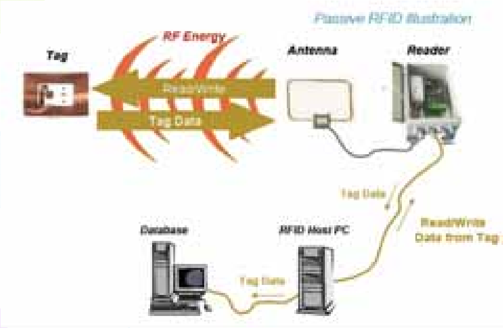
Introduction To RFID Anti-collision Protocols And Security Issues

林俊甫 NTU IM PHD Student

Agenda

- Background introduction
- Reader-tag communication protocols
- Security issues



Source from RFID security and privacy issues, Booz, Allan, Hamilton, 2005 Mid-Atlantic Logistics Conference

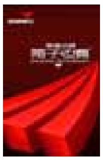
RFID Components

- Reader (transceiver)
- Tag (transponder)
  - Type
    - **Passive**
    - **Semi-active**
    - **Semi-passive**
    - **Active**
  - Store information in clear-text on the EEPROM
  - Fixed serial number format, Flexible user data (if any)
  - Have memory pages (if any)
  - Do not have read protection
  - Some have write protection (by password)
- Middleware

What is semi-active and semi-passive?

- Most people though they are the same (Semi-active=semi-passive, reference to http://en.wikipedia.org/wiki/RFID). It means that tag has its own battery for the tag IC to be constantly powered
- Further, semi-active and semi-passive are distinguished as follows:
  - Semi-active
    - Tag is waked up by reader to communicate with its own power (ex. ETC, Electronic Toll Booth Collection System)
  - Semi-passive
    - Tag contains its own power source used for its internal control circuitry but not used for transmitter power

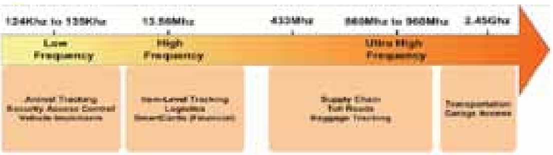
- **高速公路電子收費卡可重複加值使用，每張最高儲值上限為新台幣 10,000 元，每次加值金額至少新台幣 500 元 (僅接受 現金加值) ，**
- **e 通機液晶螢幕顯示**
  上路前，請將高速公路電子收費卡或 e 通卡插入e通機卡片插槽，並按下 e 通機右側上方操作按鈕 ，即可依序檢視卡片餘額、車型種類及電池電量 。
- **電源供應：**9V 方型鹼性電池



Country	Type	Frequency
USA	Active	0.9/2.4/5.8GHz
Japan	Active	5.8GHz
Korea	Active/Passive	5.8GHz
Singapore	Passive	2.4GHz
Europe	Passive	5.8GHz

2002/6 電波新聞別冊，Japan

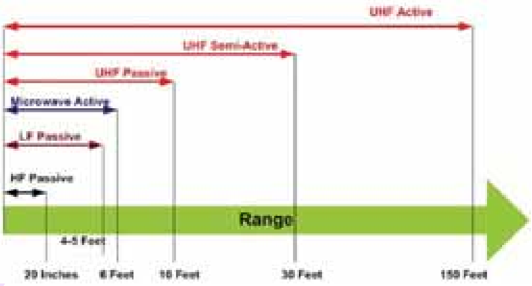
RF System Operates On ISAM Band



- Lower frequency can better withstand interference (caused from metal, moisture)
- Higher frequency can provide larger read range

Source from RFID security and privacy issues, Booz, Allan, Hamilton, 2005 Mid-Atlantic Logistics Conference

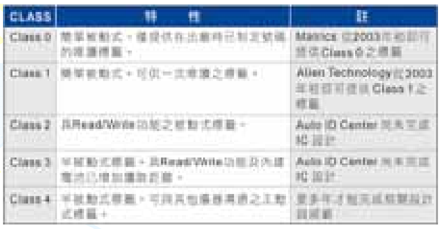
Effective Range Of Tag



RFID Standards ISO and EPC

- ISO 15693 for short range (1.5m), 26kpbs
- ISO 14443 for ultra short range (7-15mm), 847kbps
- ISO 18000 series for supply chain management
  - 18000-1 Part 1 – Generic parameters for the air Interface for globally accepted frequencies
  - 18000-2 Part 2 – parameters for air interface communications below 135 KHz
  - 18000-3 Part 3 – parameters for air interface communications at 13.56 MHz
  - 18000-4 Part 4 – parameters for air interface communications at 2.45 GHz
  - 18000-5 Part 5 – parameters for air interface communications at 5.8 GHz **(withdrawn)**
  - 18000-6 Part 6 – parameters for air interface communications at 860 to 960 MHz
  - 18000-7 Part 7 – parameters for air interface communications at 433 MHz

- EPC
  - Current release
    - Class 0: read only, for 900MHz passive
    - Class 1: WORM, 13.56MHz, 860-930MHz, passive
    - Class 1 generation 2 : UHF(860-960MHz), passive
  - In progress
    - Class 2: write/readable
    - Class 3: SRFID
    - Class 4: Can communicate with other tags
  - EPC tag lengths
    - 64bit, 96bit
    - (in future) 256bit

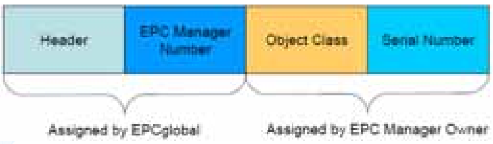


CLASS	特 性	註
Class 0	簡單被動式，僅提供在出廠時已預先寫入的唯讀標籤。	Matrics 從2003年初即可提供Class 0之標籤
Class 1	簡單被動式，可供一次寫入之標籤。	Alien Technology從2003年初即可提供 Class 1之標籤
Class 2	具Read/Write功能之被動式標籤。	Auto ID Center 尚未完成設計
Class 3	半被動式標籤，具Read/Write功能及內建電池以增加讀取距離。	Auto ID Center 尚未完成設計
Class 4	半被動式標籤，可與其他標籤溝通之主動式標籤。	要多年才能完成相關設計規範

資料來源:國家實驗研究院科技政策研究與資訊中心 2004/08/11
http://cdnet.stpi.org.tw/techroom/market/eeic/eeic028.htm

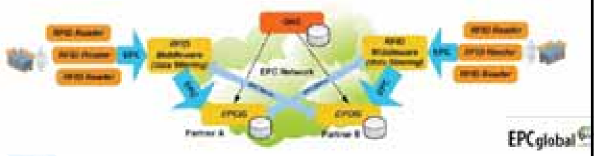
EPC Tag format

Source from RFID and EPC Essentials version 01, EPC Global



- Header
  - identifies the length, type, structure, version, and generation of the EPC
- EPC Manager Number
  - entity responsible for maintaining the subsequent partitions
- Object Class
  - identifies a class of objects
- Serial Number
  - identifies the instance

EPC Network



- EPC ID system - a collection of RFID tags and a network of RFID readers
- EPC middleware - a software specification for the aggregation, filtering, reporting of EPC data
- EPCIS - a data repository of EPC-related information
- ONS - an EPC resolution service (similar to DNS) that connects EPCIS on the network, facilitating the discovery of EPC information

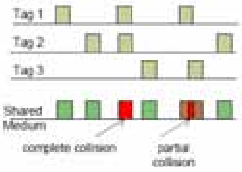
RFID multiple access methods, Luc Andre Burdet, 2004 Seminar report

Limitations

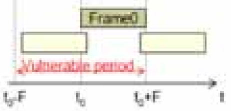
- Tag has limited memory and computation power to support little calculation capability
- Passive tag has no internal power of source which imply the detection of collision might not be feasible
- Currently most collision problems are solved by TDMA method

The Aloha Protocol

- Pure Aloha
  - A tag begins transmitting as soon as it is ready and has data to send, as referred as Tag-talk-first.

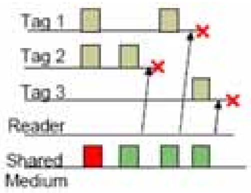


- A complete or partial collision of pure Aloha

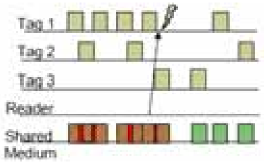


- RFID systems has the inability to detect or sense the carrier, as is assumed for classical networking.
- Apparently pure Aloha protocol is not applicable

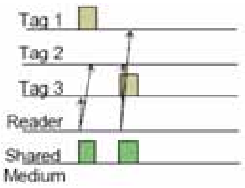
- Aloha with switch off command
  - Successfully tag responses result in the tag automatically entering a Quiet state



- Aloha with slow down command
  - The goal is to diminish tags' reply frequencies.

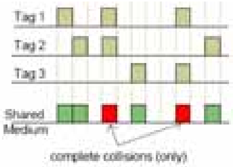


- Aloha with carrier sense [EMMicro98]
  - The reader uses its capacity to listen to the medium in order to convey extra information to the tags
  - A special MUTE command is broadcast to the remaining tags in the reader's field as early as possible after a transmission is detected,

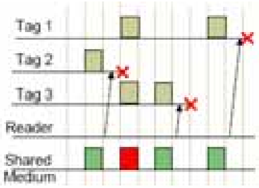


The Slotted Aloha

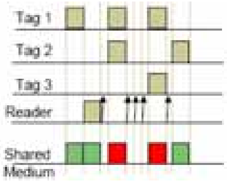
- The slots are delimited by beacons sent by the reader known as SOF (start-of-frame) and EOF (end-of-frame).



- Slotted Aloha with terminating extension [iso18000-3, C1G2Spec03]
  - Tag switches to Quiet state after a successful transmission
  - Tag in the Quiet state will re-enter to Active state upon the Wake-up command from reader

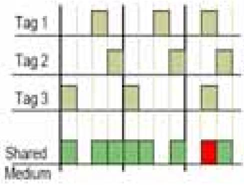


- Slotted Aloha with early end extension
  - Upon having sent a SOF command to the tags and noticing there are no responses being sent out by tags, the reader can send out an early EOF beacon effectively reducing what would have otherwise been dead or wasted time.

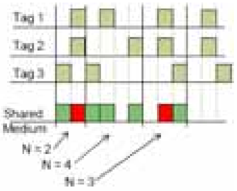


Frame-Slotted Aloha

- Slots are grouping into frames, a frame has N slots
- A tag transmits to reader once per frame
- The maximum slot number N is pre-defined and set in the tags as default

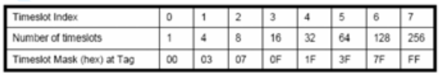


- Frame slotted Aloha with adaptation extension
  - N can be increasing to reducing collision or be decreasing to improve throughput (as there are too many empty slots)



Existing Implementations

- Philips I*Code
  - Introduced in May 1999
  - Frame-slotted Aloha protocol
  - The frame size is determined for the next round
  - , I*code sends index i (with fewer bits) Instead of number N to all tags

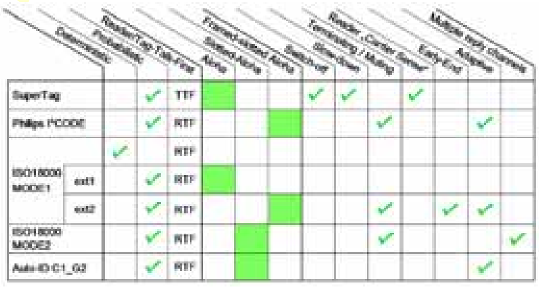


Timeslot Index	0	1	2	3	4	5	6	7
Number of timeslots	1	4	8	16	32	64	128	256
Timeslot Mask (hex) at Tag	00	03	07	0F	1F	3F	7F	FF

- ISO 18000-3 MODE 1
  - A deterministic method of querying nodes to avoid collisions
  - MaskValue and MaskLength are sent out alongside a number of slots, and used by the tags to determine the correct response slot in which to reply.

- ISO 18000-3 MODE 1 Extension 1
  - non-slotted non-terminating aloha protocol
  - Tags reply at random with self-determined intervals
  - Reply as long as in energizing field
  - Reader doesn't influence interrogation process
- ISO 18000-3 MODE 1 Extension 2
  - slotted terminating adaptive round protocol
  - Continuing dialog between Reader and Tag
  - Tags select reply-slot number, from a maximum slot number
  - Number of slots in round expands/contracts with number of Tags in field (temporarily overridden by Reader)

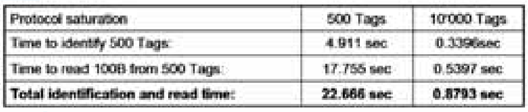
- ISO 18000-3 MODE 2
  - A combination of both Frequency and Time Division Multiple Access (FTDMA) by dividing the powering field's frequency into 8 sub-carriers, each on an individual frequency.
  - A tag following this protocol has the choice of selecting from 8 reply channels to send its ID to the reader.



		Deterministic	Probabilistic	Reader/Tag Talk-First	Aloha	Slotted-Aloha	Frame-slotted Aloha	Switch-off	Slow down	Terminating / Muting	Reader, Carrier Sense	Early-End	Adaptive	Multiple reply channels
SuperTag			✓	TTF	🟩			✓	✓		✓			
Philips I²CODE			✓	RTF			🟩			✓			✓	
ISO18000 MODE1		✓		RTF										
	ext1		✓	RTF	🟩									
	ext2		✓	RTF			🟩			✓		✓	✓	
ISO18000 MODE2			✓	RTF		🟩				✓				✓
Auto-ID C1_G2			✓	RTF		🟩							✓	

Comparison Of ISO 18000 Mode 1 And Mode 2

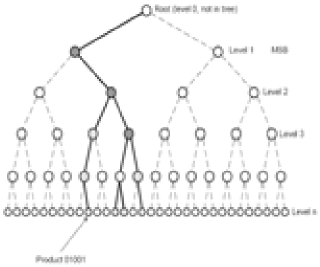
- ISO18000 MODE1 - MODE2 comparison [magellan01]



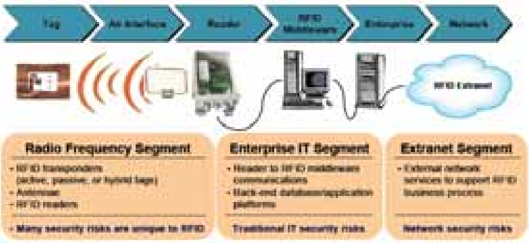
Protocol saturation	500 Tags	10'000 Tags
Time to identify 500 Tags:	4.911 sec	0.3396sec
Time to read 100B from 500 Tags:	17.755 sec	0.5397 sec
Total identification and read time:	**22.666 sec**	**0.8793 sec**

Add

- EPC Class 0 protocol: Tree Walking Algorithm (TWA)
- A population of tags to be read by the reader can be represented as
- binary tree.
- A tree will descend from the root, at the top (not considered to be part of the tree), with branches leading downwards to more nodes.



RFID security and privacy issues, Ted Philips, Booz Allan Hamilton Inc, 2005 Mid-Atlantic Logistics Conference



Radio Frequency Segment

- RFID transponders (active, passive, or hybrid tags)
- Antennae
- RFID readers

- Many security risks are unique to RFID

Enterprise IT Segment

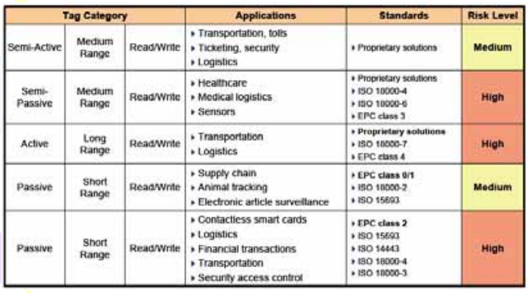
- Reader to RFID middleware communications
- Back-end database/application platforms

Traditional IT security risks

Extranet Segment

- External network services to support RFID business process

Network security risks



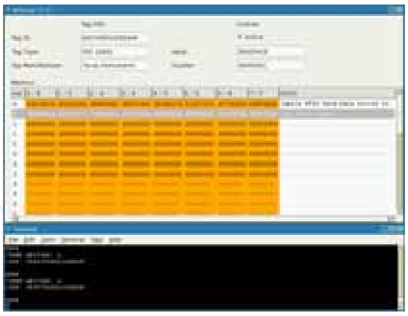
Tag Category			Applications	Standards	Risk Level
Semi-Active	Medium Range	Read/Write	▸ Transportation, tolls ▸ Ticketing, security ▸ Logistics	▸ Proprietary solutions	Medium
Semi-Passive	Medium Range	Read/Write	▸ Healthcare ▸ Medical logistics ▸ Sensors	▸ Proprietary solutions ▸ ISO 18000-4 ▸ ISO 18000-6 ▸ EPC class 3	High
Active	Long Range	Read/Write	▸ Transportation ▸ Logistics	▸ **Proprietary solutions** ▸ ISO 18000-7 ▸ EPC class 4	High
Passive	Short Range	Read/Write	▸ Supply chain ▸ Animal tracking ▸ Electronic article surveillance	▸ **EPC class 0/1** ▸ ISO 18000-2 ▸ ISO 15693	Medium
Passive	Short Range	Read/Write	▸ Contactless smart cards ▸ Logistics ▸ Financial transactions ▸ Transportation ▸ Security access control	▸ **EPC class 2** ▸ ISO 15693 ▸ ISO 14443 ▸ ISO 18000-4 ▸ ISO 18000-3	High

- In the RF segment, the attacker can
  - Intercept signal to compromise sensitive data
  - Delete, or modify data stored on tag
  - Block access of reader to tag
  - Disable a tag

- Comprise sensitive data
  - Interception of signal
    - Portable COTS can be used to
    - Tags with no encryption/authentication capabilities will reply to any query from compatible reader
    - Tags have structured data formats that disclose certain information about the owner of the tag, and class information about the asset
    - Risk level
      - Read/writable Tag > read only tag
      - Tag with on-board data > tag with id only
      - Large read range > small read range (ex. UHF)
  - Spoofing, impersonation
    - Falsifying tag or reader identity

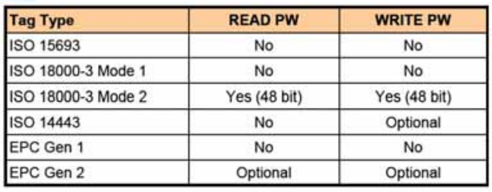
Shareware RFDump (http://www.rf-dump.org/)

- A Backend Tool that directly interoperate with any RFID ISO-Reader to get the content stored on Tags
- Features
  - Decodes tag type, tag ID, and manufacturer;
  - Displays tag memory in Hex and ASCII
  - Write memory using Hex or ASCII
- Runs under Linux/Windows PC or HP iPAQ PDA with Linux
- Has Perl script and Gtk version
- Supports ACGs, PCMCIA/CF, Multi-Tag Readers
- Supported ISO 15693, ISO 14443 A&B, Tag-it and I-Code Tags



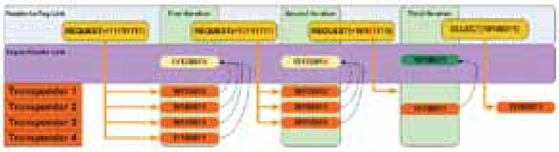
- Interference
  - Radar interference
  - Tags operating at 433 MHz have been documented producing interference with military radar
  - Hostile emissions intelligence operations could elicit responses from tags, causing them to function as unintentional emitters
  - EM effects from other RF Sources (WiFi AP, power generator, cell-phone, radios)
  - Metal Surfaces
  - Tag Orientation
    - Since the magnetic field has vector characteristics, it is important to be aware of tag orientation with respect to the reader antenna (Polarization)

- Modifying/Deleting Data On Tags



Tag Type	READ PW	WRITE PW
ISO 15693	No	No
ISO 18000-3 Mode 1	No	No
ISO 18000-3 Mode 2	Yes (48 bit)	Yes (48 bit)
ISO 14443	No	Optional
EPC Gen 1	No	No
EPC Gen 2	Optional	Optional

- RFID Blocker tags
  - Simulate a large number of tags responding to each query, creating constant RF collisions
  - Can create a denial-of-service attack within the vicinity of each device

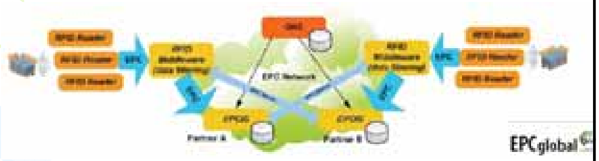


The binary-tree singulation process is used to query tags and differentiate them to control RF collisions

- The *KILL* command
  - Permanently disabling tags, created by the Auto-ID center to quell fears from privacy advocates
  - retailers are able to permanently disable tags upon customer purchase
  - The command is activated by sending an 8-bit *KILL* message to a specific tag identification
  - The 8-bit message contains a hard-coded password, with no provision for system-level password management

- The *LOCK* command
  - Issuing a *LOCK* command allows all or a portion of a tag's memory to be protected from future *WRITE* commands
  - Some types of tags require a **password** before *LOCK*ing, others do not
  - Some types of tags do not have the capability to **unlock** (the lock is permanent), others can be unlocked after supplying a password
- ISO 18000-3 Mode 1: *LOCK* command is permanent and not protected by password
- ISO 18000-3 Mode 2: *LOCK* command is permanent but is protected by password
- ISO 15693: *LOCK* command is permanent but is protected by password on some types of tags
- ISO 14443: *LOCK* and *UNLOCK* commands are present, but may or may not be protected by passwords depending on the manufacturer
- EPC Gen 1: *LOCK* command is permanent and not protected by password

- Electronic attacks
  - Electrostatic discharge
  - High-energy RF
  - Microwave ovens…
- Physical attacks
  - Crushing
  - Bending
  - Ripping
- Environmental damage



- The Object Naming Service (ONS) functions like the Internet’s Domain Naming Service (DNS)
- DNS attacks (e.g., denial of service, cache poisoning, domain hijacking, server cracks) are well documented

Conclusion

- **Data Confidentiality**
  - Develop efficient cryptographic primitives on tags
  - Store and validate protected data on tags
- **Tag-to-Reader Authentication**
  - Implement ID hashing and randomization
  - Implement challenge/response protocols for authentication
  - Implement mutual bi-directional authentication
- **RF protocols**
  - Continue optimizing protocols to leak as little information as possible about tag identity
  - Optimize collision-avoidance algorithms to minimize data compromise

- **Readers**
  - Design readers with a reliable ***kill*** capability which implement manageable passwords
  - Design readers with the ability to reliably implement ***locking*** of R/W tags
  - Give readers the ability to implement evolving privacy and security policies
- **System design**
  - Integrate secure database architectures with granular access controls
  - Implement advanced authentication and identity management techniques
  - Integrate RFID systems with existing security and privacy infrastructure
  - Design high-assurance computing systems (e.g., fail-over, redundancy, load
  - balancing)

- ***Risk management planning becomes each organization’s key line of defense***

Thank you for your attention