Security Issues in RFID and Allocated Frequency Band for RFID in Korea

October 5, 2005
Kyo-il Chung
kyoil@etri.re.kr
RFID Technology

What is RFID?
- RFID is an ADC (automatic data collection) technology that uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, locate and track, etc.

Three Main Components of RFID are
- Tags (or transponders) affixed to objects and carry identifying data
- Readers (or transceivers) read or write tag data and interface with back-end databases
- Back-end databases correlate data stored on tags with physical objects

History of RFID
- First Bar code patents: 1930s
- First use of RFID device: The 2nd World War
- First RFID Patent: 1973
- Early 1990s: IBM developed and patented an UHF RFID system
- More than 100 large end-user companies, plus the U.S Department of Defense and many key RFID vendors: 1999 to 2003
  - E.g.: Albertsons, Target, Wal-Mart
Security Problems in RFID

Possible Threats in RFID Technology

- Passive signal interception of signals from the RFID tag or Reader
- Unauthorized reading of RFID tag
  - Tags with user defined data areas are at risk (EPC Class 1 Gen 2)
- Spoofing and Impersonation
  - Falsifying tag or reader identity
- Unauthorized disabling tags
  - Disabling tags by illegal users can cause DoS attack
  - Kill, Lock, Physical attacks are possible
- Hacking tool for RFID tag was appeared
  - RFDump tool is available at http://www.rfdump.org
  - Allows reading and writing of certain types of RFID tags
- More elaborate RFID tag attacking case
  - TI’s DST RFID Tag is cracked by using specially designed FPGA chip, reader and laptop
  - The security of conventional RFID is weak and can easily be spoofed in hours
Security Technology for RFID

- In research community, many research works have been done to make security technology for RFID
  - Simple RFID security technology are developed. But they are not enough
    - Kill Tag, Faraday Cage, Blocker Tag, etc.
  - Cryptographic approach is now considered for strong security
    - Hash Lock, Randomized Hash Lock, Strong Encryption using AES, etc.

- Main Problems to make RFID secure
  - Light weight security protocol and mechanism are needed to satisfy the resource constraints of RFID
  - More complicated key distribution mechanism for large numbers of RFID tags are necessary
Standardization Efforts for RFID Security (1/3)

- There are not so much efforts in standardization for RFID Security
  - We can say that “the password in Class 1 Gen 2 tag” is used for access control to RFID tag
  - In the freight container application of RFID technology, there are some efforts in related to RFID security: eSeal technology (ISO 18185)

- In ISO TC104 SC4 WG2, they want to make a standard for eSeal Security
  - TC104 Freight Container
  - SC4 Identification and Communication
  - WG2 AEI for Container and Container related Equipment
  - Related site: [http://www.autoid.org/tc104_sc4_wg2.htm](http://www.autoid.org/tc104_sc4_wg2.htm)

- Related Documents are
  - ISO/DIS 18185-1 Communication protocol
  - ISO/DIS 18185-2 Application requirements
  - ISO/DIS 18185-3 Environmental characteristics
  - ISO/WD 18185-4 Data protection
  - ISO/WD 18185-6 Message sets for transfer between seal reader and host computer
  - ISO/DIS 18185-7 Physical layer
Current Problems in eSeal and eSeal Security Proposal (ISO 18185)

- In current ISO 18185 specification, delayed or missed read case may be happened so frequently. In the following cases,
  - high densities of containers
  - moving containers

- Also, security functions are poorly defined in current ISO 18185 specification
  - No “data integrity” function is provided
  - If we want to use the “digital signature security scheme” in the current specification, we have to extend the communication time by 40~100%

- Another problems in ISO 18185
  - The Window size is not defined. It means that each vendor’s eSeal products have different Window size each other
In the next meeting of ISO 18185 standardization, security issues in eSeal RFID technology should be more seriously considered

- Next meeting of ISO 18185 will be happened in Nagoya, Japan, from Oct. 18 to Oct. 19 2005

The following security issues should be considered for RFID security

- Accessibility
- Confidentiality
- Data integrity
- Authentication
- Non-repudiation of stored data
- Encryption
- Levels of security
Ⅱ Frequency Band for RFID in Korea
## Frequency Band for RFID

### Frequency and Application

<table>
<thead>
<tr>
<th></th>
<th>Passive/Active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.45GHz (ISO 18000-4)</td>
</tr>
</tbody>
</table>

#### KOREA Allocation (PASSIVE & ACTIVE)

<table>
<thead>
<tr>
<th>Frequency Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>125KHz, 135KHz</td>
<td>(ISO 18000-2)</td>
</tr>
<tr>
<td>13.56MHz</td>
<td>(ISO 18000-3)</td>
</tr>
<tr>
<td>433.92MHz</td>
<td>(ISO 18000-7)</td>
</tr>
<tr>
<td>860MHz~960MHz</td>
<td>(ISO 18000-6)</td>
</tr>
</tbody>
</table>

#### Frequency and Application

- **Passive**
  - 125KHz, 135KHz (ISO 18000-2)
  - 13.56MHz (ISO 18000-3)
  - 433.92MHz (ISO 18000-7)
  - 860MHz~960MHz (ISO 18000-6)

- **Active/Sensing**
  - 20KHz
  - 16KHz
  - 500KHz
  - 5.5MHz (83.5MHz)
  - (0.1~1m, <1m, <10m)

- **Sharing Amateur Radio**
  - Door Control/Security
  - Transport Card
  - Animal Management
  - Container
  - Circulation/Distribution

- **For Passport**
  - Distribution Storage, Product Circulation
Frequency Allocation

Basic Direction

- Allocation Domestic FRQ with INT Standard by Global Trend of RFID
- Allocation be Sharing with Other Services for Effective Usage of Radio Resource
- Built CJK Cooperation System for Construction of Useful RFID in ASIA

RRL : Radio Research Laboratory

RRL
INT Standard
USN Center
Foreign Trend
Company
CJK Cooperation
Korea RFID/USN Society
Allocation FRQ
Korea Technical Rule
Allocation be Sharing
ISO/IEC 18000-6 Air Interface : Aug. 31. 2004
RFID 900MHz Frequency Allocation : July. 26. 2004
RFID 900MHz FRQ Technical Criteria : Dec. 1. 2004

Frequency Allocation

- 908.5 MHz to 914 MHz
- BW : 5.5MHz

Public Service
PASSIVE RFID READER
CT1
**Frequency Allocation**: 908.5 ~ 914 MHz

**Summary of Technical Standard**

<table>
<thead>
<tr>
<th></th>
<th>FHSS</th>
<th>LBT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRQ Band</td>
<td>908.5 ~ 914MHz</td>
<td>-</td>
</tr>
<tr>
<td>Hopping CH</td>
<td>not overlapped 15 CH more</td>
<td>-</td>
</tr>
<tr>
<td>Acq BW</td>
<td>below 200kHz</td>
<td>-</td>
</tr>
<tr>
<td>ANT PWR</td>
<td>below 1W (4W EIRP)</td>
<td>50~250mW : - 90dBm</td>
</tr>
<tr>
<td>Sensing Level</td>
<td>below - 96dBm</td>
<td>250mW~1W : - 96dBm</td>
</tr>
</tbody>
</table>

EIRP : Effective Isotropically Radiated Power  
FHSS : Frequency Hopping Spread Spectrum  
LBT : Listen Before Talking
**433MHz RFID**

**History**

- ISO/IEC 18000-7 Air Interface: Aug. 31. 2004
- RFID 433MHz Frequency Allocation: Dec. 7. 2004
- RFID 433MHz Technical Standard: June. 2005

**Frequency Allocation**

- ACTIVE RFID (TAG/READER) 433.67 – 434.17 MHz
- Amateur Radio 430.0 – 440.0 MHz
433MHz RFID

Summary of Technical Standard

<table>
<thead>
<tr>
<th></th>
<th>Korea Technical Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRQ Band</td>
<td>433.67 ~ 434.17MHz (500KHz)</td>
</tr>
<tr>
<td>Aq. Bandwidth</td>
<td>Reader → Tag : 500KHz, Tag → Reader : 200KHz</td>
</tr>
<tr>
<td>ANT PWr</td>
<td>5.6dBm(max) = 3.6mW</td>
</tr>
<tr>
<td>Duty Cycle</td>
<td>60s(Tx) / 10s(Stop)</td>
</tr>
</tbody>
</table>

Sharing Test Result with Amateur Radio Using
- 433MHz Band using Only Container Pickup Area like as Harbor, Inland Container Pickup Area, Waterfront Warehouse, etc.

This frequency range can be affected by the action to provide the strong security and efficiency in eSeal RFID technology
2.45GHz RFID (Passive/Active)

- **International Standard**: ISO 18000-4
- **Frequency Allocation**: 2400~2483.5MHz (BW 83.5MHz) for RFID
- **World Trend**
  - High Speed, High Sensitivity, Small Size, Matter Management
  - **2.45GHz band is designated** for non-specific use.
In UHF RFID Spectrum Allocations in CJK, there are not special issues in CJK countries.

In allocation the 433MHz frequency, there is an issue in sharing the frequency band with Amateur Radio. Also, it may be affected the standardization results by ISO TC104 SC4 WG2 (eSeal) which is in processing.
u-Cluster Strategy in Korea
In Korea, we consider the RFID technology is the core technology to realize the Ubiquitous Information Society.

I will briefly describe about Korea’s Strategy…

**Ubiquitous Information Society**

- **8 Services**
  - WiBro Service
  - DMB Service
  - Home N/W Service
  - Telematics Service
  - RFID-based Service
  - W-CDMA Service
  - Terrestrial DTV
  - Internet Telephony

- **3 Infrastructures**
  - Broadband Convergence Network
  - Ubiquitous Sensor Network
  - Next Generation Internet Protocol (IPv6)

- **9 Growth Engines**
  - Mobile Telecomm Handset & Equipment
  - Digital TV & peripherals
  - Home Network HW/SW
  - System-on Chip
  - Next Generation PC
  - Embedded SW
  - Digital Contents & SW Solutions
  - Telematics
  - Intelligent Service Robot
RFID will be evolved to ubiquitous sensor network (USN) technology.
And, the USN is the essential technology to achieve Ubiquitous Information Society.

- Tag on all objects
- Sensing the object and environment
- Real time management on the network

**Sensor Network**

**RFID/USN Application Service Evolution**

- **ID Recognition**
  - Read
  - Product information
  - Real time stock mgmt.

- **History Management**
  - Read/ Write
  - Product distribution
  - History management

- **Sensing the Environment**
  - Sensing
  - Environment
  - (example: House – temp. & humidity change, Temp. control, etc.)

- **Ad-Hoc Network of the Sensors**
  - Traffic flow and signal control

- **Electronic Tag Control**
  - Real time, automatic control of reaction to changing environment
  - (example: Hospital – Remote medication & prescription depending on The patient condition)

**RFID/USN Technology Evolution**

- **Passive RFID System**
- **Active RFID System**
- **U Sensor Network**
How Korea can realize the vision for Ubiquitous Society

- We have designated a special economic zone near Seoul to efficiently develop the RFID technology

Songdo District

- Planned population of 250,000
- 53 square kilometers
- International affairs, knowledge-based industry, R&D center, center of RFID/USN development
u-Cluster Strategy in Korea (4/4)

- Recreation options, including:
  - New golf courses
  - Theme parks
  - Large green space

- Foreign schools with:
  - English-speaking teachers
  - Programs developed through Harvard University

- World-class English-speaking hospital (negotiations with Johns Hopkins, Harvard)

- One-stop administrative support with specialized incentives on:
  - Corporate tax exemption
  - Available cash grants
  - Discounted land price

- RFID test-bed in logistics at Incheon Airport nearby

- Shared services for RFID/USN development being planned (e.g., test-center, EMS, pilot fab)

- Songdo layout plan
  - International Business center
  - IT cluster
  - Biotech cluster
  - Living environment

Songdo layout plan

Broadband IT Korea
Thank you for your attention