Contents

Part one: Introduction

**Chapter 1: RFID overview**

1.1 Automatic identification technology

1.2 The main features of RFID

1.3 The core technology of RFID

1.4 The history and current situation of RFID

1.5 The development trend of RFID

1.6 RFID and Internet of Things

Part two: Identification

**Chapter 2: Principle of RFID system components**

2.1 Reader

2.2 RFID Tag

2.3 Software System Components

2.4 Summary

**Chapter 3: Wireless communication principle of RFID**

3.1 RF Spectrum and Electromagnetic Signal Transmission

3.2 Signal Voltage and Energy

3.3 Modulation and Multiplexing of Reader Signal

3.4 Backscatter Mechanism and Tag Encoding

3.5 Link Budget

3.6 Effects of Antenna Gain and Polarization on Transmission Range

3.7 Signal Transmission in Realistic Environments

3.8 Conclusion

Part three: Protocol

**Chapter 4: RFID tag identification protocol**

4.1 RFID tag identification protocol

4.2 ALOHA based anti-collision algorithm

4.3 Binary Tree based anti-collision algorithm

4.4 Binary Search based anti-collision algorithm

4.5 Performance Analysis of Anti-collision Algorithms

4.6 Summary

**Plus: checksum**

**Chapter 5: UHF RFID protocol standard**

5.1 EPCglobal standard

5.2 EPCglobal Class 0 protocol

5.3 EPCglobal Class 1 Generation 1 protocol

5.4 EPCglobal Class 1 Generation 2 protocol

5.5 Summary

# CHAPTER 1

1.1 Automatic Identification Technology

Human identification

The earliest identification technology originated in humans. Humans use their own perceptual system to identify external physical objects effectively, including visual, auditory, tactile, taste and so on.--The cost is too high

**Automatic identification**

The essence of the recognition technique is to distinguish and identify the physical objects using their identifiable features.

1.1.1 Fingerprint Identification

Fingerprint identification uses the uniqueness and stability of fingerprint to verify user identity by comparing the collected fingerprints with the pre-sampled fingerprints.

·Stability

·High accuracy of identification

·Low error rate

·Each fingerprint has multiple feature points Each feature point has 5 to 7 features ·Ten fingers can produce at least 4900 independent features that can be measured

·High speed

·Fingerprint match can be completed in 1 to 2 seconds

·Miniaturization

·Intelligent

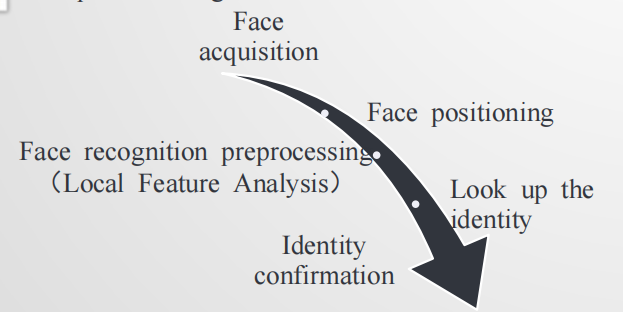
·Low price

·Security issues

Fingerprints are easy to leave over Fingerprint replication is getting easier

1.1.2 Face Recognition

Face recognition is based on human face features. It performs identityauthentication by analyzing the input face image.



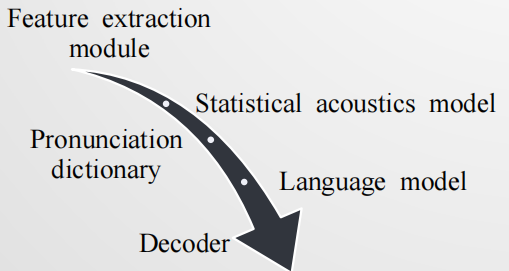
·Technical Features

·Surroundings, hair ornaments, age can affect the recognition rate

·Fast recognition speed, not easy to be aware of it

1.1.3 Speech Recognition

Speech recognition uses the difference between each person's tone and timbre to identify different people



·Technical Features

Easy to use, and easily accepted by the user

Cheap sound equipment, and not involve user's privacy

Due to the lack of international standards, there are some

difficulties in promoting

1.1.4 1D Barcode Recognition

·1D barcode is a combination of lines and blanks in accordance with certain coding rules to represent certain information.

·1D barcode only express information in the horizontal direction, and in the vertical direction does not express any information. It usually retains a certain height to facilitate the alignment of the reader.

·Limited storage capacity, need to combine with the database. The barcode size is relatively large, the space utilization is low. Fault tolerance is poor, can not restore the information after the corruption

1.1.5 2D Code Recognition

·2D code uses black and white graphics on the two-dimensional plane to record data, these geometric patterns express specific information through a certain regulation of distribution .

·Positioning point technology: 2D code usually has three positioning points for the reader to identify, because of these positioning points, 2D code can be identified no matter what direction to read.

·Fault tolerance: the information can be correctly restored when it does not recognize all of the 2D code, or if the 2D code is defaced.

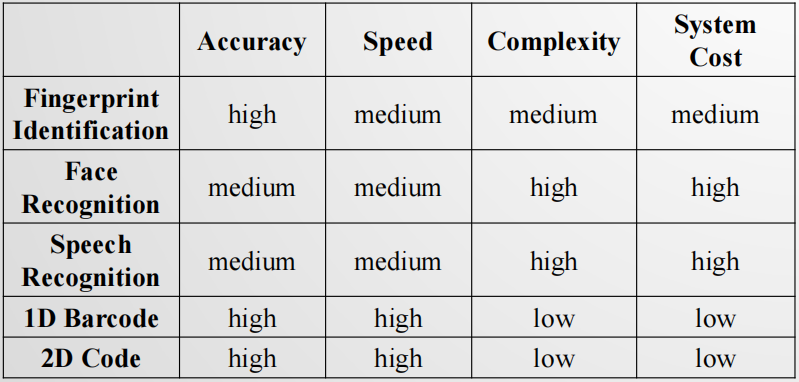
·Large storage capacity. Up to 32KB.

High information density. Can store text, sound, pictures and other information.

Powerful error correction capability. 2D code can still be identified in the case of 50% defacement.

Support for encryption. Multiple security features.

1.1.6 Summary of automatic identification technology



1.1.6 Emerging automatic identification technology

·Retina recognition technology

The retina is an extremely immobilized biological feature that doesn’t wear, doesn’t age, and is not affected by the disease, and users do not need direct contact with the device. Retina recognition distinguishes each person by analyzing the vascular pattern on the retina.

·Heartbeat recognition technology

Heartbeat waveforms differ in the presence of distinction, and even if the heartbeat accelerates, some of the inherent characteristics of the heartbeat waveform will not change. Heartbeat recognition is based on this feature, it can identify the user identity by collecting heartbeat signal pulse through a specific instrument and then identify the inherent characteristics of each person heartbeat

·RFID

• Non-contact automatic fast identification

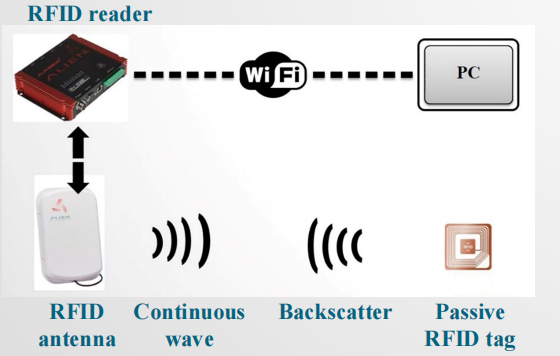
• Accurate and efficient identification

• Low cost and low power consumption

• Certain computing and storage capabilities

Provide an effective solution for the core problem of "realizing passive intelligence", "globally unique identification" and "low cost interconnection" in Internet of Things applications.

**1.2 The main features of RFID**



1.Non-contact automatic and rapid identification

The RFID tag returns data by backscattering the energy, with an effective communication range of 6- 10 m.

The RFID system uses an effective anti-collision mechanism to read tags, enabling rapid identification of a large number of tags.

2.Permanently store a certain amount of data

RFID tag has a user storage area, which can store 1KB-10KB of user data.

3.Simple logical processing

RFID has a very limited number of internal logic gates, so only a simple logical processing can be made. But the RFID system can use the basic logic processing ability of tags to achieve some effective protocols and algorithms to improve the system operating efficiency and security performance.

4.Reflection signal strength is affected by the distance and other factors significantly

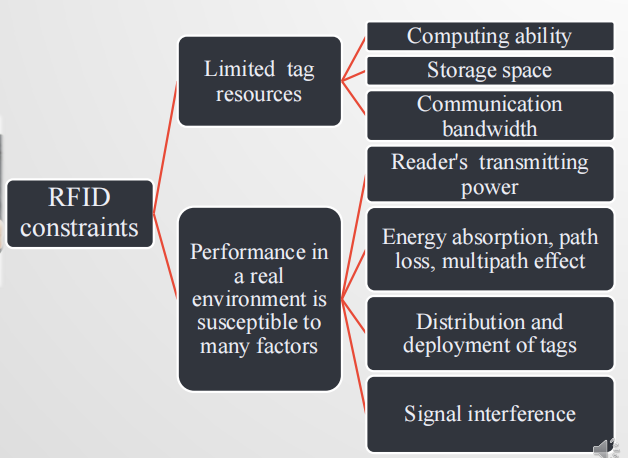
Since the RFID tag itself is a passive device, the feedback signal must be modulated by backscatter. Therefore, the strength of the RFID tag reflection signal is susceptible to the surrounding environment, including distance, reader power, signal interference, and tag deployment density.

5.Low cost, can be deployed at a large scale

RFID tags tend to large-scale mass production using printed circuits, so manufacturing costs can be significantly reduced. At present, the cost of

an RFID tag can be controlled at around 10 cents.

**1.3 The core technology of RFID**



1.Anti-collision transmission mechanism

Achieve low latency, and efficient identification

2.Positioning and mobile behavior sensing

Achieve the positioning of the target

3.Information storage, retrieval and mining

Provide a gateway from the physical world access to the information world

4.Security certification and privacy protection

Ensure the credibility and security of the interaction

1.Anti-collision mechanism

Conflict between tags, between readers, between reader and tags

– Traditional wireless communication protocols (such as CSMA / CA) are not available

– RFID environment: tag identification protocols must be simple and efficient

– How to effectively avoid conflicts, improve transmission performance, and reduce the scan delay?

3.Efficient information storage, retrieval and mining

– How to efficiently store, retrieve and mine ID, keyword information,

and sensing data carried by RFID tags in a distributed environment？

2.Make full use of the attenuation laws of backscatter signal to

assist in positioning and mobile behavior sensing

– Accuracy Low precision: within a few meters; High precision: within a few

centimeters

– Real time

– Stable Mean error, stability (confidence interval of error）

4.Security certification and privacy protection

– Forged tags: how to validate?

– Malicious reader: how to prevent illegal access and protect user privacy

effectively？

– Existing algorithms require more logical processing units,

e.g., AES requires 20000-30000 logic gates

– RFID tags have only 5000-10000 logic gates

– How to implement authentication and privacy protection protocols in a

resource-constrained RFID system in a lightweight way？

1.4 The History and Current Situation of RFID

**1.5 The development trend of RFID**

·Energy acquisition mode

1.Traditional wired transmission: obviously no longer feasible

2.Battery-powered: increase the weight and volume, the battery needs to be changed regularly

3.Wireless charging: not yet reached the practical use

4.Backscatter: time of endurance is prolonged

indefinitely, small node size

Disadvantages: rely on the reader, one to many centralized communication

Design and implement innovative energy harvesting

ways to support communication between systems, in order to fully expand the scope and deployment scale of RFID applications.）

·Ambient backscatter: Create new types of network communication by leveraging

radio signals (such as television and cellular network base station signals) that are

prevalent in the environment

·Support point-to-point communication: Design and implement innovative channel awareness technologies that enable RFID devices to establish networks and implement point-to-point communications in a passive way to support multiple distributed applications

·Combine with Sensors: Integrating existing micro-sensor devices, combined with multimode sensors, provides a richer application model based on backscatter technology

**1.6 RFID and Internet of Things**

·In the Internet of things, RFID will embed intelligence in the physical object, so that simple physical objects can also “say”.

• In the Internet of things, RFID allows a physical object to be uniquely identified in a way similar to the "IP address" of a computing node in the Internet.

• In the Internet of things, RFID provides a low-cost communication way to achieve effective communication between nodes.

• In the Internet of things, RFID makes the physical objects in a passive environment achieve "passive intelligence“, providing fundamental guarantee for the “thing-thing connection" .

# CHAPTER 2 RFID

2.1 Reader

**2.1.1 Reader’s Function**

As the bridge connecting the application layer (middleware) and RFID tags, the reader plays a significant role. Generally speaking, in RFID system the functions provided by a reader are usually summarized as follows:

·Energy Supply

A reader provides energy for RFID tags’ work.

·communication

Communication between reader and tag;

Communication and application layer between reader (middleware)

·Security Assurance

Security assurance in communication, such as encryption and decryption

·Ad-hoc networking ability

·Multiple antenna management

·Interface of middle components

·Connecting peripherals

**2.1.2 Reader’s Classification**

**·By working frequency**

RFID system’s working principle is related to the frequency of RF signals it used.

The higher the work frequency, the further the identification range, the higher the data transferring speed, the faster the signal attenuation, the more sensitive to obstacles.

LF and HF readers, work at distance <1m, typical work frequencies: 125kHz、135kHz、

6.78MHz、13.56MHz and 27.125MHz

UHF (Ultra High Frequency) and SHF (Super High Frequency) readers, work at distance >1m, typical work frequencies: 433MHz、860MHz~960MHz、 2.45GHz and 5.8GHz

**·by cost and portability/ appearance**

In practice, taking reader’s cost and portability into consideration, the appearance of a reader varies a lot, thus divided into the following 3 types:

Fixed

Wired charging

Highly integrated

Fast set up

Portable

Small volume

Battery charging

Easy to move

Industrial

Industrial related

Capable of integrating other sensors

2.1.3 Reader’s Operational Specifications

·R&W range (read out and write in range) is one of the key

performance metrics that affect the scope of reader applications.

**Influencing factors:**

The way that antenna is coupled

The output power of the reader’s RF signal

The frequency of RF carrier signal

·Antenna direction

When the polarization direction of the reader antenna and tag antenna match, the recognition range becomes maximum. In practice, mismatch is unavoidable, where measures as followed can be applied:

·Change the direction of the reader antenna

 ·Use multiple redundant antennas

 ·Increase the power of the reader antenna

 ·Increase sampling rate of the reader antenna

 ·Use a ring polarized reader antenna

·Operation environment condition (metal interference, electronic noise, multi-tag, multi-reader, etc.)

·Movement speed of tags

重点注意的要素：

• 1.Work frequency

• work frequency ↑, data transfer speed ↑, work range ↑.

• LF system using 125kHz: no more than 400b/s

• Systems with data transfer speed over 100Kb/s need UHF/microwave

• 2.Anti-collision performance

• The system’s effective data transfer rate in scenario with multiple RF tags reading and writing

• 3.Flexibility of RFID protocols

• Communication protocol: universal protocol (ISO18000-6C, EPCglobal Class1 Generation2, etc.) or exclusive protocol

• 4.Country (district) radio management specification

• USA UHF RFID bandwidth range: 902MHz-930MHz

• China UHF RFID bandwidth range:840MHz-845MHz, 920MHz- 925MHz

• Maximum transmit power requirements

• 5.Communication protocols

• Communication interface between reader and computer network system (TCP/IP, 802.11, Ethernet, RS485, etc.)

• 6.Multiple antenna support ability

• whether to support multiple antennas for one reader

•7. Middleware interface

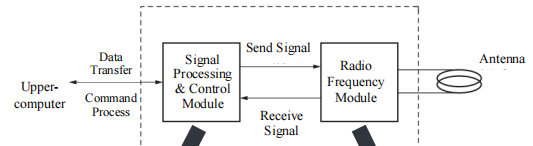
• Stable performance, easy to use

• 8.Connect external sensor nodes and control circuits

• Combine RFID and sensor networks

• Use PLC (programmable logic controller) to perform entry management for warehouses

**2.1.4 Reader’s Components**



·1.Signal Processing & Control Module

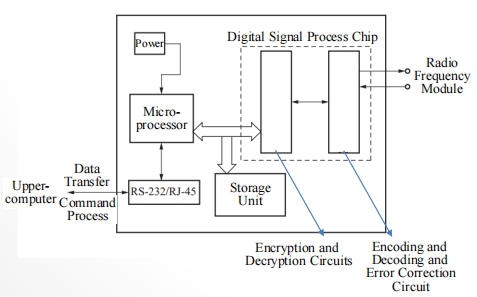
Also known as baseband control module, includes: Microprocessor to perform computing tasks ,Digital signal processing chip to encode and decode digital signal

·2.Radio Frequency Module

Also known as high frequency interface module, includes separate channels:

Transmitter signal channel and Receiver signal channel

**2.1.5 Signal Processing and Control Module**



·Communicate with upper computer, and execute command from it

·Control communication process with tags

·Encode and decode signal

·Perform anti-collision algorithm

·Encrypt and decrypt the data transferred between reader and tag

·Identity certification between reader and tag

**2.1.6 RF Modules**

**·Inductively Coupled RF Module** （电感耦合型射频模块）

Near-distance LF, HF RFID systems work via inductive couple between reader and RF tag. Tags in this working way are usually passive, while gaining energy through inductive couple.

While sending data to RF tags, a reader can apply various digital modulation technologies. While sending data to a reader, RF tags usually use load modulation technology, transferring voltage variation in antenna coil of RF tag to the reader antenna.

·**Electromagnetic Backscatter Coupled RF Module**（电磁反向散射耦合型射频模块）

Long-distance UHF RFID system use electromagnetic backscatter coupled principle between reader and RF tags, similar to radar.

In the system, to continuously provide energy for RF tags, the reader must continuously sends RF signals.

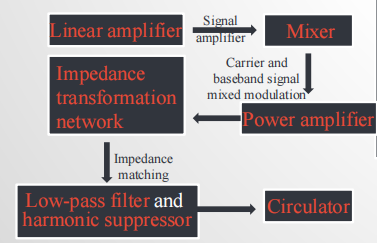
The signals sent by reader and returned by tag have the same frequency but different strength.

UHF RF modules can be divided into: source module, send module and receive module.

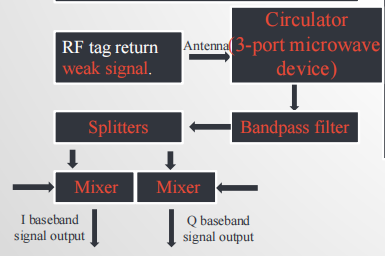
·Source module provides Local Oscillator for Send Module and Receive Module.

Amplified carrier signals are separated into two directions by splitters: to Send/Receive Module.

·Send Module consists of mixer, linear amplifier, preamplifier, power amplifier and impedance transformation network.



·Receive module consists of a linear amplifier, two splitters and two mixers.



**Main Functions of RF Module**

1.Generate high frequency send energy, activate RF tags and provide energy (passive RF tags)

2.Modulate signal to sent, transferring data to RF tags.

3.Receive and demodulate RF signal from RF tags.

2.2 RF Tags

**2.2.1 Tag Function**

The main function of RF tags is to store a certain amount of data, and send it to the reader in a contactless manner.

1.data storage

Tags store goods-related information, e.g. identifier, production date, manufacturer, etc

2.Energy Harvesting

Tags can absorb energy from electromagnetic field generated by the reader, and generate electricity for themselves.

3.Contactless R&W

Tags can be identified from a certain distance to the reader.

4.Security Encryption

5.Collision Concessions

**2.2.2 Tag Classification**

1.By Package Form

(1)card-like tag: Potable, good antenna protection, waterproof

(2)Label-like Tag:Directly attached to the items, used in industrial production and

logistics management

(3)Implantable Tag:Animal and plant management

(4)Accessories-like Tag: Easy to carry, no influence on the appearance

2.By Power Source

(1)Active Tags: Rely on its own battery

(2)Passive Tags:Rely on the carrier signal sent from reflection reader to gain energy

(3)Semi-passive Tags :The battery is integrated on the board, but as an auxiliary backup

3.By Work Frequency

(1)LF Tags

·30kHz~300kHz

• Usually passive

• Inductively coupled

• Strong penetration

(2)HF Tags

• 300kHz~30MHz

• Usually passive

• Inductively coupled

• Fast transmission rate, large storage

(3)UHF Tags

·0.3GHz~3GHz

• Passive or active

• Electromagnetic backscatter coupled

• Long distance, high speed, mobile scenario,

good multiple-tag r&w performance

4.By R&W Capability

（1）Read-only Tags

• Only readable, unique serial number

• Low price

• Simple structure

（2）Read & Write Tags

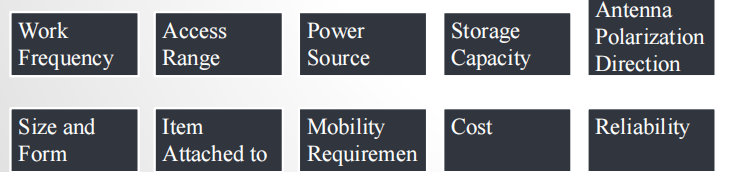
• Readable, writable

• Complex structure

• High cost

• No database related

2.2.3 Tag Operational Specification



2.2.4 Tag Components

1.Antenna

Decides the size of tag.

Receive RF signal from the reader;

Send chip data to the reader;

Provide energy for passive tags

2.Chip

Demodulate and decode signal received by the antenna, encode and modulate the signal to send from the tag, and perform anti-collision algorithm and store data.

2.2.5 Tag Antenna

Antenna is a conductor designed to be coupled and radiate electromagnetic energy.

Generally the smaller the tag size, the less the antenna radiation impedance阻抗, the shorter the tag work range, the lower the work efficiency.

Antenna performance includes direction property, antenna efficiency, antenna gain, etc.

According to work principle, tag antenna has 3 types:

Coil antenna，Microstrip patch antenna，Dipole antenna

1.Coil antenna

·Simple process, low cost, widely used in LF, HF close-range RFID system.

·Work by inductively coupled, whose principle similar to transformer. The reader antenna is equivalent to transformer primary coil, tag antenna as secondary coil, generating voltage at a varying magnetic field.

·Charged by parallel capacitors, generate power for tag chip.

2.Microstrip patch antenna

·A microstrip patch antenna is usually attached to the surface of a conductor sheet, with a metal foil ground plane on the other side.

·Light weight, small size, low cost, easy to mass production.

·Suitable for scenario of which the communication direction doesn’t change.

3.Dipole Antenna

·A dipole antenna consists of two straight wires with the same length

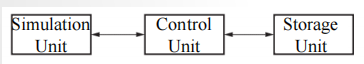
and thickness put in a straight line.

·Suitable for UHF tags.

·Typical antennas: half-wave / double line folded / triple line folded / double dipole antenna.

·A dipole antenna is omnidirectional antenna.

2.2.6 Tag Chip



·Components: simulation front end ，control unit and storage unit.

·Simulation front end: the rectified antenna input signal provides a stable voltage, the antenna input is detected to obtain a digital signal, modulate control unit signal for antenna to send, provide clock for control unit.

·Control unit: data decode, check, encode, encryption, decryption, anti-collision, · read/write control.

·Storage unit: tag data carrier

2.2.7 Tag Wake Circuit

Wake mechanism circuit

·Rectifier→1V voltage output →Transistor connection

·Rectifier→5mV voltage output →Compare with reference voltage →Transistor connection

2.2.7 Tag Manufacture

Manufacture process: Antenna produce and chip assembly

2.3 Software System Component

2.3.1 Overview

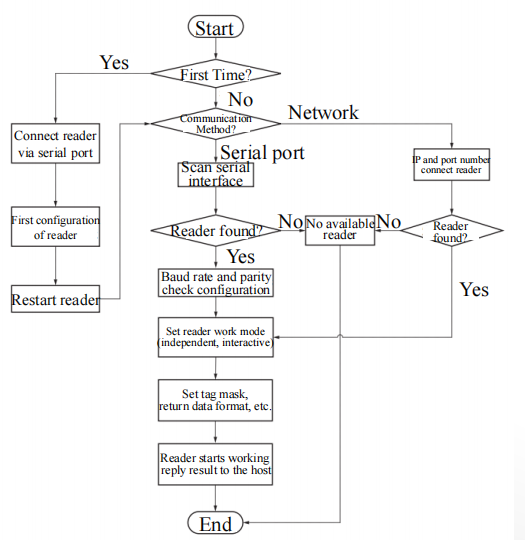
Take UHF commercial reader of Alien Technology for example.

Content:

The reader’s initialization configuration of the installation process, tag mask set, the realization of independent work, the realization of interactive work,

the storage structure and the wake-up methods.

2.3.2 工作流程



2.3.3 Alien RFID Java middleware

·Organizational structure

Include 5 package: reader、tags、 discovery、notify、util

·Reader’s connection

AlienClass1Reader class create object to control, with COM or network:

·Open or close connection

reader.open();

reader.isOpen();

reader.close();

·Send operational command to reader

Through reader object’s doReaderCommand

·Tag info class

Through getTagList function of reader object

Tag[] tagList = reader.getTagList();

public String getTagID();//return tag ID

public int getRSSI();//return signal strength

·Search available reader

Serial service listener class:

SerialDiscoveryListenerService

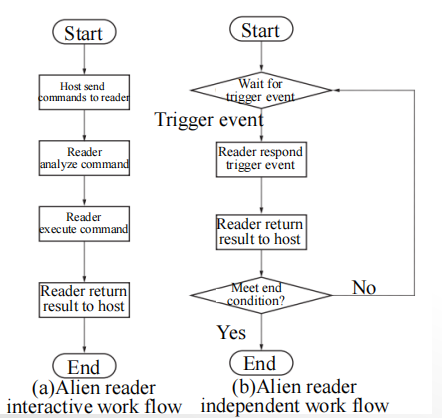
Network service listener class:

NetworkDiscoveryListenerService

·Work mode of interactive and independent

Readers see each command from host as a single

task, execute by order and return result immediately



·Tag Storage Structure

Typical tag storage structure of EPC Class1

Generation2

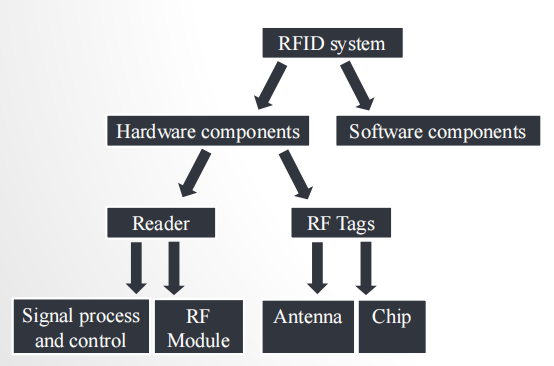
·Tag Mask

2.3.4 Reader Operation Full Example

·Connect reader by serial port

·Reader independent work mode

2.4 RFID System Component Principle Sum Up



# CHAPTER 3 Wireless Communication Principle of RFID

3.1 RF Spectrum and Electromagnetic Signal Transmission

**Electromagnetic waves** are energy and momentum transmitted as waves caused by

same-phase oscillation between mutual perpendicular electric field and magnetic field.

**Modulate various wireless signals to carrier signals with different frequencies to transmit.**

·LF：30kHz~300kHz, usually passive tags, communication range < 1m, not be disturbed by any material except for metal, typical work frequency: 125kHz~134kHz

• HF：3MHz~30MHz，usually passive tags, communication range < 1m, typical work frequency: 13.56MHz

• UHF：300MHz~3GHz, passive or active tags, communication range > 1m, cannot go through many materials, especially for water, dust, fog and other suspended particulate materials, typical work frequency: 433MHz，860MHz~960MHz

• SHF： passive or active tags, communication range > 10m at most, typical work frequency: 2.45GHz，5.8GHz（microwave signal）

**Different carrier frequency decides different work principles**：

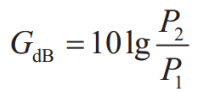
• LF & HF RFID tags: often inductively coupled, short communication range, magnetic field energy decays as the speed of cubed distance

• UHF & SHF RFID tags: often electromagnetic backscatter coupled, long communication range, energy decays as the speed of squared distance

**3.2 Signal Voltage and Energy**

The relative change is more worthy of attention in the signal processing problem.

Use decibels (dB) instead of watts (W)



Decibels are relative. The reference power is needed when describing the specific power. Commonly used is 1mW. Here the dB size is dBm.



**3.3 Modulation and Multiplexing of Reader Signal**

Continuous Wave, CW:

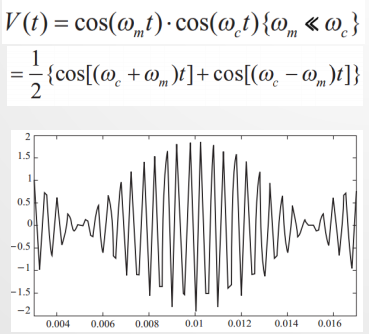
A simple periodic sinusoidal signal whose frequency, phase, amplitude

don’t change.

It can’t carry information, thus needs modulation: m(t) contains baseband information, cosine is carrier



When m(t) is also cosine signal, according to trigonometric function:

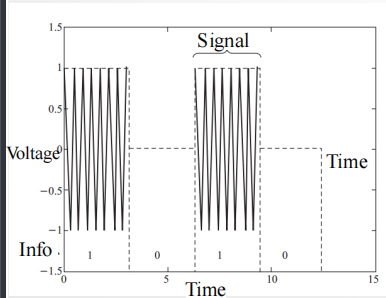


·This sinusoidal modulation divides the signal into two signals, called sidebands. One’s frequency is higher than the carrier (first part of the formula), while the other’s is lower than the carrier (second part of the formula)

·Generally, it is digital modulation that is usually performed on RFID reader signal(Digitally Modulated)

**On-Off Keying, OOK: high power for 1, low power for 0.**

An actual binary string will be converted into a section of electromagnetic waves with high or low power.



**Problem**：For passive RFID tags, the low energy of data bit 0 can’t activate

the tag, not to mention normal work

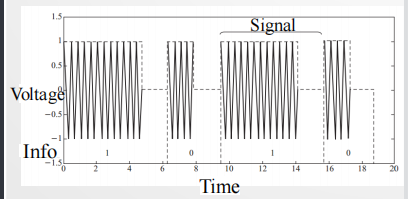
Solution:

Encode binary data bits before modulation.

Pulse Interval Encoding(PIE):

“1”：output long time of high power followed by a short time of low power

“0”：output a short time of high power followed by a short time of low power



Problem:interference

FDMA (Frequency Division Multiple Access)：need different applications to use different carrier frequencies to transmit information, and receivers only demodulate signals with specific frequencies

ALR-9900 reader: work frequency is 902.75MHz~927.25MHz, divide into 50 channels, with each channel using 500kHz frequency scope

In realistic applications, still need to pay attention to the deployment of readers, and the interference of other signals in the surrounding space

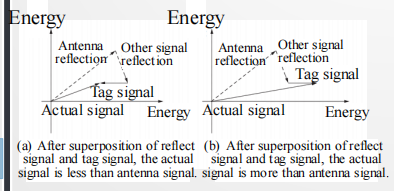
**3.4 Backscatter Mechanism and Tag Encoding**

·Any object that receives certain electromagnetic waves will transmit the same series of electromagnetic waves.

·The electromagnetic waves modulated by the receiver can return to the antenna of the transmitter, and produce a recognizable signal, which is called backscatter signal.

·The reflected signal vector received by the receiver at a certain time is the vector superposition of various signals in space.

·As shown on the right, the superposition leads to uncertainty. If backscatter mechanism is to be used, certain encoding mechanism is to be designed to make receiver able to recognize these signals according to the variety, instead of worrying about the phase or amplitude of the signal.

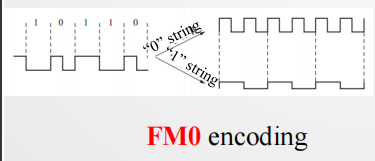


·Currently, tag encoding methods are based on a specific time interval to count tag changes, or based on the tag state change frequency.

·Belonging to frequency shift keying(FSK) variants.

“1”could be 100 turns of tag state change in 1ms

“0”could be 50 turns of tag state change in 1ms



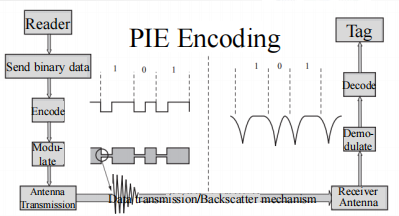
·In realistic receivers, there are usually existing noises and some inference signals together with the expected signal. For different modulating and encoding methods, there is always a constraint value for the Signal to Noise Ratio (SNR, i.e., S/N)

·FM0： 10dB or larger SNR

Readers in the PIE way have similar SNR constraints

**3.5 Link Budget**

Tags get energy from backscatter mechanism (upper-right).



The process from tags to the reader (lower-right).



The energy transfer and loss process will be analyzed

**Link budget**: forward link budget and backward link budget

·Reader’s transmit energy

·Path loss

·Tag activate energy

**3.5.1 Reader’s transmit energy**

·Power：The power of the reader is usually restricted to a certain safe range

·Frequency：Most RFID devices work at ISM (Industrial Scientific Medical) frequency band

·Realistic Application ：Maximum transmit energy shouldn’t be over 1W

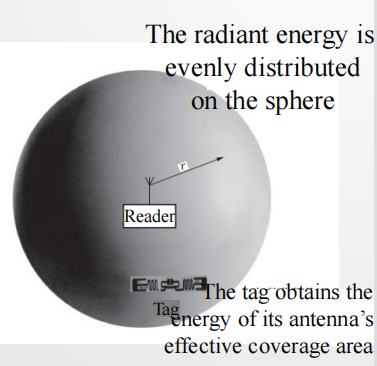
**3.5.2 Path Loss**

·Path Loss: In transmission process, the difference between actual energy sent from transmitter and that received by receiver.

·Assume that the antenna transmission is isotropic, that is, the antenna radiates energy uniformly in all directions, as shown on the right.

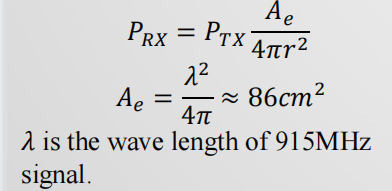
·The actual energy received by the tag is proportional to the antenna’s energy density across the tag.

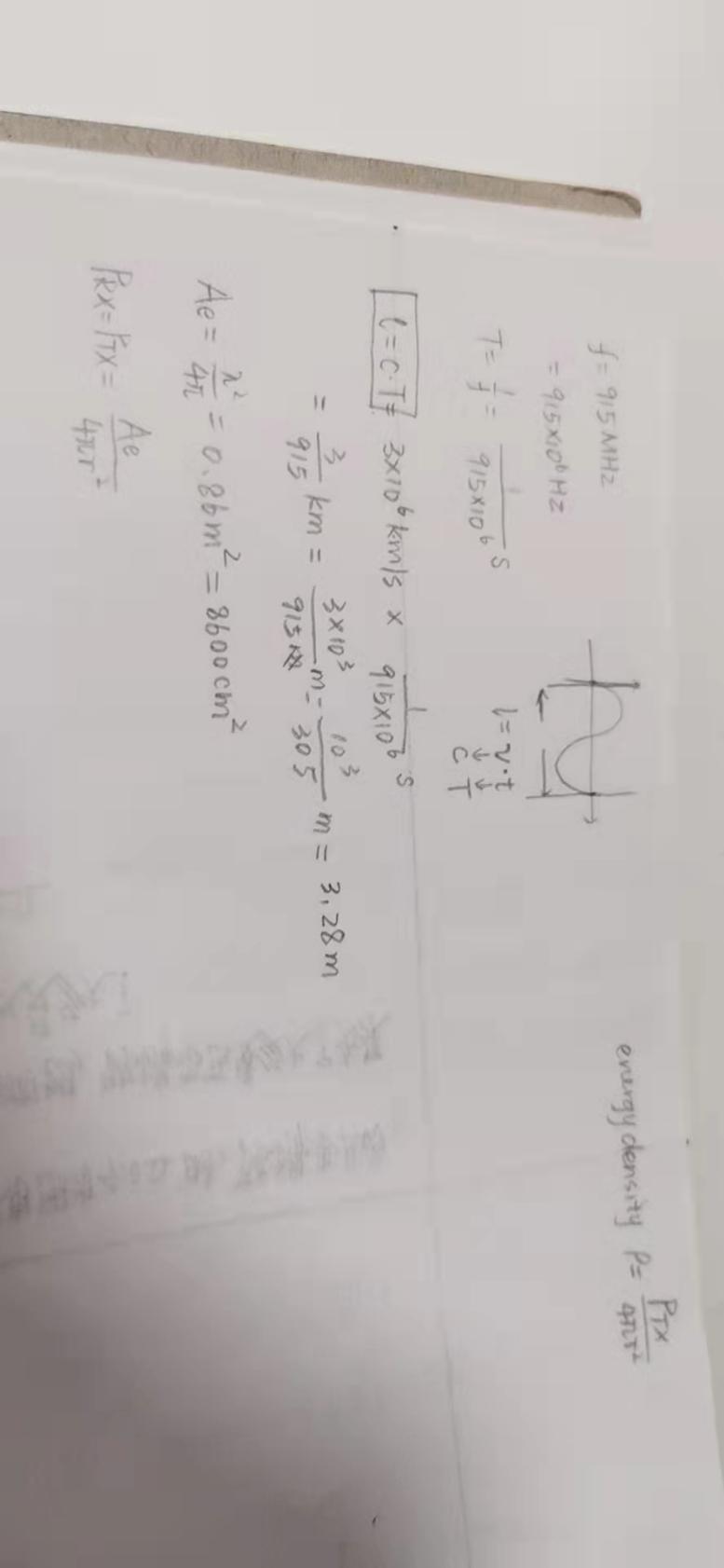
·This area is called the Effective Aperture (Ae) of the tag antenna: the actual area of the electromagnetic wave through the tag antenna



·For antennas with effective aperture , while receiving plane wave with

energy density , the energy received is : 

·In the instance of an isotropic antenna, the energy density at is the ratio of transmit energy and sphere. The received energy PTX at the tag is: 



1m: the actual received energy of the tag is 0.7mW (-1.6dBm), and the path loss is about 32dB

Path loss from 1m to 10m: 10lg(10/1)2=20dB,

10m: total path loss is about 52dB

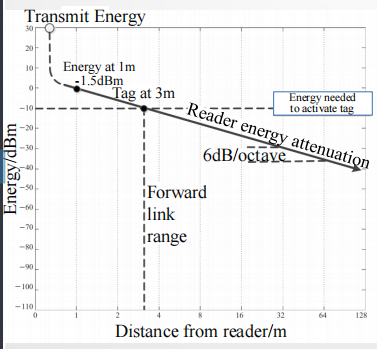
3m: total path loss is about 41dB (32+9.5)

3.5.3 Tag Activate Energy

·At tag reading phase, the tag needs an energy of 10~30uW to activate the circuit.

·But current energy utilization is merely 30%. Hence, the tag needs to obtain 30~100uW. Because the maximum energy a reader can provide is 1W(30dBm), here the threshold of the chip is set to 100uW (-10dBm), thus the max path loss is 40dB.

·The right figure draws a straight line with the start at (1m, -1.5dBm) and the slope -20dB/10m to represent the forward link attenuation mode.



·Backward link loss needs to consider the tag’s transmit energy and the minimum energy required to read tag data for the receiver.

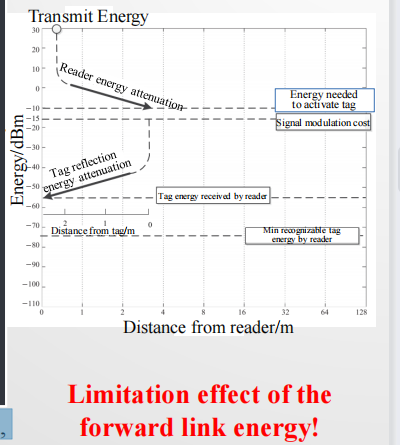
·Tag’s receive energy is -10dBm, but actual reflection energy is about 1/3 (with

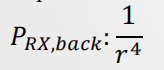
- 5dB attenuation) .

·Since the required energy for a reader to recognize differs for different tags, assume a reasonable threshold: -75dBm.

·The energy loss graph of the backward link can be plotted against the forward link energy graph.

·Reader’s receiver obtains energy -55dBm, 20dB more than the required energy.



·The energy received from the reflection link is inversely proportional to the distance from the fourth power:

3.6 Effects of Antenna Gain and Polarization on Transmission Range

Antenna gain: Under the condition of the same input power, the power density ratio of signal generated at the same point in space by actual antenna and ideal radiation unit. It quantitatively describes the extent to which an antenna concentrates the input power

Polarization: A phenomenon that things under certain conditions undergo polarization, making its properties deviate from the original state.

**3.6.1 Effects of Antenna Gain**

·For RFID readers with output 1W, with the help of omnidirectional antenna, signals can only transmit 2-3m, which is more suitable for scenarios in which the reader is

surrounded by tags.

·In practice, the reader will be placed at the edge of a certain region, while plenty of tags are placed at the center, forming an region which is in a certain angle range radiated by the reader

·Directional antenna can concentrate the energy in one place.

For RFID application scenarios, directional antennas make full use of the transmission energy, maximizing energy utilization, while reducing energy waste caused by scanning unwanted regions

For any angled relative to the center of the antenna, the edge of the curve represents the energy density of the antenna radiated in this direction.

The ratio of the radiation intensity on the direction d and that averaged in each direction, is called the directional gain of the antenna in that direction.

The radiation efficiency in this direction is the power gain of the antenna, G, also named as amplification coefficient.

For directional antenna, if higher power gain is needed, the radiation range of the signal is relatively thinner, shown on the right

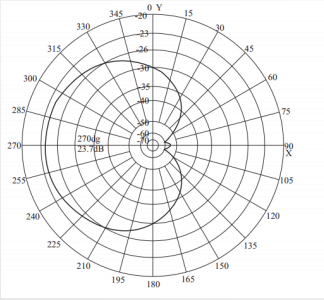


平面角（单位为弧度rad）：顶点在圆心，弧长等于半径r的圆弧 所对应的平面角定为1 rad，圆的周长（2πr）对应的角为2π rad

立体角（单位为立体弧度sr）：顶点在球心，面积等于r2的球面 对应的立体角定义为1 sr，球面的面积（4πr2 ）对应的立体角为 4π sr

The figure on the right is the directional antenna’s polar coordinate radiation pattern of commercial RFID readers.

The curve is the logarithmic mode to describe the size of the energy gain in all directions.



The beam width corresponding to 3dB is about 72°(1.25 rad), as shown in the figure, hence the corresponding beam solid angle is (1.25)2=1.6. The antenna gain is about:



·Not all antennas are specifically directional, one of which is the dipole antenna

The dipole antenna does not radiate the signal along the axis but is uniformly radiated in all directions perpendicular to the axis.

The antenna gain relative to dipole antenna is 2.2 dB smaller than that relative to omnidirectional antenna.

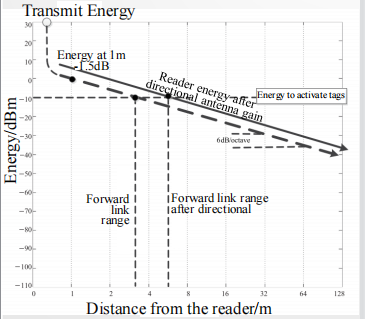
By means of the gain and transmission energy of the antenna, it’s possible to calculate the input energy required for the maximum gain effect in the direction indicated by the directional antenna by using an omnidirectional antenna, which is called the effective omnidirectional radiated power(EIRP, Equivalent Isotropic Radiated Power).

·EIRP is often or explicitly or implicitly to specify the energy limits on wireless operation.

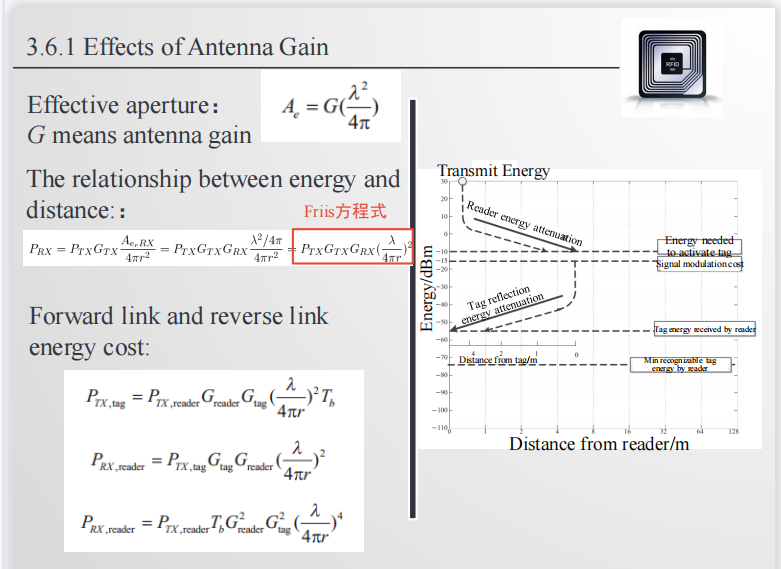
For example, FCC regulations in the United States, a non-irradiated transmitter can transmit 1W of energy signals, and can use 6dBi antenna; antenna gain increased by 1dB, transmission energy needs to be reduced by 1dB. In fact, FCC is not more than 36dBm(30dBm+6dBi).

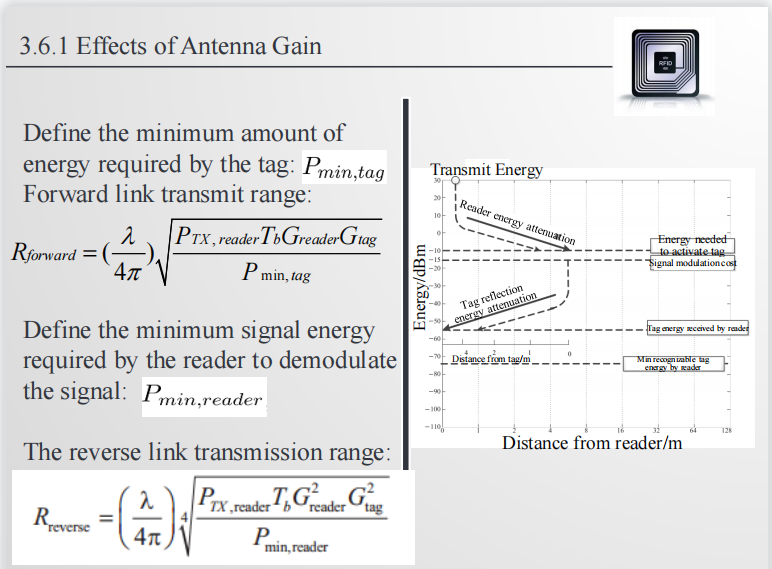


The figure on the right shows the effect of 6dBi antenna gain when the tag is located in the direction of the directional antenna gain. The transmission distance of the forward link increases from 3m to 6m. The energy loss is accompanied by a decrease in the square velocity of the distance.



定向天线：





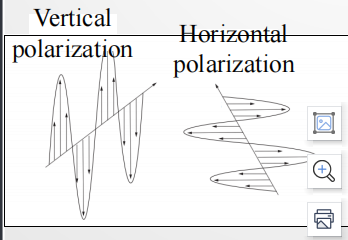
3.6.2 Linear Polarization and Circle Polarization

The direction of the electric field and the magnetic field are perpendicular to each other, and the direction of the field is always perpendicular to the propagation direction. The waves perpendicular to the vibration direction and the propagation

direction are called transverse waves.横波

The direction of the field determines its polarization direction.

The way that polarization direction is always fixed is also known as linear polarization.

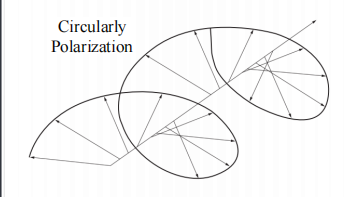


The direction of the electromagnetic field can change by time.

When the direction of the electromagnetic field is rotated around the axis of the propagation direction over time without changing its field strength, the result

is circularly polarized radiation similar to linear polarization.

Through a simple vector superposition process, we can convert the pure circle polarization into a linear polarization superposition.



When the circularly polarized electromagnetic wave acts on a linearly polarized antenna, similar to the previous decomposition process, only the electric field component in the same direction as the conductor produces potential, and the vertical component will have no effect.

Double dipole: Mainly by simultaneously placing two orthogonal antennas on the tag to achieve the purpose of absorbing energy in different directions.

For linear polarization, we only need to multiply a triangular sine variable to represent its component, where the polarization direction and the direction of the receiving antenna angle, as shown in the right formula.



3.7 Signal Transmission in Realistic Environments

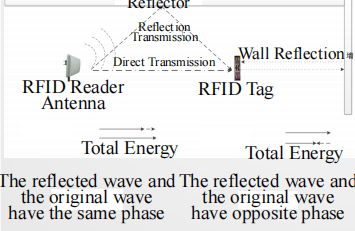
·All of above are in ideal environments for the relevant calculations, but the actual

environment is always full of noise and interference.

·The scattering of the reader’s own signal,

·The interference signal after the reflection.

·Not a simple energy superposition, but the accumulation of each point potential, the results are unpredictable, namely: multipath effect

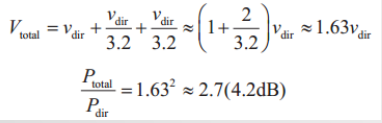


·After superimposing a bunch of electromagnetic wave from reader and its two reflected waves from the floor and the wall, if the reflected wave has 1/10 of the original electromagnetic wave energy, the superposition potential will be:

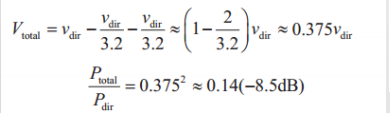
where represents the phase difference between the reflected wave and the original electromagnetic wave, and ν represents the ratio of the amplitude of the reflected wave to that of the original electromagnetic wave.

·The phase difference depends on the length of electromagnetic wave transmission distance, the length increases by ¼ of the wavelength, and the phase changes by 90°.

·Consider the worst case, when the phase difference is 0°, the superposition potential is:3.2=根号10，因为假设reflected的能量是原来的1/10，所以电势是原来的根号1/10

（增益最大值）

When the phase difference is 180° , the superposition potential is:

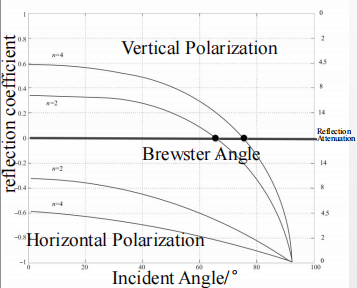
（增益最小值）

共有12.7dB的偏差

In RFID systems, the ground reflection interference is very serious, the concrete reflectivity is up to 2.5.

What also affect the recognition efficiency are the incident angle and the polarization mode.

The vertically polarized waves can not be reflected on a ground at a certain angle called the Brewster angle, as shown on the right（大概是65°）水平极化没有



# Chapter 4 Tag Identification Protocol

4.1 RFID tag identification protocol

Like other wireless transmission systems, RFID systems also have the problem of signal interference.

·In RFID systems, there are two main types of signal interference:

**1.Conflict interference among readers （Multiple readers send signals**

**simultaneously ）**

**Time Division Multiple Access （TDMA)**

**Frequency Division Multiple Access（FDMA)**

**Carrier Sense Multiple Access （CSMA)**

2.Conflict interference among tags （Multiple tags respond to the reader simultaneously ）

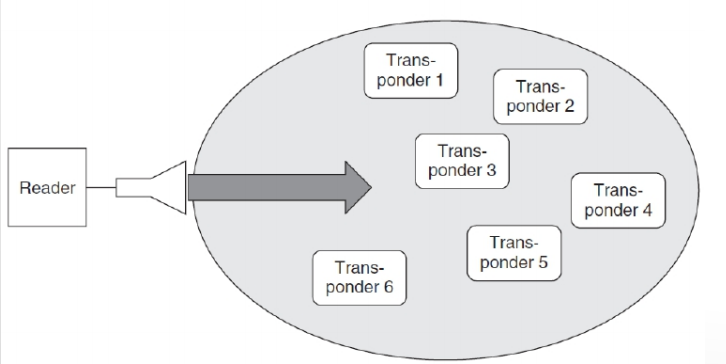
·RFID systems: numerous transponders (应答器，tags), a single interrogator (询问器，reader) reader : a ‘control station’ ，transponders : a number of ‘participants’

two main forms of communication ➢ broadcast ➢ multi-access

1.Broadcast mode

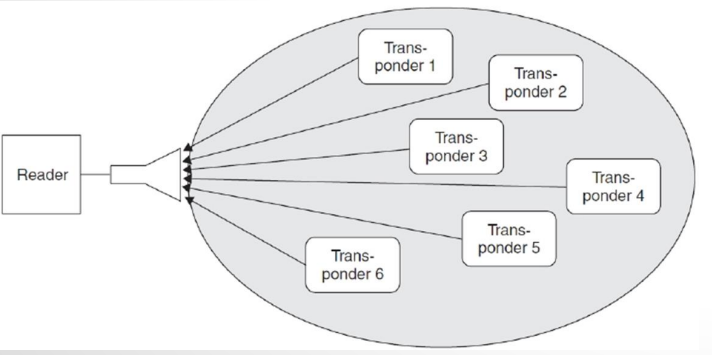
➢ transmit data from a reader to the transponders

➢ received by all transponders simultaneously



2.Multi-access

➢ data transmission: from many individual transponders in the reader’s interrogation zone to the reader



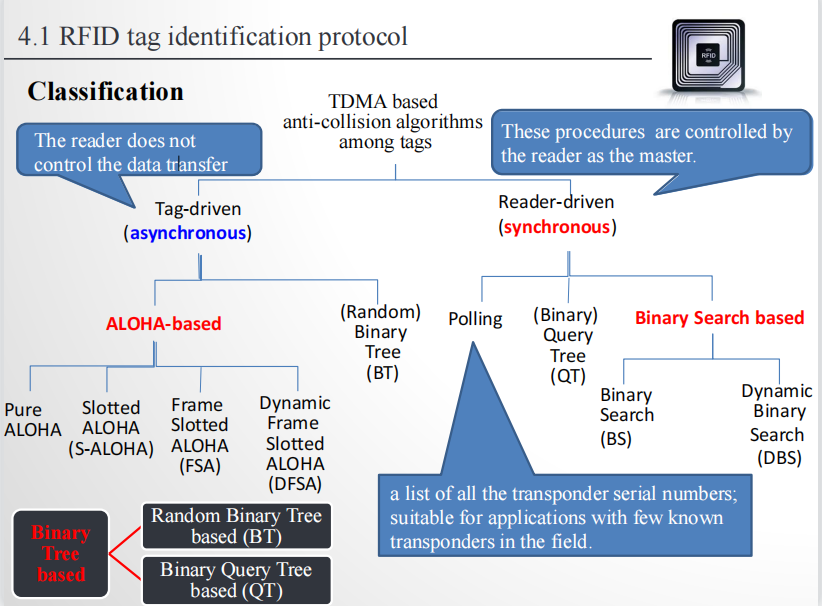
➢ space division multiple access (SDMA)

➢ frequency division multiple access (FDMA)

➢ time division multiple access (TDMA)

➢ code division multiple access (CDMA)

Classification



**4.2 ALOHA based anti-collision algorithm**

ALOHA-based anti-collision algorithms use a rollback mechanism, and tags participate in the identification process in the way of probability.

Four ALOHA-based anti-collision algorithms:

➢Pure ALOHA algorithm

➢Slotted ALOHA algorithm (S-ALOHA)

➢Frame slotted ALOHA algorithm (FSA)

➢Dynamic frame slotted ALOHA algorithm (DFSA)

Features of ALOHA-based protocols: simple and fair

**4.2.1 Pure ALOHA algorithm**

·If the tag receives a success acknowledgment message, its identifier is no longer sent. Otherwise after a period of time it will be sent again until the success of transmission.

The algorithm is simple and easy to implement, but the channel utilization can only reach 18.4%, poor performance.

·data transmission time: only a fraction of the repetition time, long pauses between transmissions.

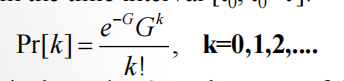
·the repetition times for the individual transponders differ slightly

·offered load G : the number of transponders transmitting simultaneously within a unit time interval

·throughput s is 1: an error-free data packet transmission

·throughput s is 0: data was not transmitted, collision

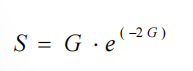
·Suppose packets come following Poisson process, the probability of k packets in the time interval [t0 , t0+tao]:



where G =arrival rate \*tao, i.e. the mean of the Poisson distribution.

When a packet is sent at t0+, it can be transmitted successfully, if and only if no other packet is sent within the time interval [t0 , t0+2tao].

So the success probability is 

the average throughput S of a transmission channel 

·S reaches a maximum of 18.4% at G= 0.5 .

– smaller offered load: unused most of the time

– offered load increased: the number of collisions increase sharply

– an anticollision procedure only for read-only tags

**4.2.2 Slotted ALOHA algorithm**

The S-ALOHA algorithm divides the time of the pure ALOHA algorithm into several time slots, each slot is greater than or equal to the time length to send tag identifier, and each tag can only send an identifier at the beginning of the slot. Due to the time synchronization of the system, the channel utilization of the S-ALOHA protocol is

36.8%, which is twice of the pure ALOHA.

The throughput S :



maximum of 36.8%: offered load G=1

·REQUEST

Synchronizes all transponders

Prompts the transponders to transmit their serial numbers in one of the time slots that follow

·SELECT(SNR) Sends a serial number(SNR) to the transponder as a parameter.

The transponder with this serial number performs read and write commands (selected).

Transponders with a different serial number react only to a REQUEST command.

·READ\_DATA

The selected transponder sends stored data to the reader.

**Procedure:**

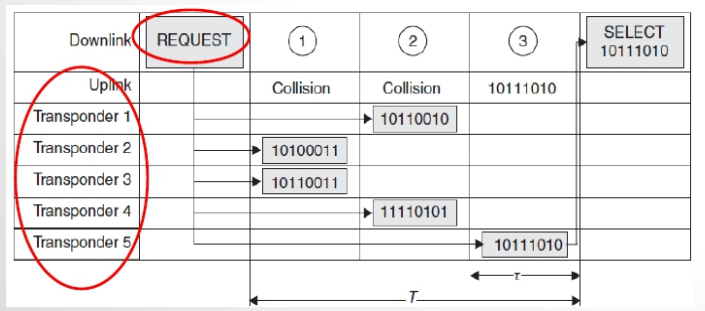
reader: transmits a REQUEST command

transponders :

• recognize the REQUEST command,

• randomly select one of the three available slots ,

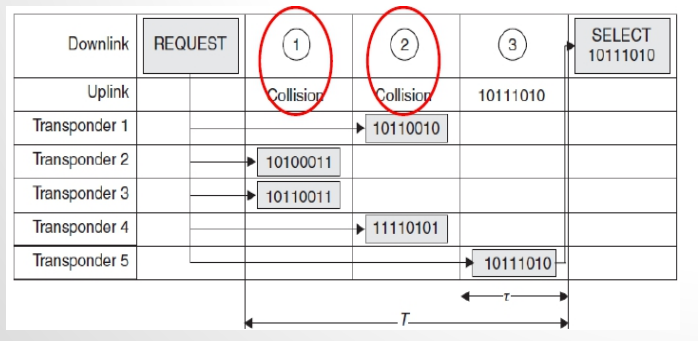
• send its own serial number to the reader.



– slots 1 and 2: collisions

– slot 3: transponder 5, selected by a SELECT command, read or written without further collisions.

– if no serial number detected: repeat the REQUEST command cyclically



**4.2.3 Frame Slotted ALOHA algorithm**

·Based on S-ALOHA, several time slots are organized into one frame, and the reader identify tags by frame.

·FSA algorithm has many advantages, such as simple logic, simple circuit design, less memory requirement, and the only one randomly sent in the frame further reduces the probability of conflict.

·FSA becomes one of the most commonly used ALOHA based anti-collision algorithms in RFID systems

·Limitations of FSA algorithm: fixed frame length

 When the number of tags is much larger than the frame length Conflict probability of tags increases, and the time to identify tags will greatly increase

 When the number of tags is much smaller than the frame length Waste too many slots, and the identification time will increase

 When the frame length is equal to the number of tags in the reader field, FSA

has best identification performance, and the max channel utilization rate is 36.8%

**4.2.4 Dynamic Frame Slotted ALOHA algorithm**

In practice, the number of tags is often dynamic.

It can solve the limitation of FSA by dynamically and adaptively adjust the frame length.

Commonly used frame length adjustment method:

➢According to the number of idle slots, the number of conflicted slots, and the number of single slots (success in tag identification) acquired by the previous frame, estimate the current number of tags and set the optimal length of the next frame

➢According to the feedback of the previous slot, dynamically adjust the frame length as an integer multiple of 2. The most representative algorithm is the Q algorithm designed in the EPCglobalGen2 standard.

**Q algorithm：**

When there are too many slot conflicts in one frame, the reader will end the frame ahead of time and resend a larger frame;

When there are too many idle slots in one frame, the reader will end the frame ahead of time and restart a smaller frame.

Q algorithm can adaptively adjust the frame length with high identification efficiency, and it has been widely used in UHF RFID systems.

·ALOHA based anti-collision algorithm is simple, and take into account the fairness.

However, there is a problem of starvation for tags. When a tag selects a slot that always conflicts with other slots, the tag may never be identified.

**4.3 Binary Tree based anti-collision algorithm**

·The basic idea of Binary tree based anti-collision algorithm ： The conflicting tag set is divided into two subsets in a recursive way until only one tag is left in the set.

·Algorithm for dividing subsets:

➢(Random) Binary Tree (BT) algorithm: Let tags randomly select the sets to which they belong

➢(Binary) Query Tree (QT) algorithm: Divide subsets according to tags’ identifier

4**.3.1 Random binary tree based anti-collision algorithm**

·Random binary tree based anti-collision algorithm requires that each tag maintains a **counter** (initial value is 0). At the beginning of each slot, if the tag’s counter is 0, it immediately sends its identifier, otherwise it does not respond. In general, the tag will

enter the silent state and will not respond to the reader’s command any more after it is successfully identified.

·In-field tags adjust the counter rule: If the slot is a collision slot, the corresponding tag will randomly select 0 or 1 and add to its own counter.

·The whole identification process is like a binary tree with pre-order traversal.

·There is no problem of starvation, but the counter needs to be maintained.

**4.3.2 Binary Query Tree based anti-collision algorithm**

·Binary query tree based algorithm is a stateless protocol, and the tag only needs to be compared to the identifier prefix broadcasted by the reader

·The reader maintains a **binary prefix** (initial value is 0). At the beginning of each slot, the reader broadcasts the binary prefix, which compares with the first few digits of the tag identifier, and if they are the same, then the tag sends the identifier.

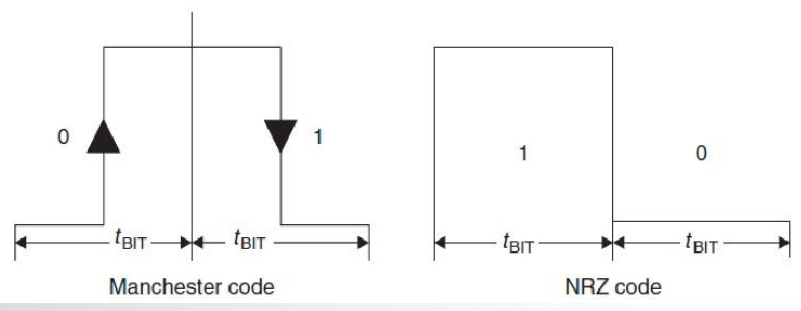
·The whole identification process is like creating a query binary tree based on tags’ identifier.

·Can be used for tags without writable storage area. Tags have no starvation problem. ·It will be affected by ID length and distribution.

**4.4 Binary Search based anti-collision algorithm**

·requires : the precise bit position of a data collision is recognized in the reader.

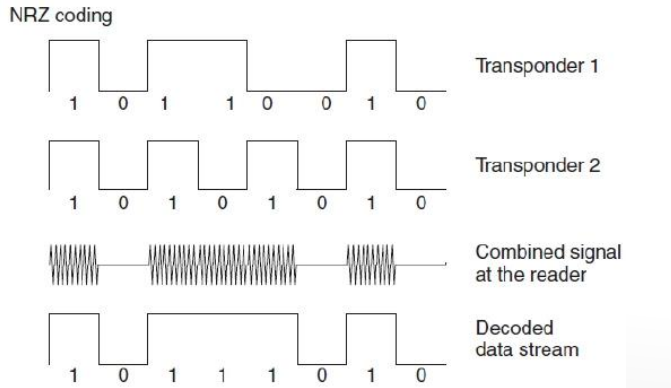
– compare the collision behavior of NRZ (non-return-to-zero) and Manchester coding



·NRZ code

– The reader cannot detect whether the sequence of bits:

• the superposition of transmissions from several transponders or the signal from a single transponder

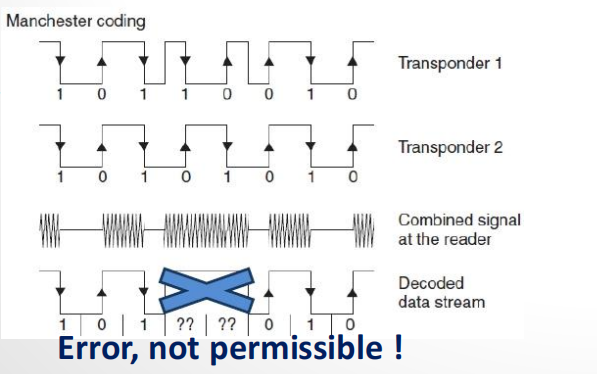


·Manchester code: if two transponders simultaneously transmit bits of different values

– the positive and negative transitions cancel each other out

– a subcarrier signal received for the duration of an entire bit

use Manchester coding for binary search algorithm



·REQUEST(SNR) Sends a serial number to transponder.

If the transponder’s own serial number is less than (or equal to) the received serial number: sends its own serial number back.

·SELECT\_(SNR) Sends a serial number to transponder.

The transponder with the identical address process other commands. (selected)

Transponders with different addresses only respond to a REQUEST command.

·READ\_DATA

The selected transponder sends stored data to the reader.

·UNSELECT

The selection of a previously selected transponder is cancelled and the transponder is ‘muted’. (completely inactive)

例子：

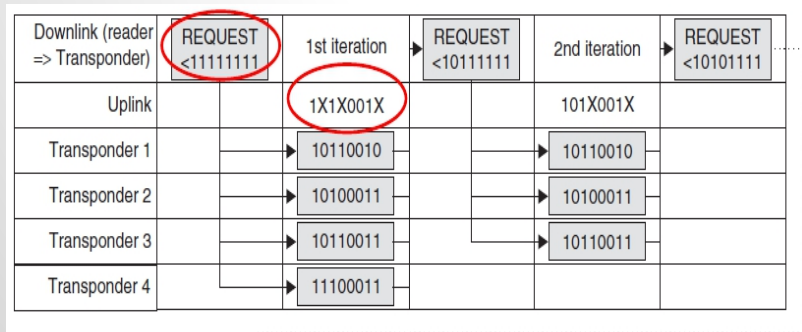
reader: REQUEST (≤ 11111111)

– all transponders must be less than or equal to 11111111b

– answered by all transponders

– precise synchronization, bit position of a collision

– bit 0, bit 4 and bit 6 : there is a collision (X)



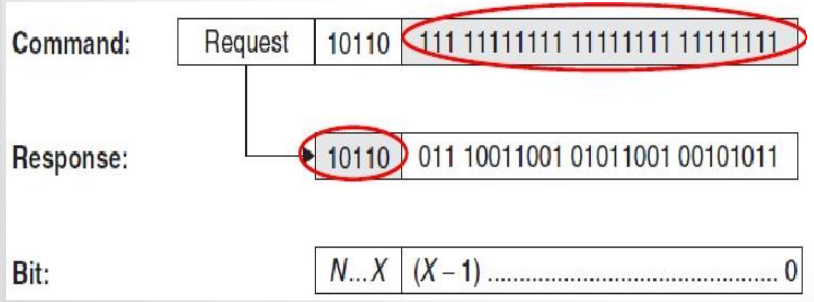
the received bit sequence 1X1X001X : eight possibilities for the serial numbers

**Dynamic Binary Search based anti-collision algorithm**

binary search procedure : both the search criterion and the serial numbers, always transmitted at full length

– Bits (X-1) to 0 of the command contain no additional information , always set to 1

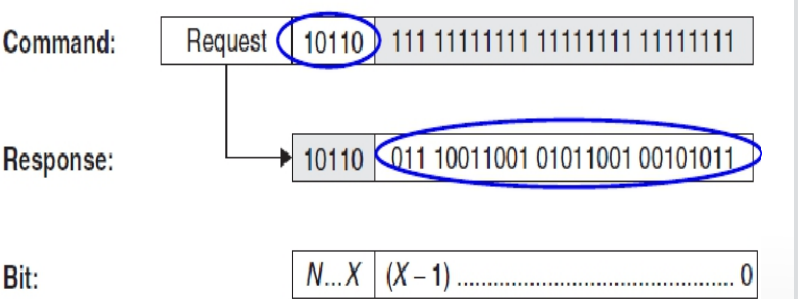
– Bits N to X of the serial number in the transponder’s response contain no additional information for the reader.



The reader : sends only the known part (N − X) as the search criterion

– Transponders that correspond to the search criterion in the bits (N − X) : transmitting the remaining bits, (X −1) to 0

– NVB (number of valid bits) : inform transponders the number of subsequent bits



**4.5 Performance Analysis of Anti-collision Algorithm**

Advantages and disadvantages of ALOHA based anti-collision algorithm:

Pros:

Simple, good tag identification performances, the results can be statistically analyzed

Cons:

Tag starvation, the worst case the delay tends to 无穷

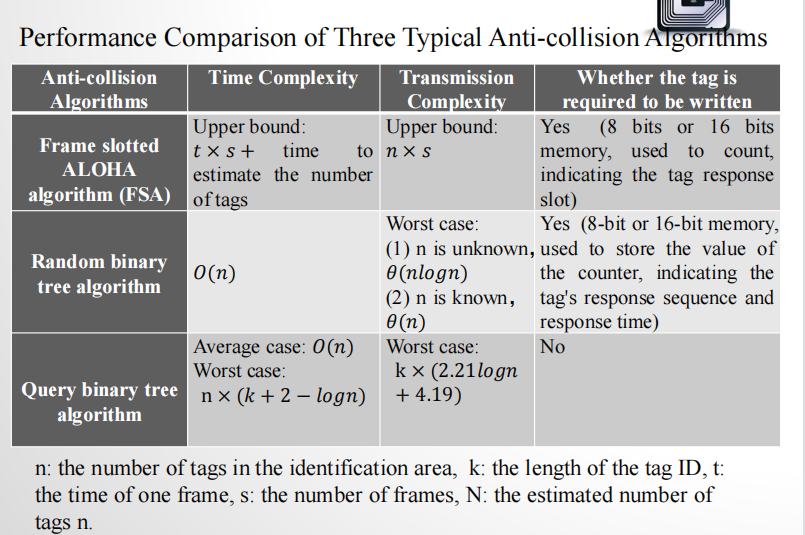
Advantages and disadvantages of binary tree based anti-collision algorithm:

Pros:

Simple, not need to store intermediate state variables

Cons:

The tag identification delay is affected by tad ID distribution and length



# Chapter 4+ Checksum

1. Parity checking

– A parity bit is incorporated into each byte

– 9 bits are sent for every byte

– odd parity: an odd number of the 9 bits have the value 1

– even parity: an even number of the 9 bits have the value 1

– simple

– poor error recognition

• an odd number of inverted bits (1,3,5, …) : detected

• an even number of inverted bits (2,4,6,…) : the errors cancel

appear to be correct.

a parity generator for even parity: the XOR logic gating of all the data bits in a byte ， for odd parity: invert the output

2. LRC procedure

longitudinal redundancy check (LRC) procedure

• The XOR checksum is generated by the recursive XOR gating of all the data bytes in a data block.

• Byte 1 is XOR gated with byte 2, the outcome of this gating is XOR gated with byte 3, and so on.

• If the LRC value is appended to a data block and transmitted with it, then a simple check for transmission errors can be performed in the receiver by generating an LRC from the data block + LRC byte.

• The result of this operation must always be zero; any other result indicates that transmission errors have occurred.

·can be calculated very simply and quickly

• not very reliable because it is possible for multiple errors to cancel each other out, and the check cannot detect whether bytes have been transposed within a data block

• primarily used for the rapid checking of very small data blocks (e.g. 32 byte)

3. CRC procedure

– CRC (cyclic redundancy check) procedure : originally used in disk drives

– excellently suited for error recognition

– highly reliable method of recognizing errors

– cannot correct errors

– A CRC checksum is calculated by the division of a polynomial using a so-called generator polynomial.

– The CRC value is the remainder obtained from this division.

·advantage : reliability of error recognition

A16-bit CRC : checking the data integrity of data blocks up to 4Kbytes in length

RFID systems : data blocks, shorter than 4Kbytes, 12- and 8-bit CRCs

**Coding and modulation**

·From the reader to the transponder

– signal coding and the modulator in the reader (transmitter)

– the transmission medium (channel)

– the demodulator and signal decoding in the transponder (receiver)

·Signal coding

– matches the message optimally to the characteristics of the transmission channel

– protection against interference or collision

– protection against intentional modification

– coding in the baseband

·Modulation

– altering the signal parameters of a high frequency carrier

– amplitude

– frequency

– phase

·The transmission medium

– transmits the message over a predetermined distance

– magnetic fields (inductive coupling)

– electromagnetic waves (electromagnetic backscatter coupling)

·Demodulation

– reclaim the signal in the baseband

– contain both a modulator and a demodulator

– modem (modulator – demodulator)

·Signal decoding

– reconstruct the original message from the baseband-coded received signal

– recognize any transmission errors and flag them

1 Coding in the baseband

◼ NRZ coding (Not Return to Zero)

– binary 1 : a ‘high’ signal

– binary 0 : a ‘low’ signal

◼ Manchester coding

– binary 1: a negative transition

– binary 0: a positive transition

– used for data transmission from the transponder to the reader, based upon load modulation using a subcarrier

◼ Unipolar RZ coding

– binary 1 : a ‘high’ signal during the first half-bit period

– binary 0 : a ‘low’ signal lasting for the entire duration of the bit

◼ DBP (differential bi-phase)

– binary 0 : a transition of either type in the half-bit period

– binary 1 : lack of a transition

– the level is inverted at the start of every bit period

– the bit pulse can be more easily reconstructed in the receiver

◼ Miller coding

– binary 1 : a transition of either type in the half-bit period

– binary 0 : continuance of the 1 level over the next bit period

– a sequence of zeros : transition at the start of a bit period

– the bit pulse can be more easily reconstructed in the receiver

◼ Modified Miller coding

– each transition : a negative pulse

– highly suitable for use in inductively coupled RFID

systems : data transfer from reader to transponder

– tpulse << Tbit , ensure a continuous power supply to the transponder during data transfer

◼ Differential coding

– binary 1 : a change (toggle) in the signal level

– binary 0 : the signal level remains unchanged

◼ Pulse-pause coding (PPC)

– binary 1 : a pause of duration t before the next pulse

– binary 0 : a pause of duration 2t before the next pulse

– popular in inductively coupled RFID systems: data transfer from the reader to the transponder

**2 Digital modulation procedures**

◼ Modulation

– influencing signal parameters – power, frequency, phase position – of an electromagnetic wave by messages (data)

◼ carrier : an unmodulated electromagnetic wave

◼ demodulation

– reconstruct the message

– analyzing the characteristics of an electromagnetic wave

– measuring the change in reception power, frequency or phase position of the wave

◼ Analogue modulation

– amplitude modulation

– frequency modulation

– phase modulation

◼ Digital modulation: used in RFID systems

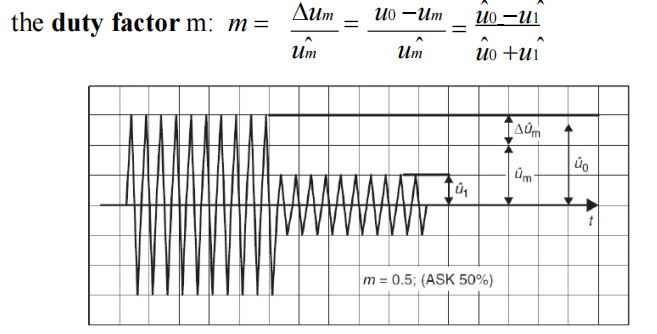
– ASK (amplitude shift keying)

– FSK (frequency shift keying)

– PSK (phase shift keying)

**1.Amplitude shift keying (ASK)**

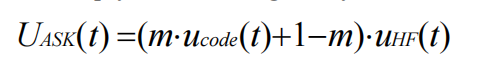
amplitude of a carrier oscillation : switched between two states u0 and u1, by a binary code signal.



In the case of duty factors <15% and duty factors >85%, the

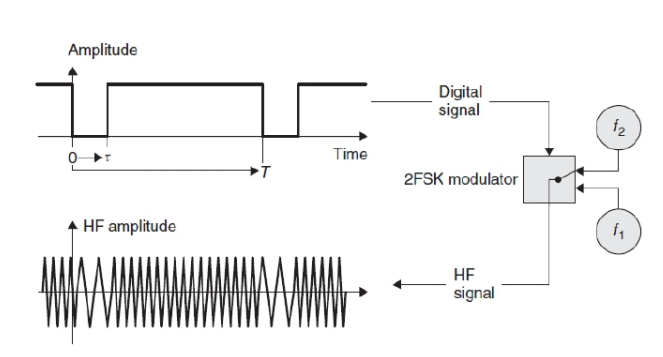
differences between the two calculation methods can be

disregarded.



**2. Frequency shift keying (FSK)**

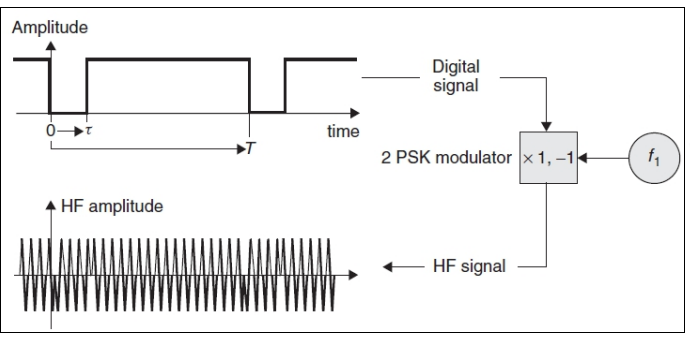
·2FSK, the frequency of a carrier oscillation : switched between two frequencies f1 and f2, by a binary code signal.

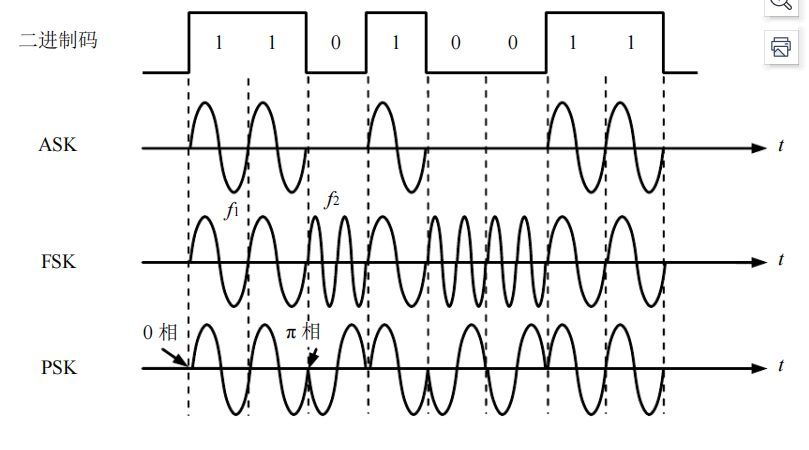


**3. Phase shift keying (PSK)**

– 2PSK: switched between the phase states 0°and 180 °

– corresponds with the multiplication of the carrier oscillation by 1 and -1





# Chapter 5

5.1 EPCglobal standard

· In 2003, Article Numbering Association International (EAN) and the Uniform Code Council (UCC) founded EPCglobal (converted from Auto-ID Center ), a worldwide, open nonprofit organization for the international implementation of EPCglobal Network

· Mission

– develop and oversee the standards of electronic product codes (EPC) by using the RFID technology

– provide registry service of the codes

– coordinate with ISO for their review and ratification

·The **EPCglobal Network** is a technology that

– allows trading partners to document and determine the location of individual goods

– if possible in real time additional information

– production and use-by date of a product

– can be exchanged between trading partners

·The EPCglobal Network defines and uses the following five basic services：

– Electronic product code (EPC): a unique number for Identifying individual objects

– The identification system

• transponder : attached to products , contains the EPC

• reader : read out the EPC , route it via EPC middleware into the network

– EPCglobal Middleware : administrates the information made available by readers , a software interface

– Discovery Service (DS): a group of services

• allow users to find data regarding a certain EPC in the EPCglobal Network

·Object Naming Service (ONS)

– EPC Information Services (EPCIS)

• allow users to exchange EPC-related data via EPCglobal Network with their trading partners

·**EPC: Electronic Product Code**

– naming and identification scheme

– enable the unique identification of all objects combination of three unique numbers

– Domain Manager number

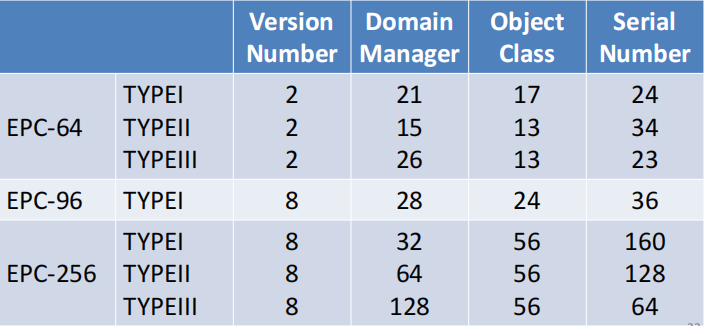
– Object Class number

– Serial number

· **Domain Manager number + Object Class number + Serial Number:** uniquely identifies an object

·Version Number: indicates the number of bits contained in each of the remaining three partitions

Domain Manager, Object Class, and Serial Number







Transponders: classified according to functionality

There are the following classes:

Class 0 Passive read-only transponder with 64-bit or 96- bit EPC.

Class 1 Passive transponders, write once read many with 64-bit or 96-bit EPC.

• A ‘kill’ function that permanently disables the Tag

• Optional password-protected access control

• Optional user memory

Class 2 Passive transponders with the following anticipated features above and beyond those of Class 1 tags

• An extended Tag ID

• Extended user memory

• Authenticated access control

• Additional features (TBD) as will be defined in the Class 2 specification

Class 3 Semi-passive transponders with the following anticipated features above and beyond those of Class 2 tags

• An integral power source

• Integrated sensing circuitry

Class 4 Active transponders with the following anticipated features above and beyond those of Class 3 tags

• Tag-to-Tag communications

• Active communications

• Ad-hoc networking capabilities



**EPC Gen 2** EPCglobal UHF Class-1 Generation-2 ：used for item identification in retail environments

“Class-1” : the functionality of the tag

“Gen-2” : the physical and logical standards of tag and the encompassing system

· The EPC Gen2 standard: adopted with minor modifications as ISO 18000-6C in 2006.

**·Basic procedures of the EPC Network**

·EPC: an identification number for an object moving through the supply chains ·all information about the object: administered in the EPCglobal Network

·each company in the EPCglobal Network: administers and controls the EPC data sets and object data

 · access rights to object data

– locally configured on the individual EPCIS

– accessed by trading partners with the corresponding privileges

·the manufacturer: attach the transponder to the product ①

·all data assigned to the product: stored in the manufacturer’s EPCIS ②

 ·EPCIS registers the entries with EPC Discovery Services : in

order to find the information in EPCglobal Network ③

·product: shipped to a retailer ④

·At the retailer’s goods-in point: the corresponding data are

stored in the retailer’s EPCIS ⑤

· registered by EPCIS with EPC Discovery Services ⑥

·the company prefix of the EPC attached to the product ①

·The company prefix : sent to the Root ONS ⑦

·Root ONS ⑦ -> Local ONS ⑧ -> the EPCIS ⑨

**5.2 EPCglobal Class 0**

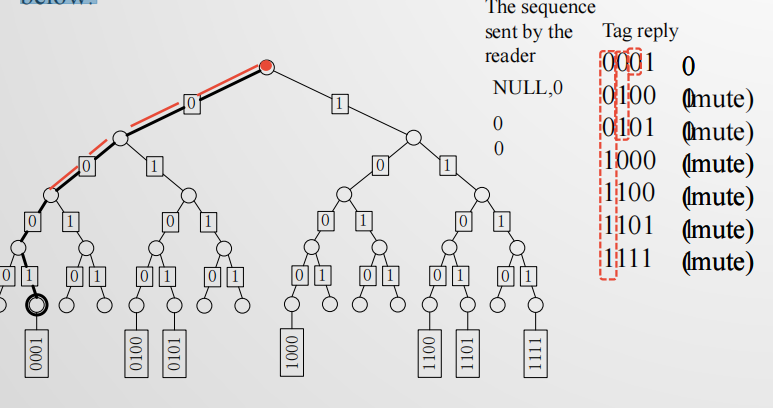
·EPCglobal Class 0 tags are read-only

·The information contained in it is written by the manufacturer and can not

be written by the user。

The EPC code (Electronic Product Code) includes 64 bits and 96 bits.

The EPCglobal Class 0 standard uses a **binary tree based variant algorithm** for media access control, and the access mode is shown below:



**5.3 EPCglobal Class 1 Generation 1**

·The EPC C1G1 tag is a passive tag, can reflect a unique ID to the reader.

·In the EPC C1G1 standard, it is assumed that all tags can be rewritten at least once.

·The EPC C1G1 tag may have 64 bits or 96 bits, and supports the LOCK and KILL commands.

·The EPC CIG1 standard uses a packet-based half-duplex protocol.

·The EPC C1G1 and EPCglobal Class 0 standards are not compatible, whether in tag

symbols, media access control, command sets, or in state diagrams

·The EPC C1G1 standard provides commands to improve the media access control process and has commands that can directly access the tag EPC code.

**PingID**: A mask filter is provided that specifies the starting position of the traversal process and the access to the tag.

**5.4 EPCglobal Class 1 Generation 2**

·The operating frequency of the RFID system which complies with the EPCglobal Class 1 Generation 2 (EPC G1G2) standard is at 860MHz ~ 960MHz.

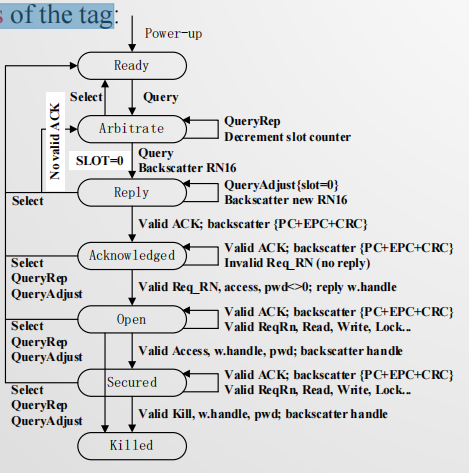
·The EPC C1G2 standard is dedicated to providing a unified approach to reading data from RFID tags, writing data to tags, and the tag communication.

·The physical layer communication interface in EPC C1G2 is the same as the one in the seven-layer model of the OSI protocol stack.

·There are two communication links in the EPC C1G2, namely, a reader-to-tag communication link and a tag-to-reader communication link. The two links are independent and have different data encoding schemes, data rates and data modulation modes

·The EPC C1G2 protocol standard is a half-duplex protocol that allows only one reader or one tag to send a signal in a single transmission.

·In the EPC C1G2 protocol standard, the behavior of a tag can be described by a finite state machine. The following are the seven states of the tag



·The EPC C1G2 uses dynamic frame slotted ALOHA anti-collision algorithms to reduce data corruption caused by collisions.

·The RFID system must allow multiple readers to communicate with the same tag.

·Session mechanism: In the EPC C1G2 standard, up to four readers can be allowed to communicate with the tag in the same time frame

·In the EPC C1G2 protocol, collecting the EPC code (ID) of tag is a very important operation.

**Four Commands to identify the tag.**

Select command

Query command

QueryRep command

QueryAdjust command

1.select:Defines the number of tags participating in the next query process and

selects the subset of tags that participate in the next round of queries.

The select command may allow the reader to change the selected flag or any one of the four flags stored in the tag( S0,S1,S2,S3)

2.Query command

Initiates a new identification process, identifies the set of tags that will participate in the next round of querying, and selects the tag-to-reader encoding way and data rate.

Specify the value of the SL flag and the value of the flag in a particular session.

The tag will participate in the next round of identification only if the flag

of the tag and the flag in a particular session are the same as those in the

query

3.QueryRep command

is used to indicate that the tag has entered the next time slot. When the tag command responds to the command, its own slot counter is decremented by 1, and when it is decremented to 0, the tag sends RN16 to the reader

4.QueryAdjust command is used to adjust the number of time slots and select a new time slot counter, or command instruct the tag to select a new time slot counter without changing the number of time slots. And it will not start a new round of inquiries

5.4.4 Select the specified tag

·The process of selecting a tag: The reader establishes a communication process with a specific tag for reading the EPC code or the advanced command (read, write, and secure command).

·The EPCglobal standard defines 11 different data encoding methods of tags. One of the data formats is a generic identifier (GID-96), which is a 96-bit EPC code



**5.4.5 Performance trade-offs**

Build a set of tags involved in the recognition process

• Select command and query command are required

Select the way of data encoding, for the readerto-tag, the tag-to-reader, the reader itself and the tag itself

• Depends on the RF environment where the system is working（RF environment）

**Identify and access tags with the same type**

**Identify and access multiple types of tags from one manufacturer**

**Identify and access multiple types of tags from multiple manufacturers**