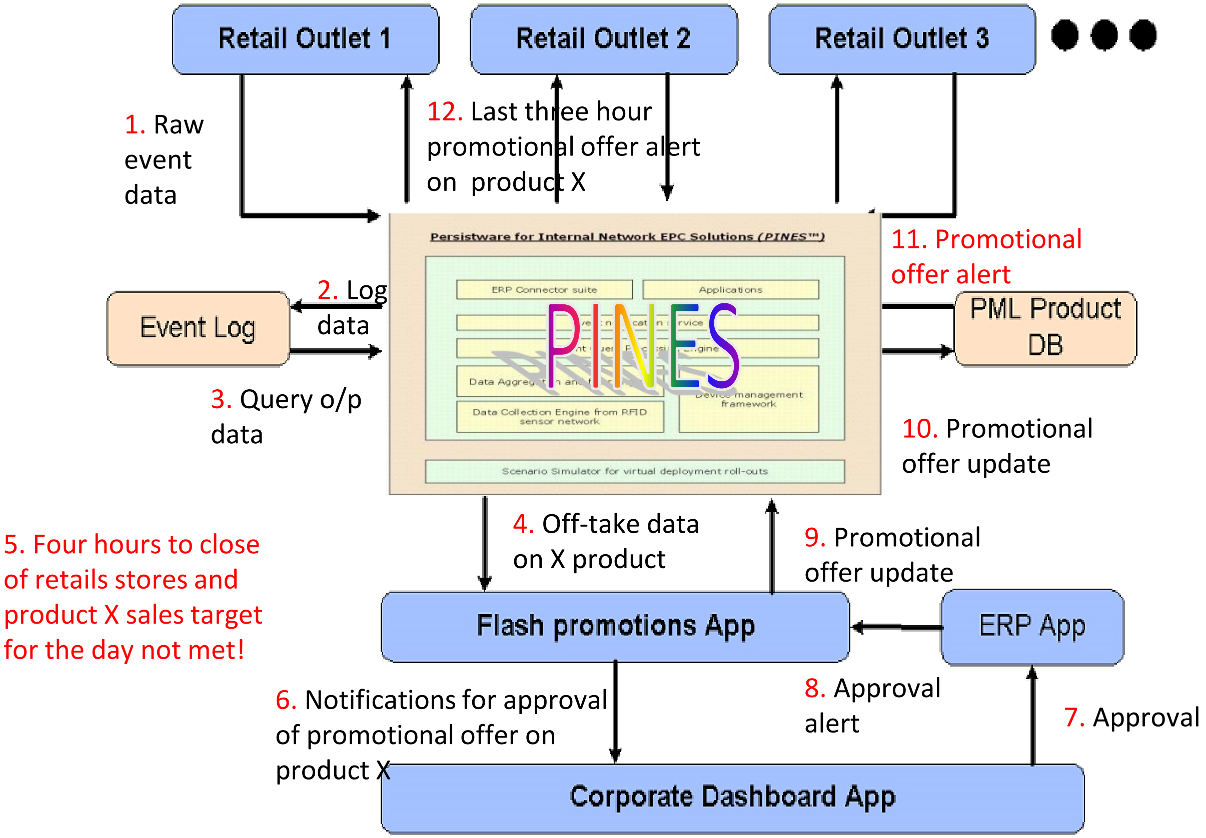
RFID Middleware

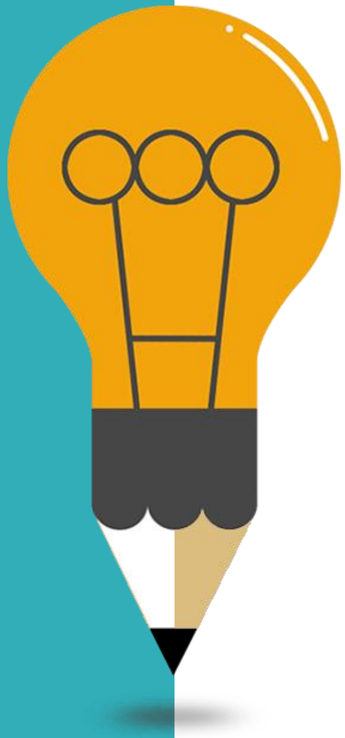


Middleware Framework: PINES™



Retail Case Study: Enabling Real-Time Decisions





Outline

01 Overview of RFID

Reader-Tag; Potential applications

02 RFID Technology Internals

RF communications

Reader/Tag protocols

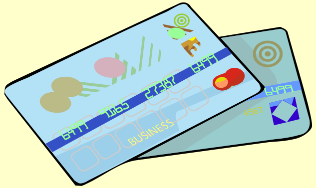
Middleware architecture

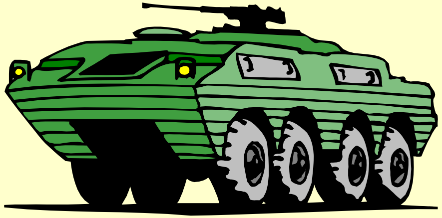
03 Security and Privacy

04 Conclusion

RFID Underpins Essential Infrastructure

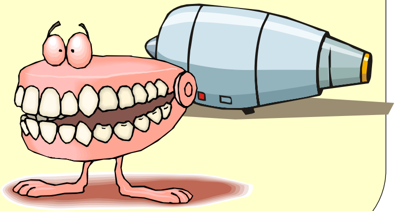
PAYMENT DEVICES





MATERIEL

INDUSTRIAL & MEDICAL PARTS

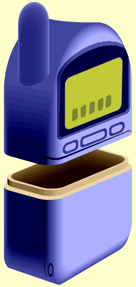


PHYSICAL SECURITY

BORDER CONTROL

FOOD SUPPLY

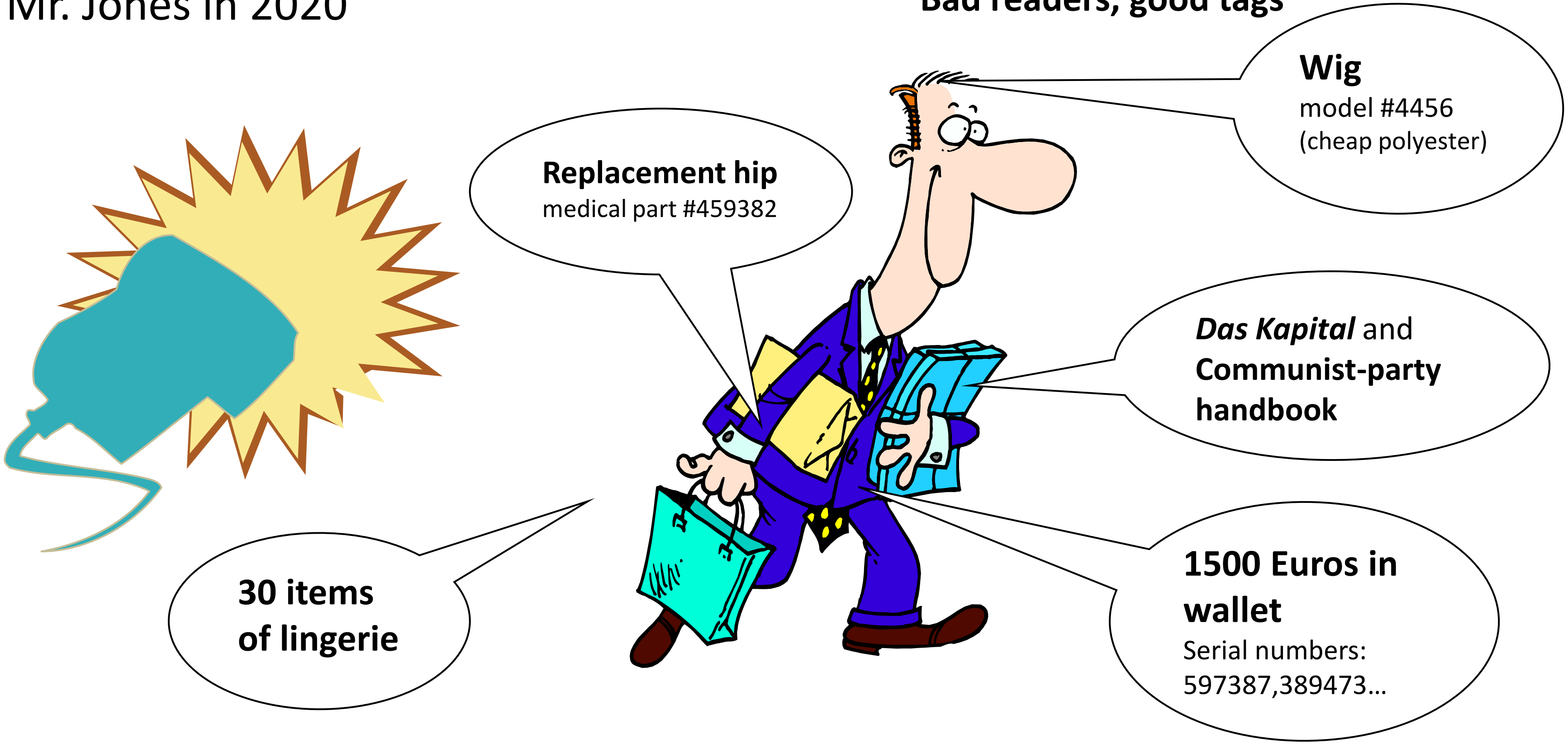
CONSUMER GOODS



The Privacy Problem

Mr. Jones in 2020

Bad readers, good tags



Privacy: The Flip Side of RFID

- Hidden placement of tags
- Unique identifiers for all objects worldwide
- Massive data aggregation
- Unauthorized development of detailed profiles
- Unauthorized third party access to profile data
- Hidden readers

"Just in case you want to know, she's carrying 700 Euro…"

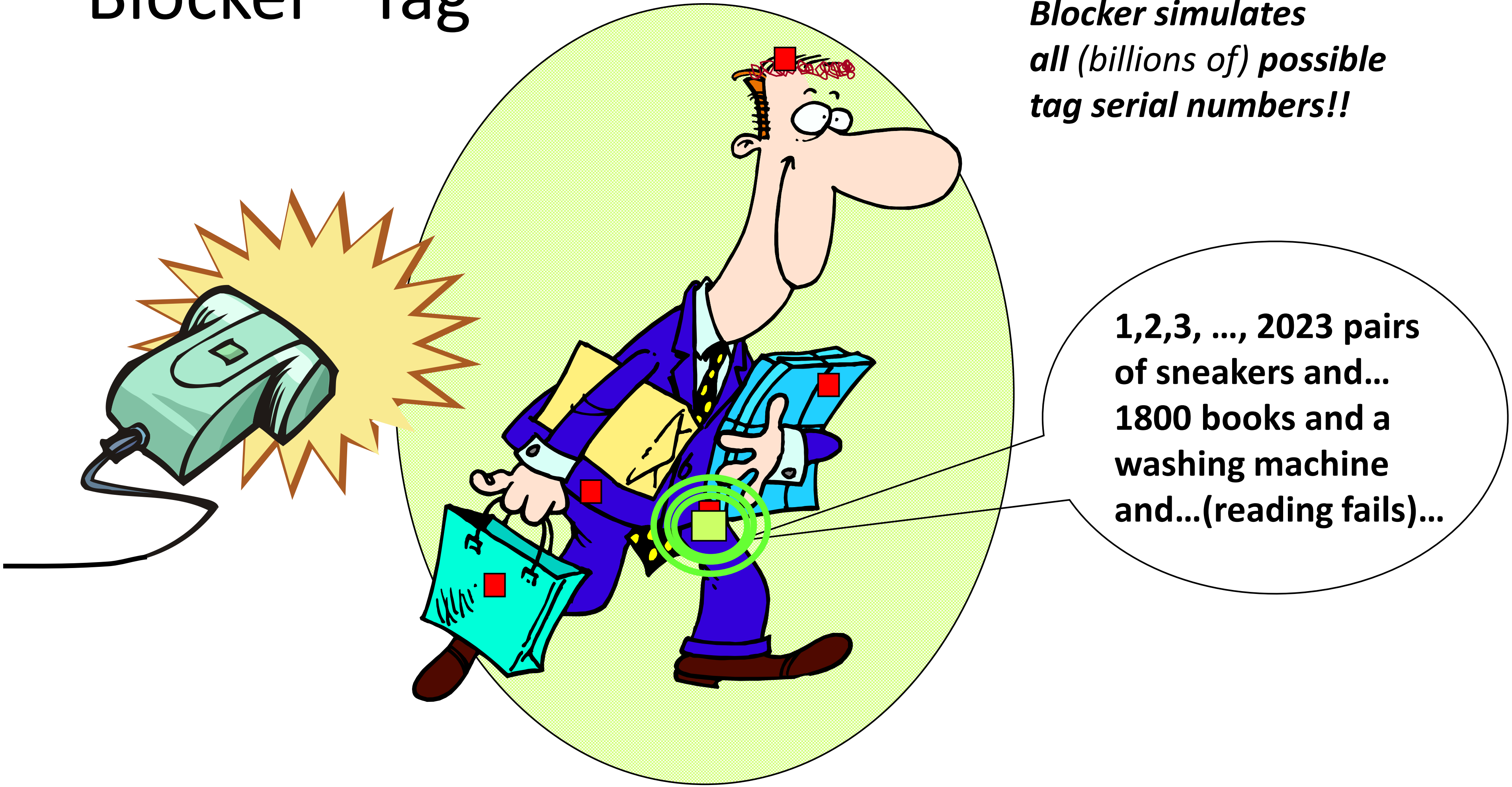
Content privacy: Protection against unauthorized scanning of data stored on tag

Content Privacy via “Blocker” Tags

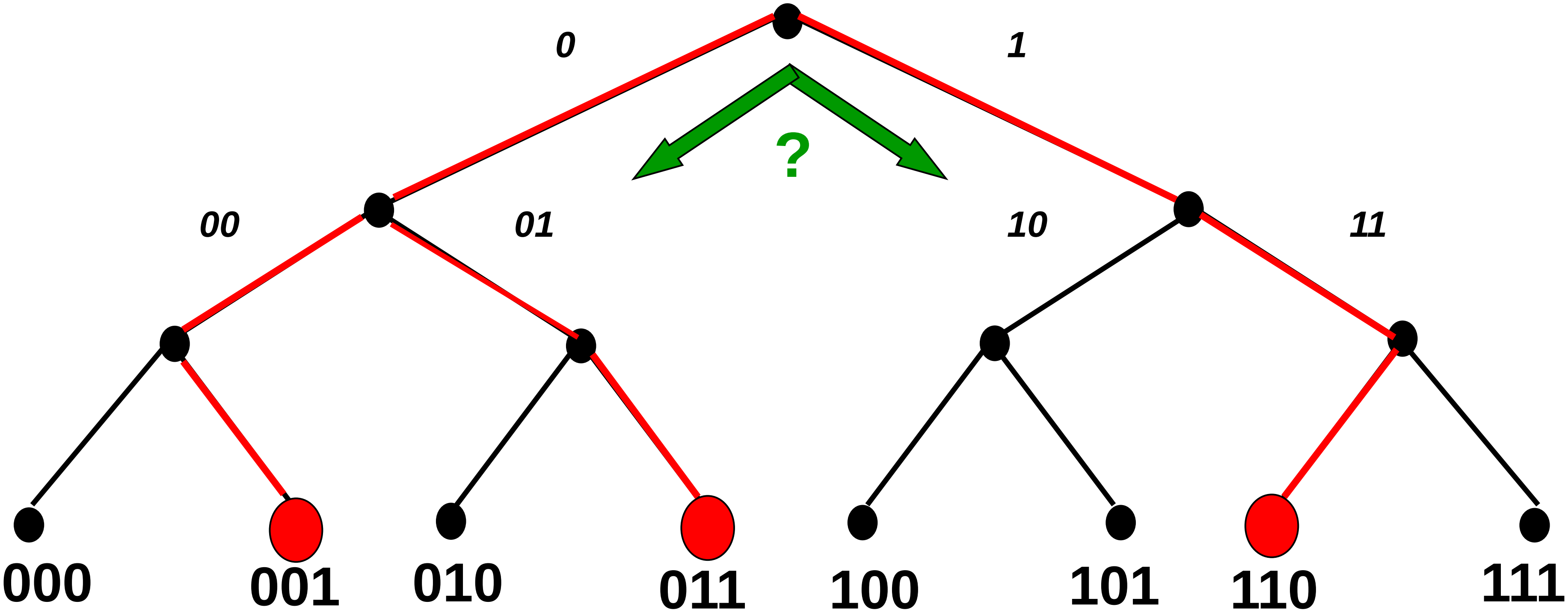
The “Blocker” Tag

“Blocker” Tag

Blocker simulates
all** (billions of) **possible
tag serial numbers!!



“Tree-walking” Anti-Collision Protocol for RFID Tags



In a Nutshell

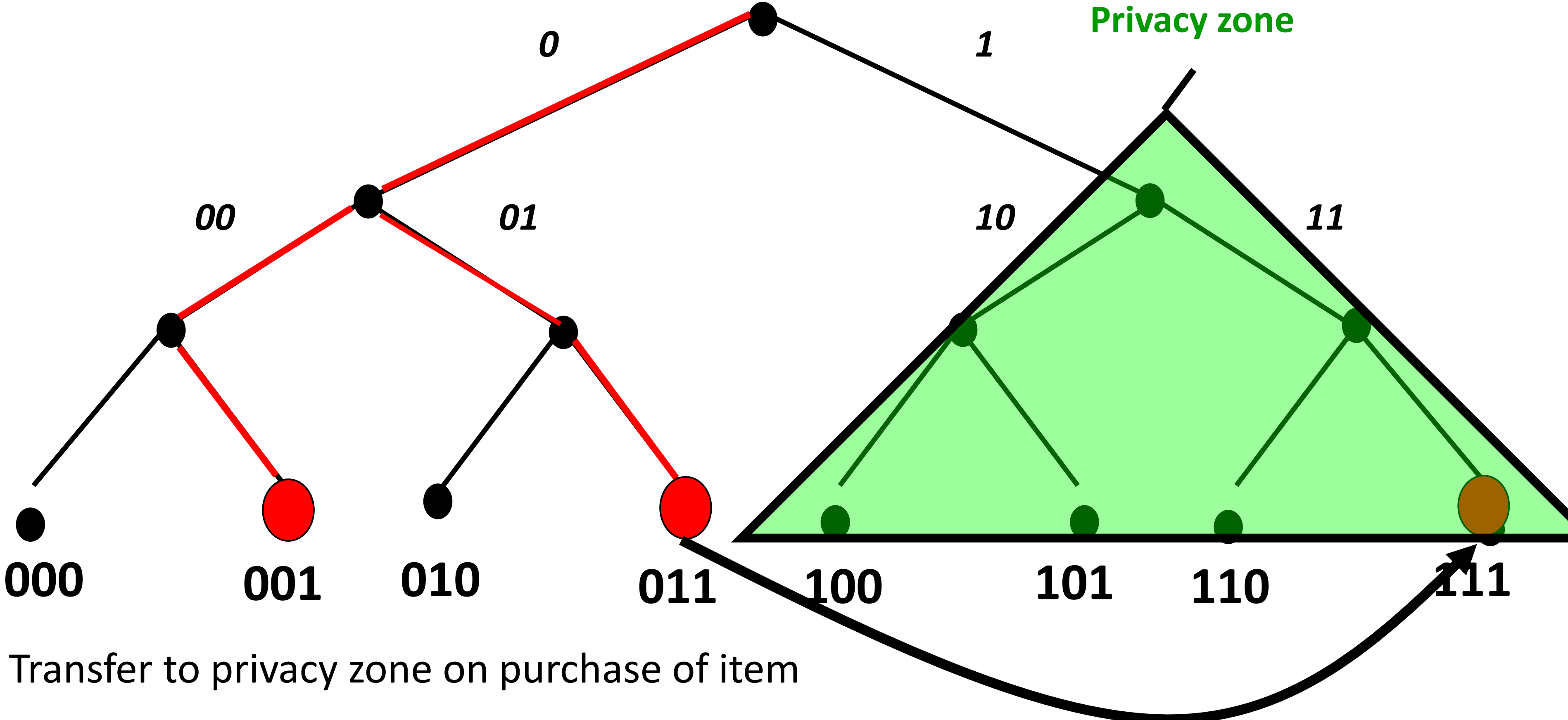
- “Tree-walking” protocol for identifying tags recursively asks question:
  - “What is your next bit?”
- Blocker tag always says ***both ‘0’ and ‘1’***!
  - Makes it seem like *all* possible tags are present
  - Reader cannot figure out which tags are actually present
  - Number of possible tags is *huge* (at least a billion billion), so reader stalls

Blocker tag system should protect privacy but still avoid blocking un-purchased items

Consumer Privacy + Commercial Security

- Blocker tag can be ***selective:***
  - *Privacy zones:* Only block certain ranges of RFID-tag serial numbers
  - *Zone mobility*: Allow shops to move items into privacy zone upon purchase
- Example:
  - Blocker blocks all identifiers with leading ‘1’ bit
  - Items in supermarket carry leading ‘0’ bit
  - On checkout, leading bit is flipped from ‘0’ to ‘1’
    - PIN required, as for ‘kill’ operation

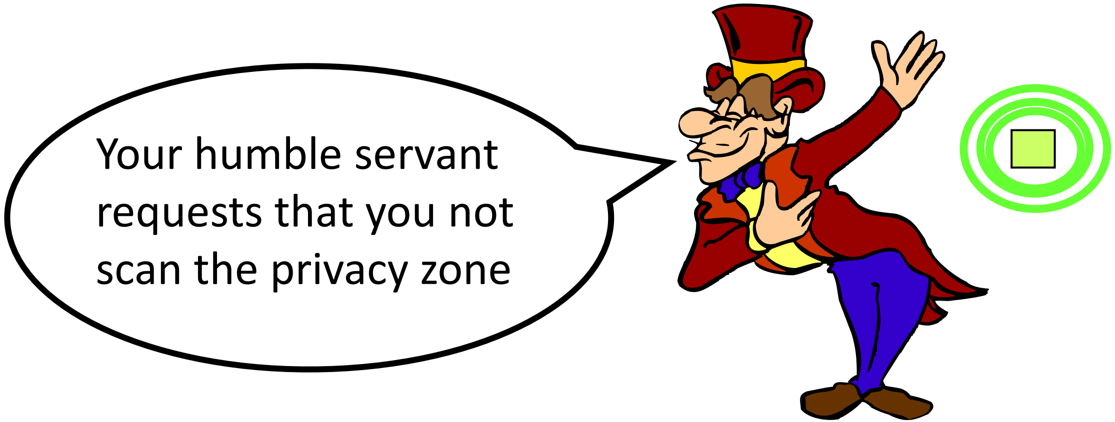
Blocking with Privacy Zones



Transfer to privacy zone on purchase of item

Polite Blocking

- We want reader to scan privacy zone when blocker is not present
  - Aim of blocker is to keep functionality active – when desired by owner
- But if reader attempts to scan when blocker is present, it will stall!
- Polite blocking: Blocker informs reader of its presence



More about Blocker Tags

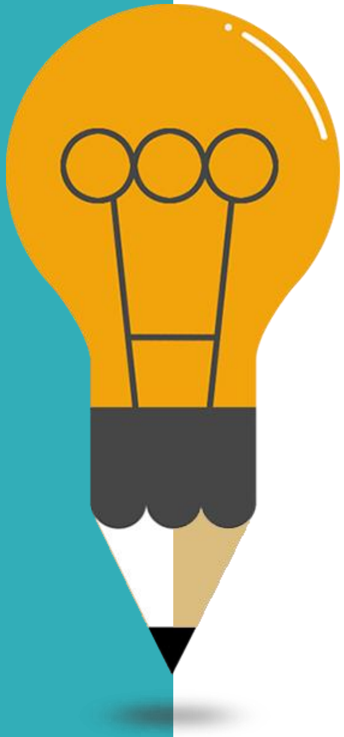
- Blocker tag can be cheap
  - Essentially just a ‘yes’ tag and ‘no’ tag with a little extra logic
  - Can be embedded in shopping bags, etc.
- With multiple privacy zones, sophisticated, e.g., graduated policies are possible

An Example: The R$_X$A Pharmacy

RFID-Tagged Bottle + “Blocker” Bag

RFID-Tagged Bottle + “Blocker” Bag

Outline



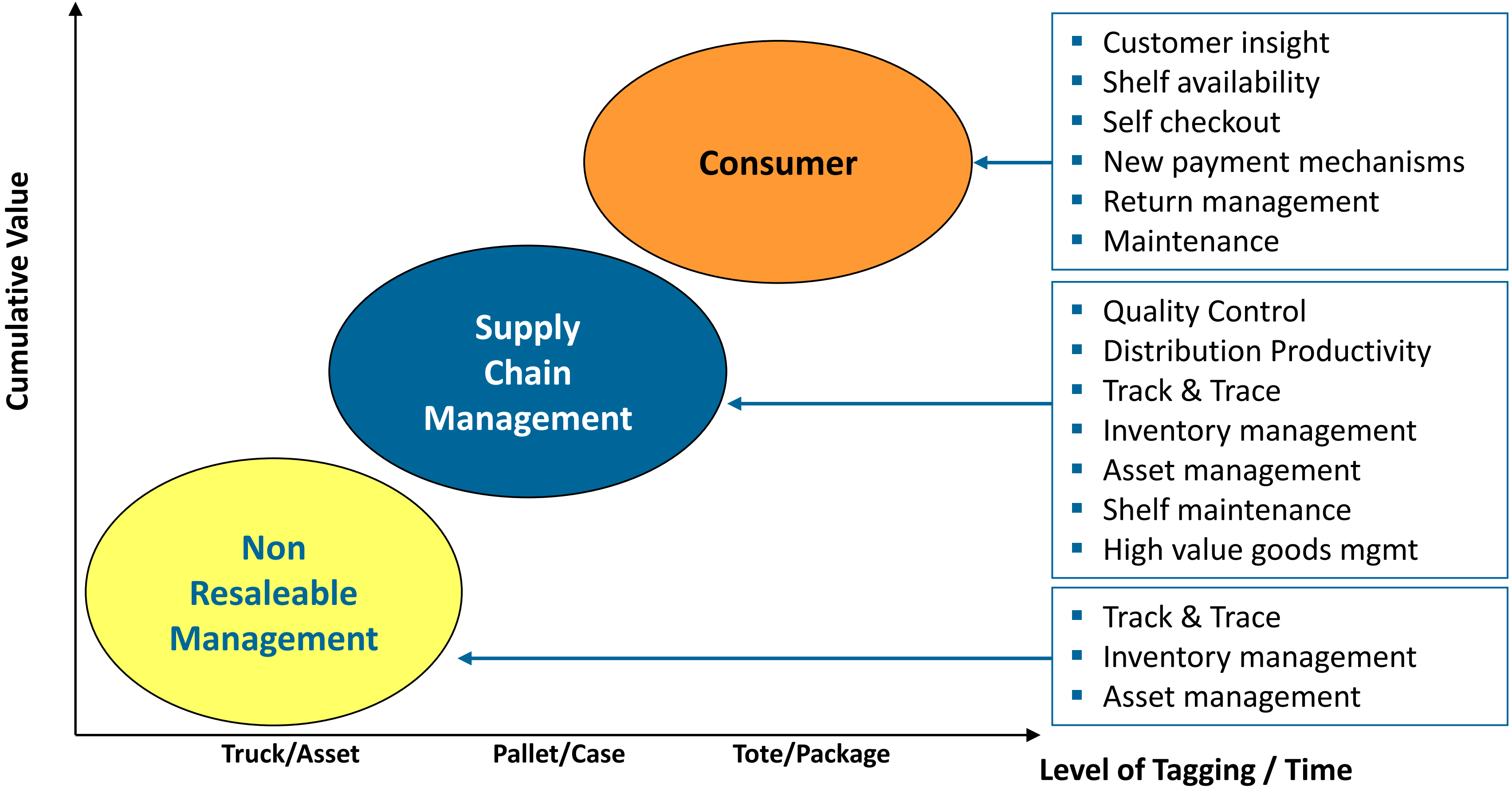
01 Overview of RFID
Reader-Tag; Potential applications

02 RFID Technology Internals
RF communications
Reader/Tag protocols
Middleware architecture

03 Security and Privacy

04 Conclusion

Business Implications of RFID Tagging



RFID Deployment Challenges

- Manage System costs
  - Choose the right hardware
  - Choose the right integration path
  - Choose the right data infrastructure
- Handle Material matters
  - RF Tagging of produced objects
  - Designing layouts for RF Interrogators
- Tag Identification Scheme Incompatibilities
  - Which standard to follow?

- Operating Frequency Variances
  - Low Frequency or High Frequency or Ultra High Frequency
- Business Process Redesign
  - New processes will be introduced
  - Existing processes will be re-defined
  - Training of HR
- Cost-ROI sharing

Getting Ready for RFID

- Identify business process impacts
  - Inventory control (across the supply chain)
  - Manufacturing assembly
- Determine optimal RFID configuration
  - Where am I going to tag my components/products?
    - Surfaces, metal environment and handling issues
  - Where am I going to place the readers?
    - Moving from the lab environment to the manufacturing or distribution center can be tricky
  - When am I going to assemble the RFID data?
- Integrate with ERP and other systems

RFID Services Value Chain

Strategy/ Consulting	Hardware	Middleware/ Device Mgmt	EPC Network Services	Data & Information Management	Enterprise Application Integration	Business Applications
System Integration and Solution Delivery						
• Business Process Integration • Solution Framework • Network Setup • RF aspects	• Tags • Readers • Label Printers	• Event Monitoring • Data filtering • Reader coordination • Policy Management	• Directory Services • Discovery Services • Authorization/ Authentication Framework	• Product Catalog and Attribute Management • Data Synchronization	• ETL Services • Legacy Application Integration	• Supply Chain Execution • ERP • Warehouse Management • Store Management • Distribution Management

RFID: The Complete Picture

- Technology which today is still more expensive than barcode
- Lost of efforts made around the price of the tag which is the tip of the iceberg
- What else need to be considered when one want to deploy a RFID system?

- Identifying Read Points
- Installation & RF Tuning
- RFID Middleware
- Connectors & Integration
- Process Changes
- Cross Supply-Chain View

RFID Summary

Strengths	Weaknesses
➢ Advanced technology ➢ Easy to use ➢ High memory capacity ➢ Small size	➢ Lack of industry and application standards ➢ High cost per unit and high RFID system integration costs ➢ Weak market understanding of the benefits of RFID technology
Opportunities	**Threats**
➢ Could replace the bar code ➢ End-user demand for RFID systems is increasing ➢ Huge market potential in many businesses	➢ Ethical threats concerning privacy life ➢ Highly fragmented competitive environment

Some Links

- http://www.epcglobalinc.com/
- http://www.rfidjournal.com/
- http://rfidprivacy.com/
- http://www.rfidinc.com/
- http://www.buyrfid.com/

End of This Chapter