RFID Technology and Applications

Anthony Quattrone

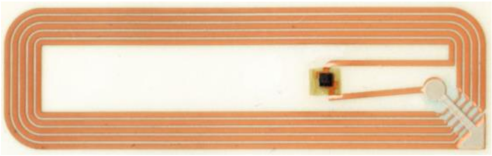
History of RFID Tags

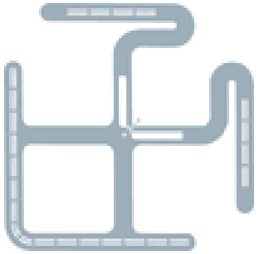
- **Radar**
  - To warn of aircrafts
  - Could detect only presence of an aircraft
  - No friend or foe distinction
- **First active RFID System**
  - Watson-Watt: first active identify friend or foe (IFF) system
  - Each aircraft had a transmitter
  - After transmitter received a radar signal it broadcast a signal back identifying an aircraft as friendly

Source: http://www.rfidjournal.com/article/articleview/1338/1/129/

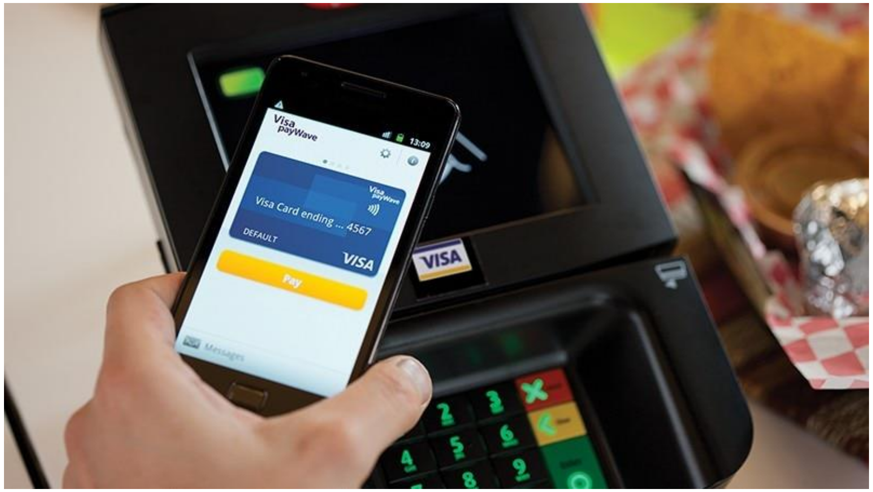
RFID Technology I

- **Tag**
  - Microchip connected to an antenna
  - Can be passive, semi-passive, active
  - No battery: passive
  - Semi-passive: circuit is battery-powered except communication
  - Promiscuous (true for most) or secure
  - Interrogate/query tags via radio signals
- **Reader**
  - Interrogate/query tags via radio signals





RFID Technology I

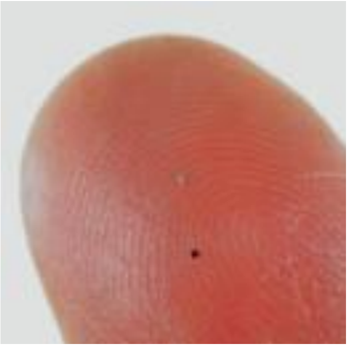


RFID Technology

- **RFID (radio frequency identification)**
  - Reader (base station) sends a radio interrogation signal
  - RFID tag backscatters its ID
  - Proximity-based technology: determine the tag location by measuring the signal's time of flight (in theory)
- **Characteristics**
  - No line-of sight necessary (in contrast to barcodes)
  - Resist environmental conditions: frost, heat, dirt, …
  - RFID tags with read & write memory (nonvolatile EEPROM)
  - Smartcard functionality (JavaCard): cryptographic computations for personal contact cards

Passive RFIDs

- **Operation**
  - Do not need an internal power source
  - Operating power is supplied by the reader
  - Electrical current induced in the tag's antenna by the radio signal pulse of the reader
- **Features**
  - Can be used for distances of up to 3 meters
  - Can be very small: 0.15 mm × 0.15 mm, 7.7μm thick (RFID powder, mu-chip from Hitachi)
  - Very cheap (a few cents)



Active RFIDs

- **Operation**
  - Own power source (battery life expectancy: up to 10 years)
- **Features**
  - Cost: a few dollars
  - Size: as small as a small coin
  - Support read ranges up to 100 meters
  - Deployment in more difficult RF situations (water)
  - Tags have typically a higher scanning reliability
  - Combination with sensors (vibration, light, humidity, …)

RFID: Technical Features

- **Data rate**
  - 9.6 –115 kbit/s
- **Devices**
  - Reader: simultaneous detection of up to 256 tags, scanning of up to 40 tags per second
  - Response time of an RFID tag: less than 100 milliseconds
- **IDs**
  - Typically 64 or 96 bit (up to 128 bit)

Source: http://www.andrew.cmu.edu/user/cjs/tech.html

RFID Frequencies

- **LF: low frequency (125 – 134.2 kHz, 140 – 148.5 kHz)**
  - Good penetration of materials including water and metal
  - Widely adopted (and used longer than HF)
  - No collision protocol available (see later)
  - Typical read range: 30cm
- **HF: high frequency (13.56 MHz)**
  - Provides anti-collision protocols
  - Up to 1m read range
- **UHF: ultra-high frequency (868 – 928 MHz)**
  - Difficult to penetrate of water and metal (similar to light)
  - Read range: up to 3m
- **Microwave: 2.4 – 5.8 GHz or UWB: 3.1 – 10 GHz**
  - Read range: up to 2m (projected up to 200m for UWB)
  - High data rate

Short RFID Discussion

- **Advantages**
  - Very cheap, high volume, large variety
  - Long industry experience
  - Scanning even with high speeds possible (300km/h)
  - No maintenance, simple to manage
- **Disadvantages**
  - No quality of service
  - Only passive data acquisition (asymmetric communication)
  - Possible interference with ISM bands

The EPC (Electronic Product Code)

- **Code**
  - Created by Auto-ID center
  - Successor of universal product codes (12 digit barcodes)
  - Unique number to identify an item in the supply chain
  - Specifies manufacturer, product category, item
- **96 bits: 22.114DDA2.1888A8.123ABC45D**

Header	EPC Manager	Object Class	Serial Number
8 bit	28 bit	24 bit	36 bit
64 or 96 bits	> 268 million manufacturers	> 16 million product categories	<68 billion items

EPC Device Classes

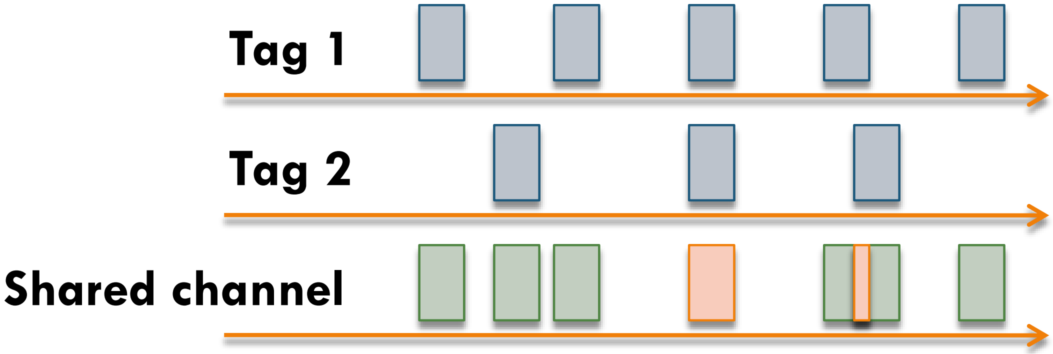
EPC Device Class	Definition	Programming
Class 0	“Read only” passive tags	Programmed by the manufacturer
Class 1	“Write-once read-many” passive tags	Programmed by the customer; cannot be reprogrammed
Class 2	Rewritable passive tags	Reprogrammable
Class 3	Semi-passive tags	Reprogrammable
Class 4	Active tags	Reprogrammable
Class 5	Readers	Reprogrammable

Anti-Collision & Singulation

- **Problem**
  - RFID tags are simple and cannot communicate with other tags
  - High probability that two tags in communication range respond simultaneously
  - Collision: response on the same frequency at the same time
- **Anti-collision and singulation protocols**
  - Algorithms to identify all tags
  - Anti-collision: trade time for the possibility to interrogate all tags
  - Singulation: identify (iterate through) individual tags

ALOHA Protocol

- **Simple idea**
  - Based on the classical ALOHA protocol (Abramson, 1970)
  - “Tag-Talks-First” behavior: tag automatically sends its ID (and data) if it enters a power field
  - If a message collides with another transmission, try resending it later after a random period
- **Collision types**
  - Partial & complete



Reducing Collisions in ALOHA

- **Switch-off**
  - After a successful transmission a tag enters the quiet state
- **Slow down**
  - Reduce the frequency of tag responses
- **Carrier sense**
  - No carrier sense possible (tags cannot hear each other)
  - Use ACK signal of the reader in communication with another tag
  - Reader broadcasts a MUTE command to other tags if it interrogates one tag

Slotted ALOHA protocol

- **Frame vulnerability**
  - Partial overlap leads to maximum throughput of a 18.4% (assuming a Poisson distribution)
- **Slotted ALOHA**
  - “Reader-Talks-First”: use discrete timeslots SOF (start-of-frame) and EOF (end-of-frame)
  - A tag can send only at the beginning of a timeslot
  - Leads to complete or no collision
  - Increased maximum throughput of 36.8%
  - “Early end”: reader sends out an early EOF

Discussion

- **Frame-slotted ALOHA**
  - Group several slots into frames
  - Only one tag transmission per frame
  - Limits frequently responding tags
  - Adaptive version: adjust the number of slots per frame

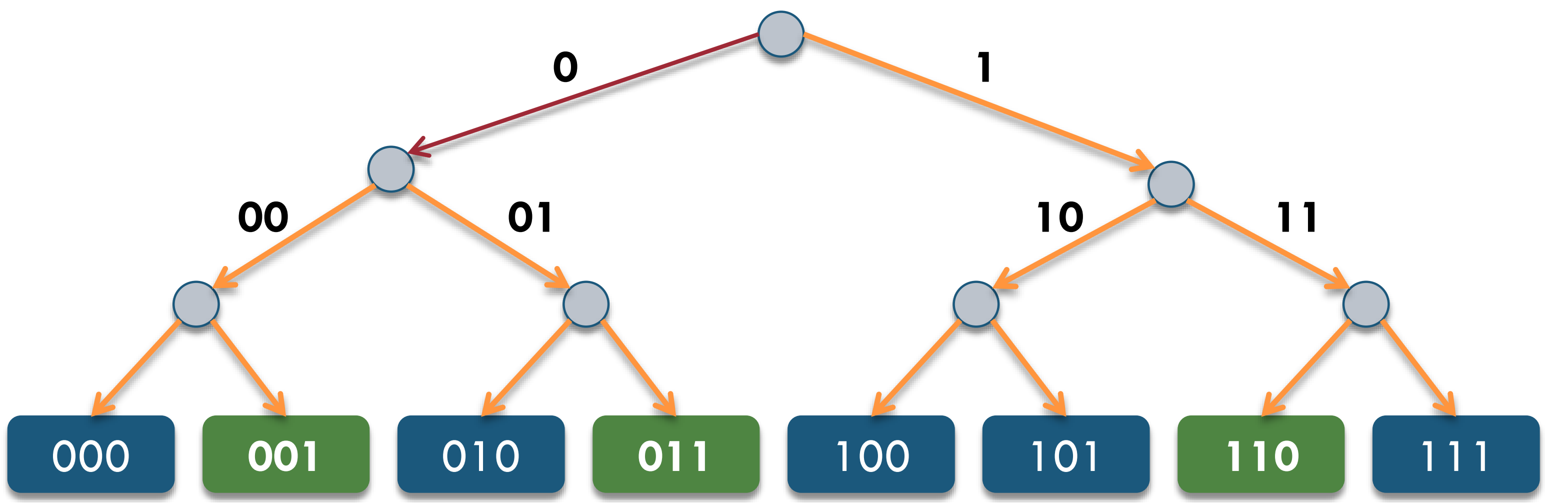
Protocol	+	-
ALOHA	Adapts quickly to changing numbers of tags Simple reader design	Worst case: never finishes Small throughput
Slotted ALOHA	Doubles throughput	Requires synchronization Tags have to count slots
Frame-slotted ALOHA	Avoids frequently responding tags	Frame size has to be known or transmitted; similar to slotted ALOHA

Binary Tree Protocol I

- **Tree traversal algorithm (depth first search)**
  - “Reader-Talks-First” behavior: reader broadcasts a request command with an ID as a parameter
  - A sub-tree T is searched by an identifier prefix
  - Only tags with an ID lower or equal respond
  - An interrogated tag is instructed to keep quiet afterward
  - Repeat algorithm until no collision occurs or all tags are quiet

Binary Tree Protocol II

- Each sub-tree T corresponds to an identifier prefix
- Reader searches T by sending prefix, interrogating tags for their next bit
  - If all “0” search Left(T)
  - If all “1” search Right(T)
  - If both “0” and “1” search Left(T) and Right(T)



RFID Applications I

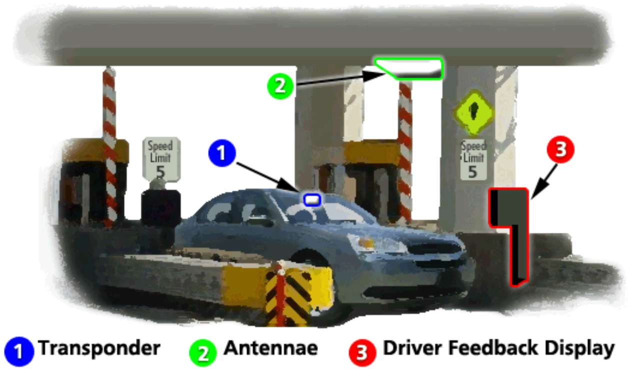
- **E-passports**
  - Biometric passports from the UK & USA with RFID tags
  - Metal lining should prevent access if passport is closed

- **Transportation payment**
  - Moscow metro introduced RFID smartcards in 1998
  - NY city runs a trial for their subway system
  - Octopus card in Honk Kong since 1997; now used as “cash card”
  - Transperth (public transport system) in Perth using MIFARE from Philips

Source: http://www.passport.gov.uk/general_biometrics.asp

RFID Applications II

- Electronic toll collection
  - California: FasTrak
  - Eastern states: E-ZPass



- Vehicles
  - RFIDs in car keys for as theft protection
  - Smart key/smart start from Toyota: car acknowledges the key's presence within 3 feet
  - RFIDs in tires (Michelin)

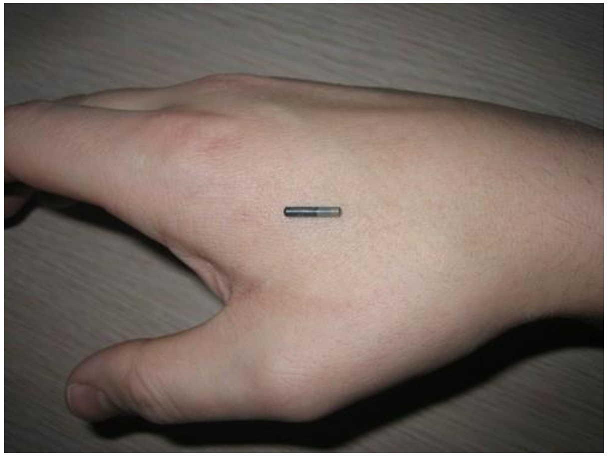
Source: http://www.bayareafastrak.org/static/about/howit.shtml

RFID Applications III

- **Supply chain & inventory management**
  - Potentially the largest impact for RFID in the next decade
  - Wal-Mart requires top 100 suppliers to deploy RFID at pallet level by 2005
  - Gillette announced order for 500,000,000 RFID tags (Infoworld Feb 2003)
- **Prevention**
  - Lost containers, counterfeits, gray market products
  - Prevent shoplifting (alert suspicious removal of large quantities)
  - Detect misplaced items and improve inventory level despite shoplifting

RFID Applications IV

- **Product tracking**
  - Cattle identification (Canada, USA)
  - Poultry movements (bird flu)
  - Baggage tracking, containers, pallets, …
  - American Express Blue credit card (payment)
  - Books, CDs, DVDs, …
- **Human implants**
  - Payment (VIP Baja Beach Club in Barcelona, Spain)
  - Patient identification, e.g., Alzheimer's



Source: http://www.amal.net/rfid.html

Summary of RFID Applications

- **Alerting**
  - Payment: RFID smartcards and electronic toll collection
  - Security risk: denial of service
- **Authentication**
  - E-passport and car immobilizers
  - Security risk: forgery
- **Identification**
  - Like barcodes but more data and faster to process
  - Privacy risk: sniffing
- **Monitoring**
  - Product tracking and inventory management
  - Privacy risk: tracking

Status Quo of RFID Systems

- **No authentication**
  - Readers are blind: if tag does not reply, reader does not know about it
  - Tags are promiscuous and reply to any reader
- **No access control**
  - Malicious reader can link to a tag
  - Malicious tag can spoof a reader
- **No encryption**
  - Eavesdropping possible (especially for the reader)
- **Man-in-the-middle attack**

Privacy Concerns

- **Unauthorized surveillance**
  - Simple RFID tags support no security mechanisms
  - Permanent RFID serial numbers can compromise privacy (RFID tag remains intact even after disposal of goods)
- **Potential risks**
  - Tags in goods might be a potential risk (high gain antennas allow RFID scanning over larger distances
  - Threat: scanning of assets of high value

RFID Tag Privacy I

- **Killing: tag deactivation**
  - Kill a tag permanently (kill command + password)
  - Part of EPCGlobal/AutoID standard
  - No future use: return defective goods, recycling, airline tickets, stamps, …
- **User intervention**
  - User presses a button on a tag to authorize scanning
  - Assumes user can identify a rogue scanner
  - No protection against passive eavesdropping

RFID Tag Privacy II

- **Silencing: metal lining**
  - Faraday cage that is not penetrable by radio signals
  - Cheap and effective (tin foil)
  - Only works for small items but not for clothing, human implants, …

DIFRwear:
RFID Blocking Passport Case

RFID Tag Privacy III

- **Active jamming**
  - Device that broadcasts radio signals to block/disrupt RFID
  - Sledgehammer approach could cause disruptions
- **Hash-locking**
  - Lock a tag so that it refuses to reveal its ID until it is unlocked
  - Locked with a meta ID y
  - Unlocked by presentation of a key x such that $y = h(x)$ for a standard one-way hash function h
  - Practical solution for more than a small number tags?
  - Expensive since cryptographic operations are required

RFID Tag Privacy IV

- **Encrypting: silent tree walking**
  - A reader is much easier to eavesdrop than a tag
  - However: tree walking relies on broadcasts from the reader
  - Encrypt readers transmission: a passive eavesdropper cannot infer the tag IDs
  - Expensive since cryptographic operations are required
- **One time identifiers (pseudonym rotation)**
  - Set of cryptographically unlinkable pseudonyms is computed by a trusted verifier
  - A small number of pseudonyms stored on tag
  - Tag cycles through pseudonyms

RFID Tag Privacy V

- **Hiding: blocker tags**
  - A blocker tag carried by a consumer simulates the full spectrum of possible serial numbers for tags
  - A blocker tag forces a reader to sweep the very large space of all possible tag identifiers
  - When a reader queries tags in a sub-tree, the blocker tag simultaneously broadcasts a 0 and 1 bit
  - 2^k possible reads; if k is large the reader stalls
  - Works only for tree-based scanning algorithms
  - Selective blocker tags enable
    - Privacy zones (block a certain range of RFID tags) for graded policies
    - Zone mobility (shopping and checkout)

RFID Tag Privacy VI

- **Keyless “Encryption”**
  - Delay, not Deny!
  - A tag carries multiple, random-looking IDs
  - Only a valid verifier can determine if two IDs belong to the same tag
  - Disclose one ID at a time with a slow rate
- **Effective against sniffing and tracking**
  - Only owner knows IDs (no sniffing)
  - ID changes often (hard to track, big gaps)
- **Effectiveness drops sharply with more items**
  - An adversary could query a tag multiple times to harvest all names
  - Solution: authorized readers can refresh pseudonyms

RFID Tag Privacy VII

- **Shamir tags: Unknown tags take long time to read**
  - Bitwise release (e.g., one random bit/sec)
  - Intermediate results meaningless (encryption)
  - Decryption requires all bits being read
- **Impedes tracking & unauthorized identification**
  - Known tags can be directly identified
  - Initial partial release of bits enough for identification from a limit set of known tags
  - Allows owner to use tags without delays or restrictions

RFID Tag Authenticity

- **Threats**
  - Cloning: copying existing tags
  - Forgery: creating new tags with a valid identity
  - Relabeling
- **Track & trace**
  - Application anticipates tag movements, detects and reports anomalies and duplicates
  - Protection for both threats but only with hindsight

Tag Authenticity Approaches I

- **Static authentication**
  - Tag identifier includes a digital signature
  - Protects against forgery, but not cloning
- **Static authentication with public-key protocol**
  - Tag authenticates reader by public-key protocol
  - Encrypts digital signature with reader’s public key

Tag Authenticity Approaches II

- **Pseudonym tag with mutual authentication**
  - Tag presents one-time identifier
  - Reader sends corresponding one-time PIN
  - Tag returns its own one-time PIN for authenticity
  - Protection against both threats if enough identifiers
- **But: key exchange**
  - Reader must know password
  - A single password is a bad password
  - If more passwords: reader needs to know which tag it is!
- **Solution?**
  - Reader checks many passwords
  - How does the reader know about the passwords (e.g., world-wide deployment?

RFID Security Schemes

- **Rolling code schemes (cheap)**
  - Common pseudo-random number generator in transmitter and receiver to produce a sequence
  - Transmitter sends code in sequence
  - Receiver compares this code to its calculated code
  - Implementation compares within the next *n* codes
- **Challenge-response protocols (expensive)**
  - Secret information is never communicated insecurely
  - Reader issues a challenge to the tag
  - Tag responds with a cryptographic encoding using a key

RFID "Bill of Rights"

- **Consumers should have the right**
  - To know whether products contain RFID tags
  - To have RFID tags removed or deactivated when they purchase products
  - To use RFID-enabled services without RFID tags
  - To access an RFID tag's stored data
  - To know when, where and why the tags are being read

Source: http://www.technologyreview.com/read_article.aspx?id=12953&ch=infotech

RFID Future Directions

- **Super-distributed RFID infrastructures**
  - Massive number of tags are placed on an object
  - Redundancy: a single tag becomes insignificant
  - Leads to discretization of the world around us
- **Applications**
  - Indoor localization and positioning
  - Collaboration
  - Distributed storage of information

Large-Scale Deployments

- **Tagging every (!) item**
  - Enables continuously tracking and monitoring of RFID-enabled items
- **Super-distributed RFID infrastructures**
  - Tagging objects such as walls, carpets, tables, … with a large number of RFID tags
  - Discretization of the world around us
  - Interaction, navigation, and self-localization based on RFID technology

Next-Generation Data Management

- **Challenge: vast amount of real-time data**
  - High-entropy, infinite stream of RFID data and updates
  - Possibly paired with sensed information (e.g., temperature)
- **Research themes**
  - Stream management techniques
  - Search engines for real-time RFID data
  - Data mining of RFID information
  - Localization based on RFID information

Next-Generation Applications

- **RFID-enabled object management systems**
  - Identifying misplaced items in libraries and shops in real-time
- **Pervasive computing environments**
  - Combination of mobile computing devices with wireless networks, local and global positioning, and large-scale deployments of RFID tags
  - Example: Active “Where am I”
  - Example: “Where can I park my car and have a quiet (available) seat for a cup of coffee right now?”
- **RFID-enabled spatial data management systems**
  - Indoor position technology whose spatial resolution can be tailored to the application domain

RFID Technology: Literature

- **Further reading**
  - Tuttle, J. (1997). Traditional and emerging technologies and applications in the radiofrequency identification (RFID) industry, In *Radio Frequency Integrated Circuits (RFIC) Symposium, IEEE*, 5 – 8.
  - Juels, A.; Rivest, R. & Szydlo, M. (2003). The blocker tag: selective blocking of RFID tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on computer and communications security, ACM Press*, 103 – 111.
  - Bohn, J. & Mattern, F. (2004). Super-Distributed RFID Tag Infrastructures. In *Proc. 2nd European Symp. on Ambient Intelligence (EUSAI 2004)*, Springer, Vol. 3295, 1 – 12.
  - Garfinkel, S. & Holtzman, H. (2005). Understanding RFID Technology. In Garfinkel, S. & Rosenberg, B. *(eds.), RFID: Applications, Security, and Privacy*, *Addison Wesley*, 15 – 36.
  - Bohn, J. (2006). Prototypical Implementation of Location-Aware Services Based on Super-Distributed RFID Tags In *Proceedings of the 19th International Conference on Architecture of Computing Systems (ARCS’06)*, Springer, Vol. 3894, 69 – 83.

Autonomous Navigation

Autonomous Navigation I

- **Where am I?**
  - Determine initial location
  - Determine initial orientation
- **How do I get there?**
  - Path planning
  - Computation of a path leading from the start to the destination
- **Did I reach my destination?**
  - Identification of the goal location

Autonomous Navigation II

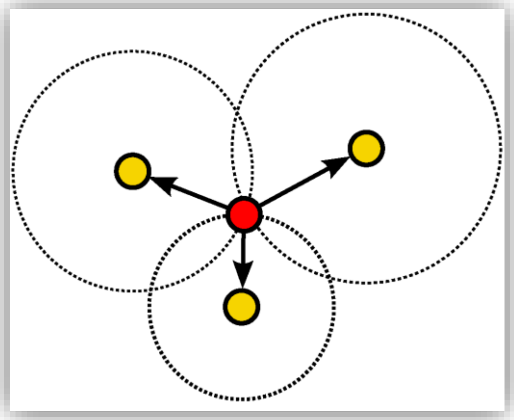
- **How do I monitor progress?**
  - Where am I relative to the start and destination?
  - Am I still on the pre-computed path?
- **How do I adapt to changes in the environment?**
  - How do I recognize new obstacles?
  - How do I make new plans?
- **How do I interact with the environment?**
  - Navigation is often only a subtask of a more complex task such as getting an item

Indoor Localization

- **Status quo**
  - GPS does not work indoors
  - No single (dominant) indoor positioning technology
- **Challenges**
  - Low cost
  - High precision and accuracy
  - Easy deployment
  - Scalability

Indoor Location Sensing Techniques I

- **Triangulation**
  - Lateration: distance measurements
  - Direct & time of flight
  - Attenuation
  - Angulation: angle measurements



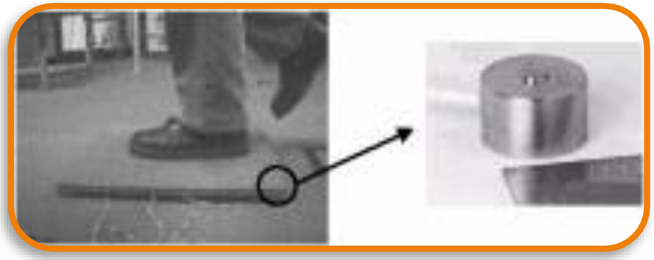
- **AT&T's Active Bat**
  - Based on ultrasound
  - Time-of-flight lateration technique
  - Precision: 9 cm for 95 percent of the measurements

Indoor Location Sensing Techniques II

- **Scene analysis**
  - Observe the surrounding scenery: map creation and updates
  - Static (database) & differential
  - Problems if the scenery changes
- **RADAR (Microsoft)**
  - Sample signal strength at different locations
  - Determine the location whose sampled signal strength is closest to the observed signal strength
  - Accuracy: a few meters

Indoor Location Sensing Techniques III

- **Proximity**
  - Nearness to beacons or sensors
  - Physical contact pressure or touch sensors
  - Wireless cellular access points
  - RFID tags



- **Smart Floor**
  - Plates are equipped with pressure sensors
  - Precision depends on the number of tiles
  - Can identify individuals by unique pressure patterns

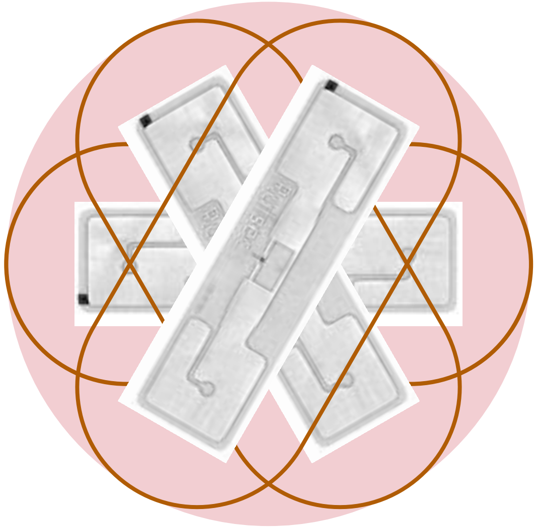
Discussion of Current Techniques

- **Triangulation**
  - Efficient but only as accurate as the distance (or angle) measurements
  - Dedicated infrastructure (expensive)
- **Scene analysis**
  - No dedicated infrastructure
  - Relies on a stable environment but cannot guarantee high accuracy
- **Proximity**
  - Can be very robust but is often imprecise

Our Approach

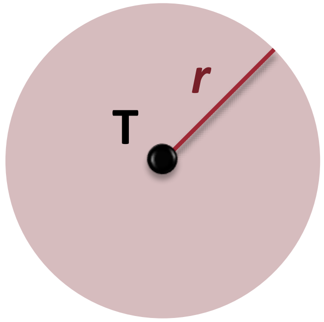
- **Design goals**
  - No initial discovery or external map of the environment necessary
  - Efficient updates of the environment such as new obstacles
- **RFID**
  - Tag-based space partitions
  - On-demand interaction with the environment as tag IDs can indicate different roles
  - High accuracy combined with a minimum number of tags
  - Uses a single sensor, the RFID reader

Interrogation Field of an RFID Tag

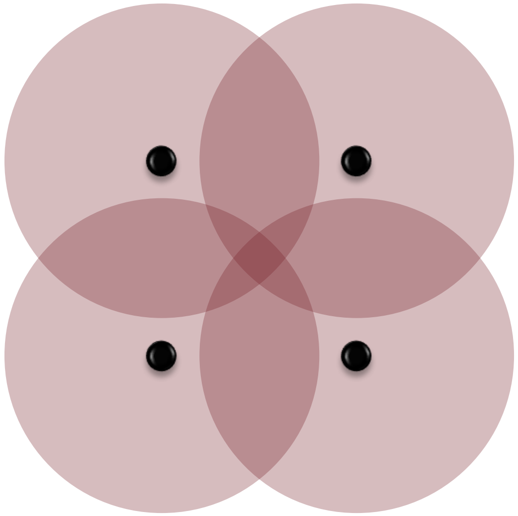


Space Partitions I

- **Read range**
  - The area in which a tag can be read can be approximated as a disc of its reading range r centred at T



- **Partition**
  - A partition is a non-empty region where one or more tags can be simultaneously detected by a reader

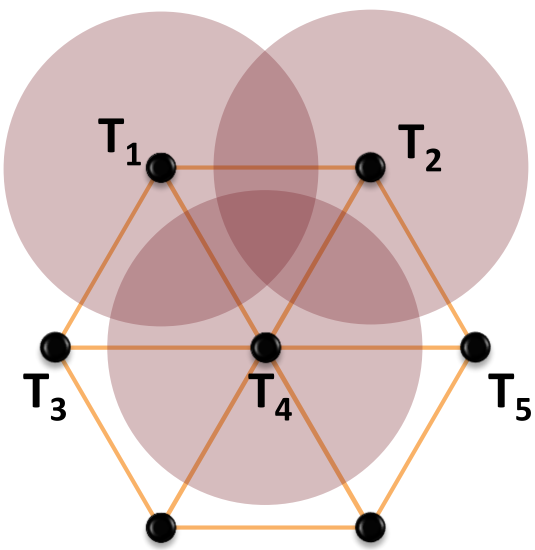


Space Partitions II

- **Problem**
  - Minimize the number of tags such that at least k tags are readable from every position
  - Instance of the circle covering problem for k = 1

- **Solution (Kershner)**
  - Tags are the vertices of an equilateral triangular network
  - Each triangle has sides of length:

$$r \times \sqrt{3}$$



Location Mapping

- **Problem**
  - Map a set of read IDs to a location
- **Solution: Maps?**
  - Map each ID to a location and compute an agent's position
  - Map creation violates our original goals
- **Solution: Coordinate systems**
  - Cartesian coordinate system requires decimal points
  - Not efficient to represent floating point numbers with short IDs: 2 * 32 bit = 64 bit

Triangular Coordinate System

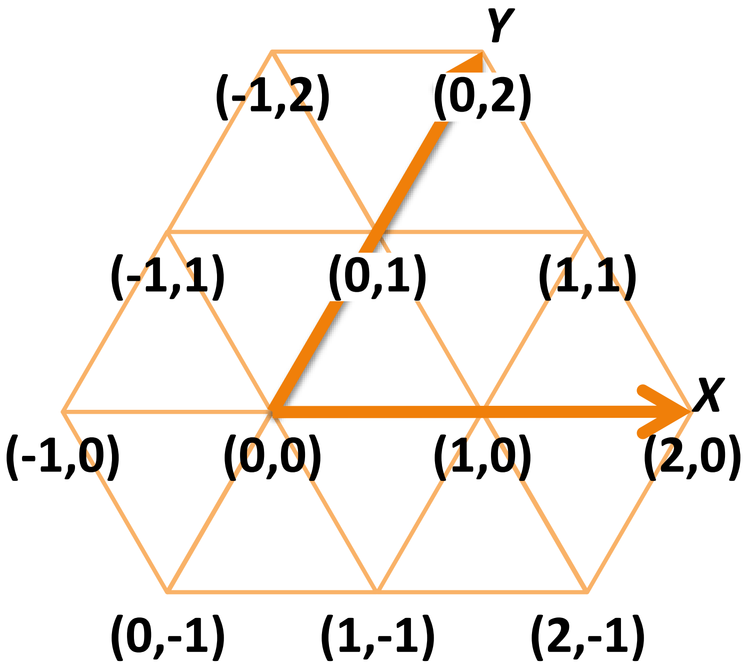
- **Transformation to Cartesian Coordinates**
  - Given triangular coordinates

$$(\hat{x}, \hat{y})$$

  - Cartesian coordinates

$$x = \hat{x}\left(\sqrt{3}r\right) + \hat{y}\frac{\left(\sqrt{3}r\right)}{2}$$

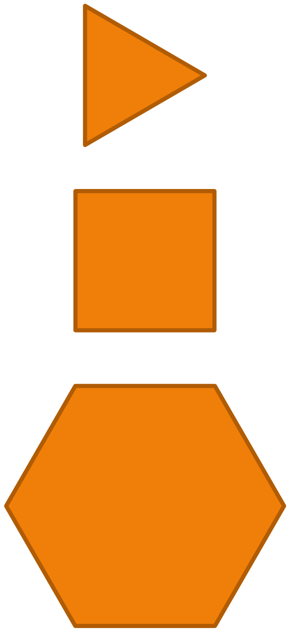
$$y = \hat{y}\left(\frac{3}{2}r\right)$$

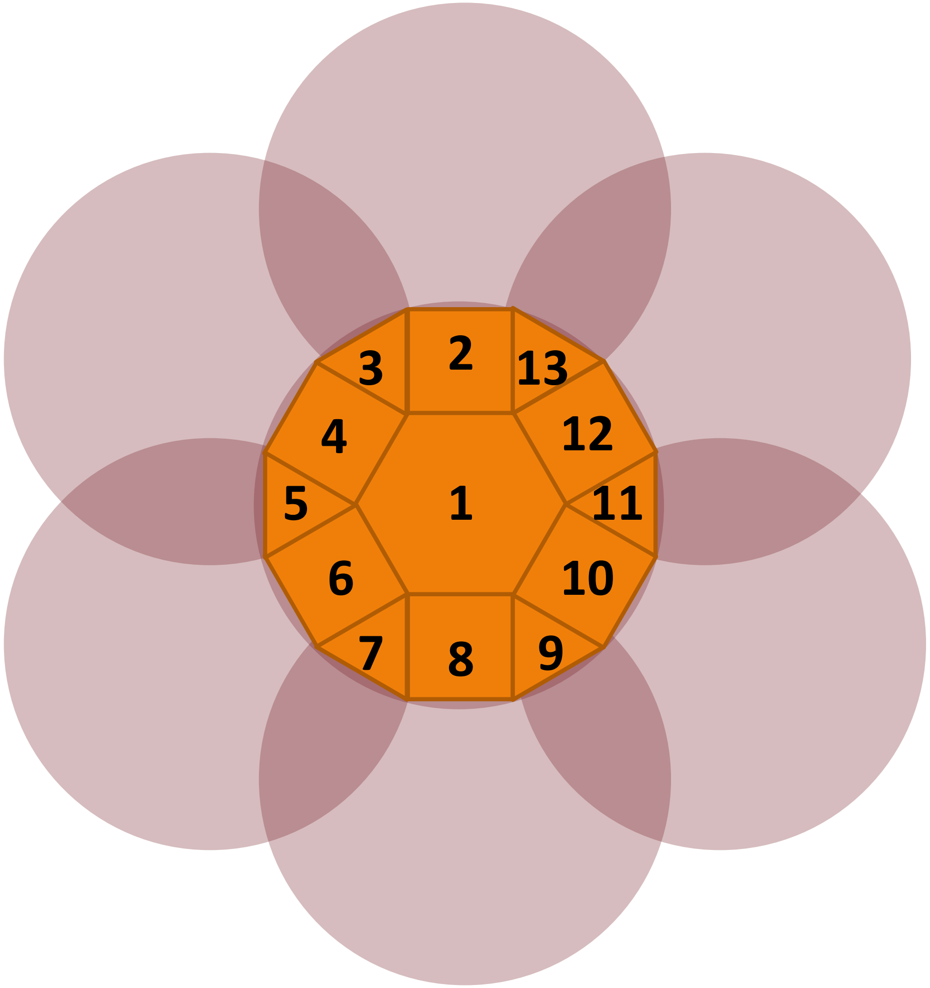


Start: Where am I?

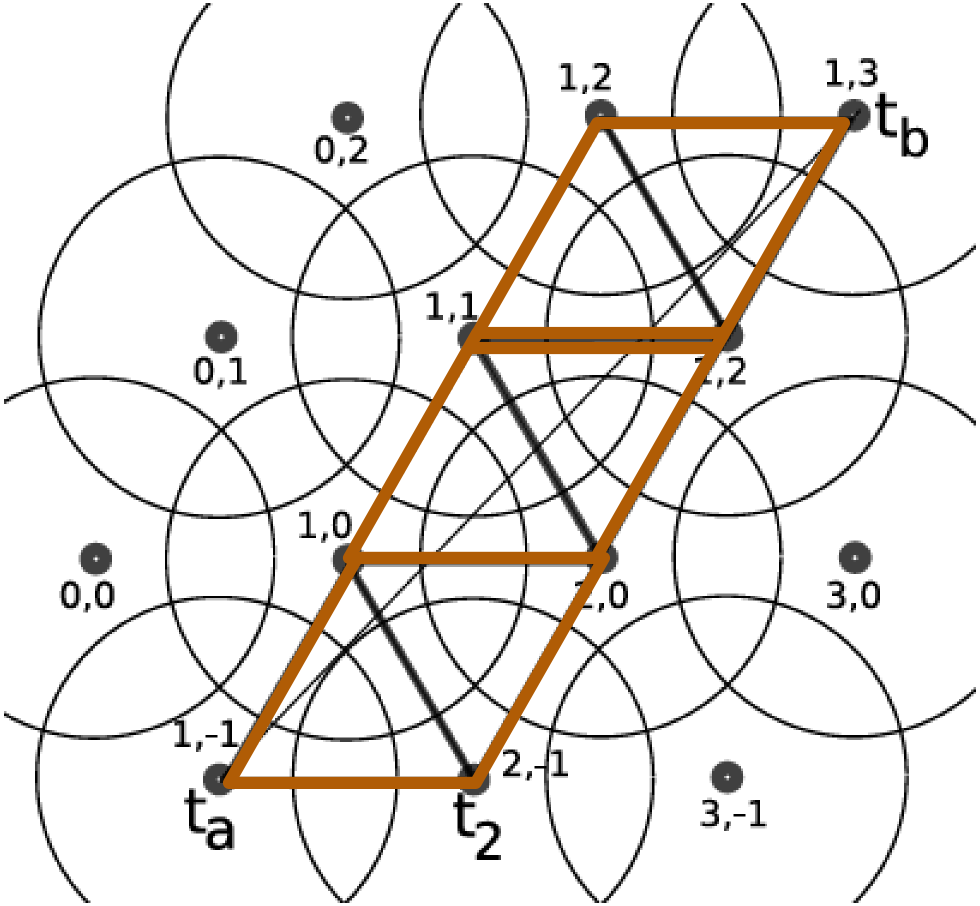
- **Location approximation**
  - Location = mean location of the tags forming a partition
- **Orientation approximation**
  - An agent moves on a straight line between successive partitions
  - Movement leads to a bound on the angle

Polygonal Representation of Partitions





Path Computation: How Do I Get There?



Monitoring Progress

- **Deviation**
  - Permanently scan partitions (tag IDs)
  - An agent encounters a partition that is not in the computed path
- **Recomputation**
  - Approximate orientation using the list of traversed partitions
  - Compute a new path to the destination
  - Rotate towards the destination
  - Start following the new path

Object Localization in Active Indoor Environments

Object Localization

- Detecting misplaced books in a library …

Using RFID as Binary Sensors

- **RFID antenna fields**
  - RFID reader is a binary sensor: detects presence or absence of a tag
  - However: no direct localization within the field is possible
  - Challenge: RFID technology is susceptible to noise and changes in the environment
  - Passive tags cannot help with computations

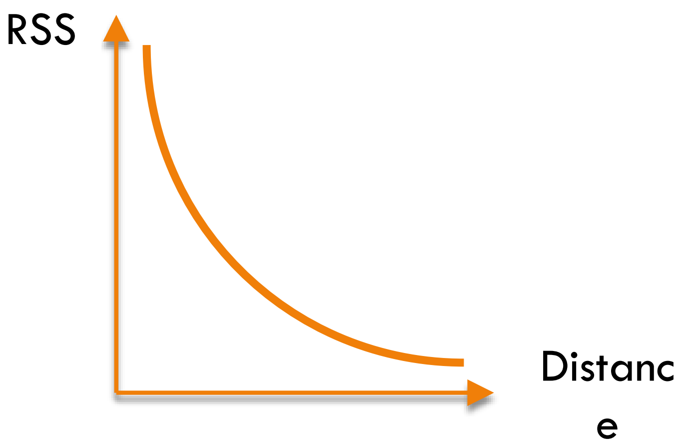
RSSI: Received Signal Strength Inverse

- **Path loss model**

$$P_{RX} = c \times \frac{P_{TX}}{d^{\alpha}}$$

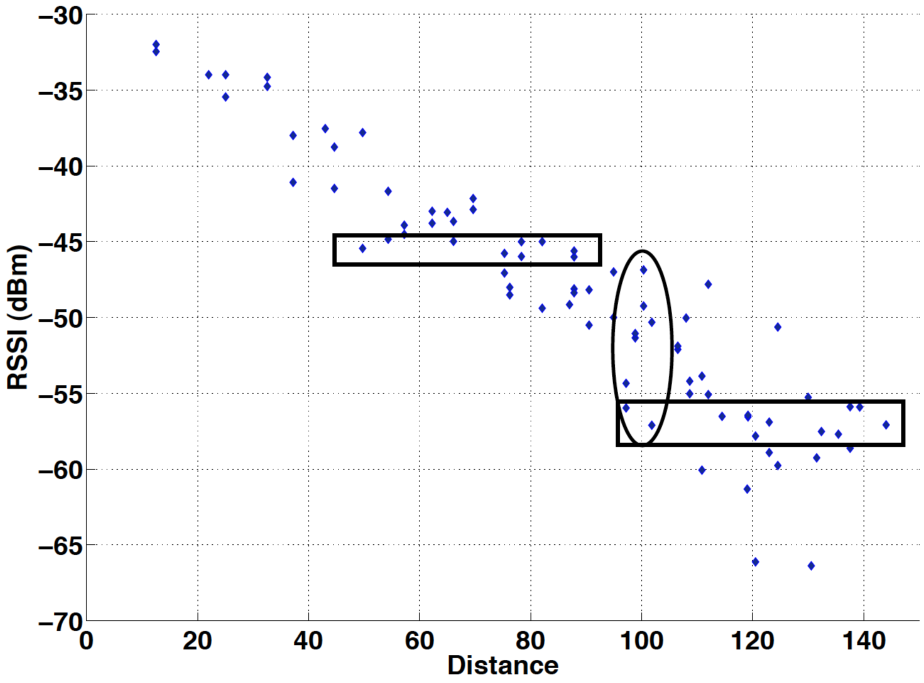
  - P_{TX} transmitted power, P_{RX} received power, d distance

- **Use RSSI?**
  - Measure RSSI for RFID tags
  - Simple but inaccurate range estimates due to fading, interference, position of antenna



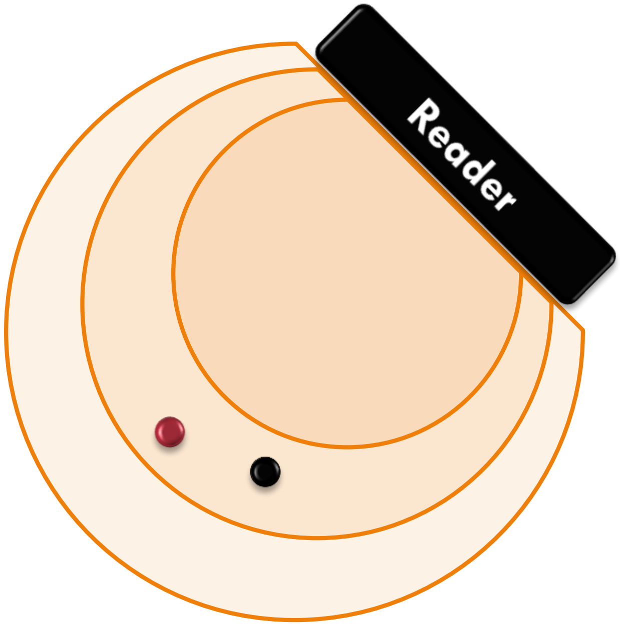
RSSI for RFID Tags

- **Problems**
  - Tags located at the same distance can have significantly different RSSI values (elliptical region)
  - Tags at different distances may receive same power (rectangles)



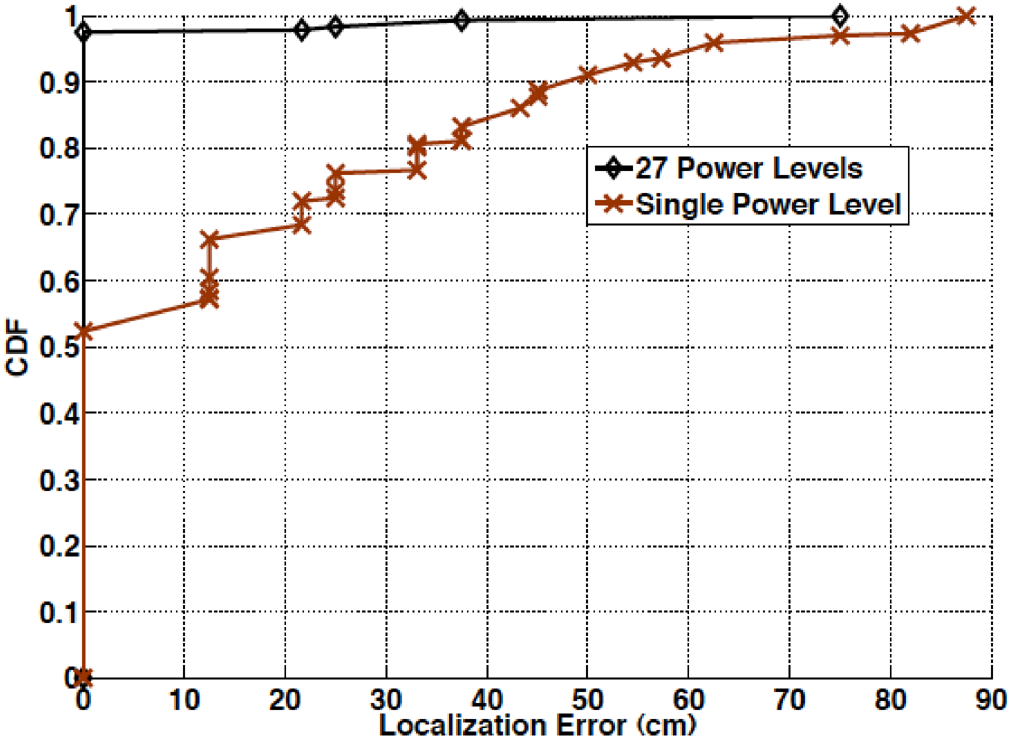
Use of Power Levels I

- **Antenna**
  - Can be powered up with different power levels
  - Each power level corresponds to an interrogation field
  - Each power level leads to a different RSSI
  - Use of reference tags (colored in red) to adjust to environment changes



Use of Power Levels II

- **Experiment using 27 power levels**
  - Cumulative distribution function (CDF) of the errors
  - Precision from 0 cm to 90 cm

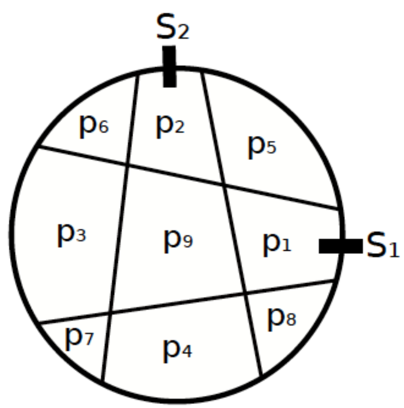


Setup

Motion Tracking Using RFID

Motion Tracking Using Binary Sensors

- **Purpose**
  - Track the movement of a user, e.g., the movement of an arm or an object using RFID tags
- **Computational approach**
  - Not every geometric region is unique
  - Approximate regions via sectors

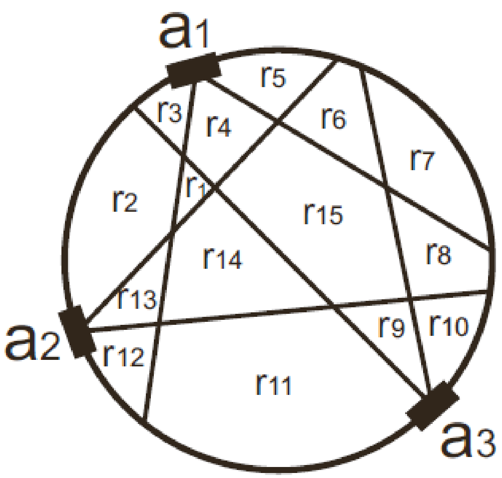


sensors	partition(s)
{}	p_5, p_6, p_7, p_8
$\{s_1\}$	p_1, p_3
$\{s_2\}$	p_2, p_4
$\{s_1, s_2\}$	p_9

- **Questions**
  - Total number of unique regions
  - Optimal number of equally sized regions

Motion Tracking using Binary Sensors

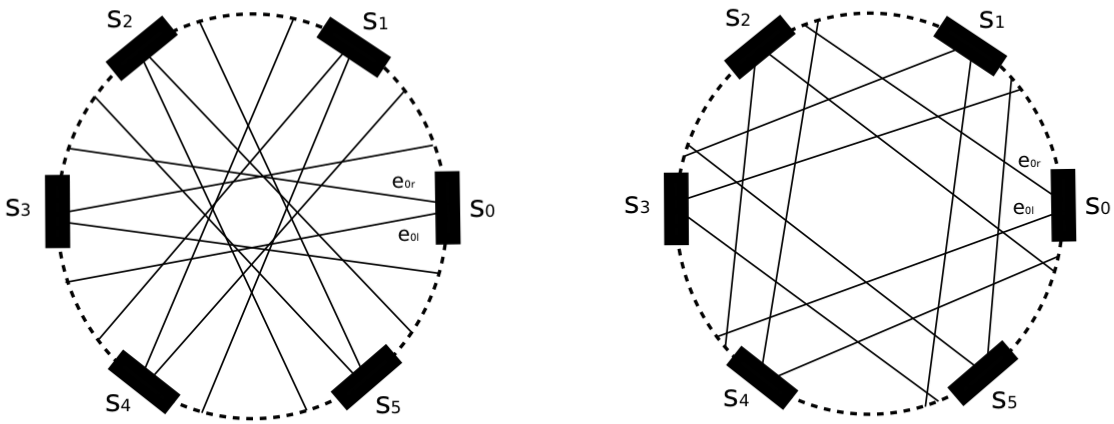
- **Approach**
  - Compute the number of unique regions for *n* antennas
  - Track movements of tags sets
- **Open question**
  - Optimal number of equally sized regions



Reg	ID
r1	100
r2	000
r3	001
r4	101
r5	001
r6	011
r7	010
r8	110
r9	101
r10	100
r11	100
r12	000
r13	010
r14	110
r15	111

RFID-enabled User Interfaces

- **Results**
  - General line arrangements: $n^2/2 + n/2 + 1$
  - Our case: $2n^2 + n + 1$, but some regions are not unique!
  - Upper bound for n sensors: $2n^2-3n+2$
- **Configurations**



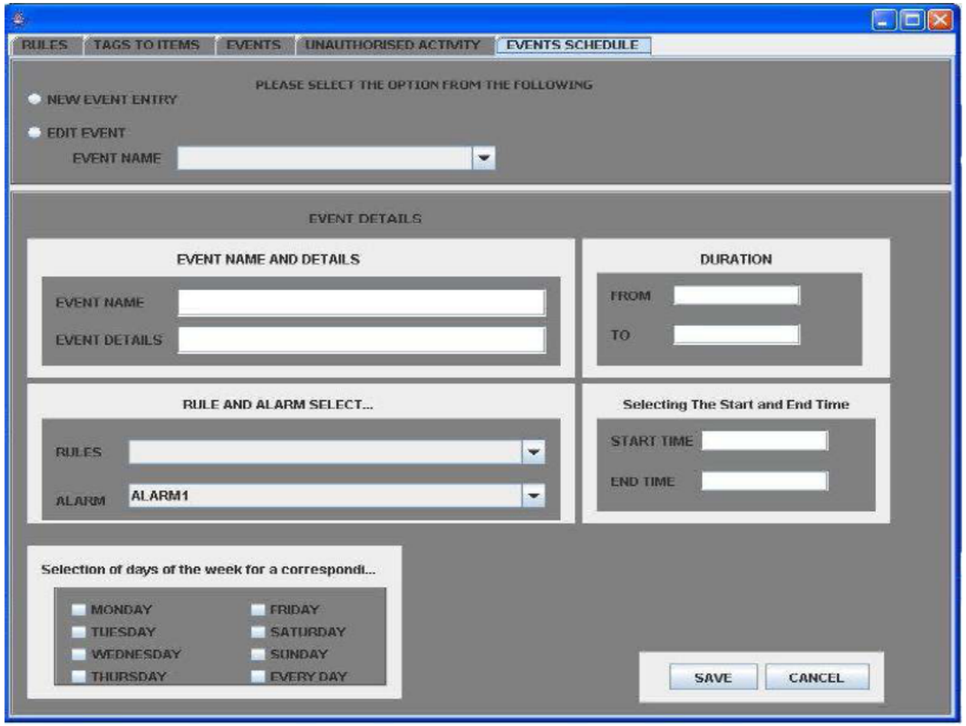
An "Active Reminder System" Using RFID

An Active Reminder System Using RFID

- **RFID**
  - Binary sensor (similar to infrared)
  - (Personal) objects have an ID (attached RFID tag)
- **Desired application areas**
  - Reminder system
  - Access control to rooms
  - Ability to remove items from a lab
- **Basic idea**
  - Item sets identify access and indicate whether items belong together

Active Reminder System

- **Schedule events**
  - Location, time, purpose
  - Set of items for a certain type of event
  - Example “lecture event”: wallet, laptop, mobile phone, laser pointer, pens



Experiments: Access Control

- **Scenario 1**
  - Two users want to access the door at the same time (from a lab, close to antenna)
    - Access not allowed (only if one tag is correctly identified)
- **Scenario 2**
  - Access from outside (shielding of door)
    - No major impact
- **Scenario 3**
  - A user carries some items for which he/she is not authorized
    - Immediately flagged, unless read errors

Experiments: Reminder System

- **Scenario 4**
  - A user carrying all or some items passes the door
    - Around 90% accuracy if items are not close body (bag)
    - Down to 65% accuracy if shielded by body (or in wallet)
- **Scenario 5**
  - Height of tag (tall user or tag under shoes)
    - Limits accuracy (3 antennas needed)
    - Tag placement on the ground does not work
    - Good if antenna is under the doormat and tag under sole
- **Our lesson**
  - Better to sense what is missing than what is passed through