目录

[Chapter 1 1](#_Toc21871)

[Chapter 2 3](#_Toc23293)

[Chapter 3 6](#_Toc23205)

[Chapter 4 8](#_Toc23337)

[Chapter 5 14](#_Toc2521)

# Chapter 1

**·Comparison of different automatic identification technologies**

**·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.

·**Constraints of RFID technology**

1.limited tag resources : computing ability, storage space, communication bandwidth

2.performance in a real environment is susceptible to many factors

Reader’s transmitting power,

energy absorption, path loss, multipath effect,

Distribution and deployment of tags,

Signal interference

**·Core technologies 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

**·The advantage of RFID in IoT**

·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" .

**·the development trend**

1.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

# Chapter 2

**·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

**·Reader’s classification: by working frequency, by appearance**

**·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

**·Influencing factors of R&W range**

The way that antenna is coupled

The output power of the reader’s RF signal

The frequency of RF carrier signal

**·Reader’s components and their functions: signal processing and control module, RF modules (two types)**

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

·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.Radio Frequency Module

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

Transmitter signal channel and Receiver signal channel

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 types: Inductively Coupled RF Module ,Electromagnetic Backscatter Coupled RF Module

**·Tag’s functions**

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

**·Tag classification: by package form, by power source, by work frequency, by R&W** **capability**

**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

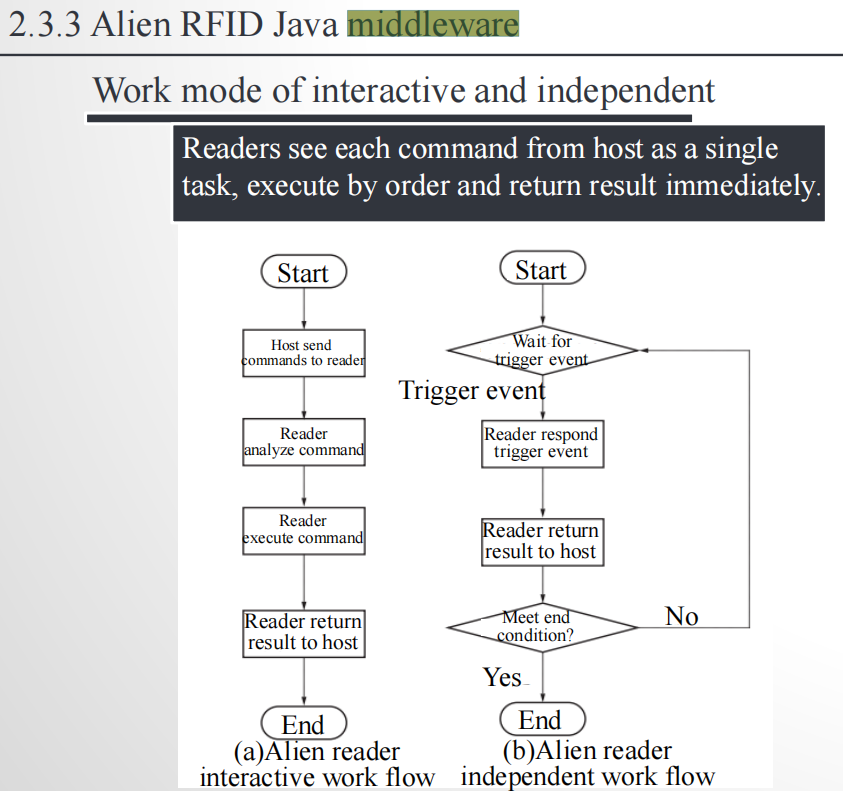
• Readable, writable

• Complex structure

• High cost

• No database related

**·Two work modes of RFID middleware**



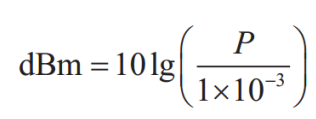
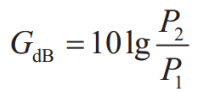
# Chapter 3

**·Different work principles of different carrier frequency**

• 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

**·Signal voltage and energy: dB, dBm，重点：如何计算**



**·Modulation of reader signal: OOK and its problem, solution: PIE; Tag encoding: FM0**

**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

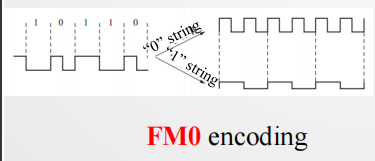
“0”：output a short time of high power followed by a short time of low power

Problem:interference

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

FM0：

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

**·Link budget (重点)**

forward link budget and backward link budget

·Reader’s transmit energy

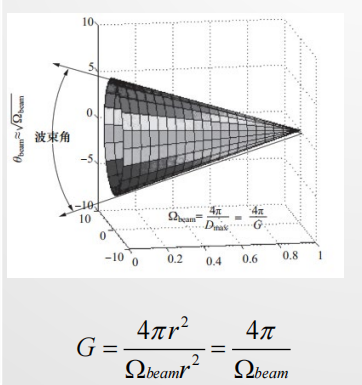
·Path loss

·Tag activate energy

**·Antenna gain and polarization, EIRP**

**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.





**·Effects of antenna gain，重点：分析 link budget，几个计算公式？？？**

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

# Chapter 4

**·Difficulty of traditional anti-collision algorithms for solving collision detectio**n between RFID tags :signal interference. (Conflict interference among readers+ tags)

**·TDMA, FDMA, CSMA**

Time Division Multiple Access （TDMA)

Frequency Division Multiple Access（FDMA)

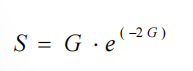
Carrier Sense Multiple Access （CSMA)

**·ALOHA based protocols: pure ALOHA, S-ALOHA, FSA, DFSA, Q 算法。重点：性能分析、执行过程**

**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.

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

**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.

maximum of 36.8%: offered load G=1

REQUEST ,SELECT(SNR) ,READ\_DATA

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.

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.

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.

**·Binary tree based protocols: BT, QT, 重点：执行过程**

The basic idea of Binary tree based anticollision 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.

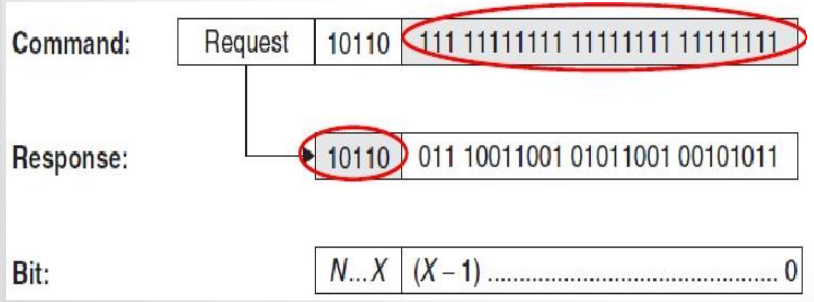
**·Dynamic binary search,** 重点：执行过程

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.

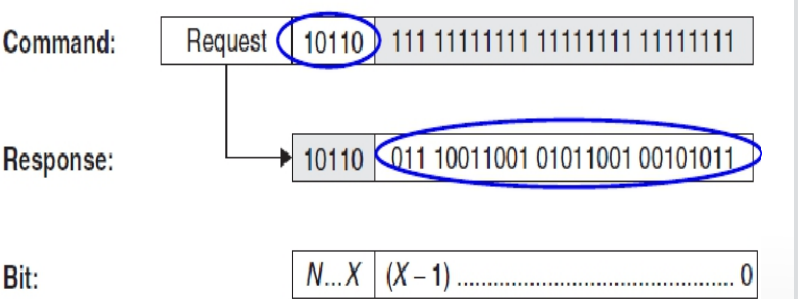


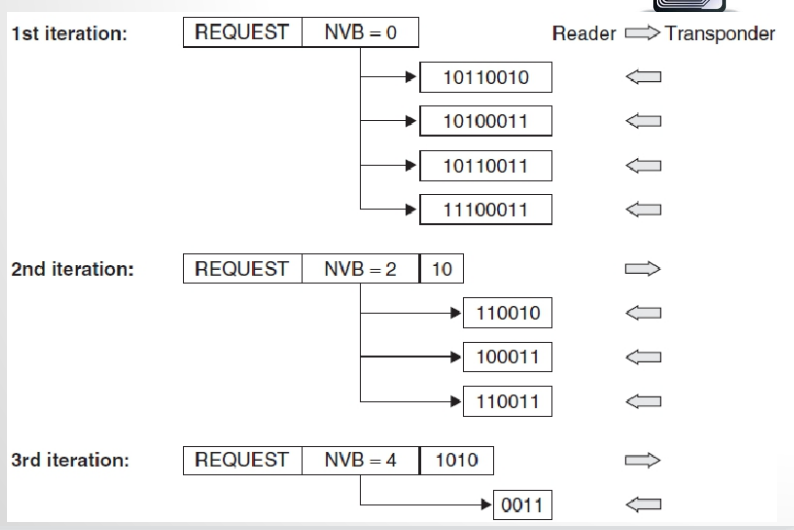
The reader : sends only the known part (N − X) as the search criterion

– 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





**·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

**·Checksum procedure: parity checks, LRC, CRC**

**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

each other out, appear to be correct.

a parity generator for even parity: the XOR logic gating of

all the data bits in a byte

– 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

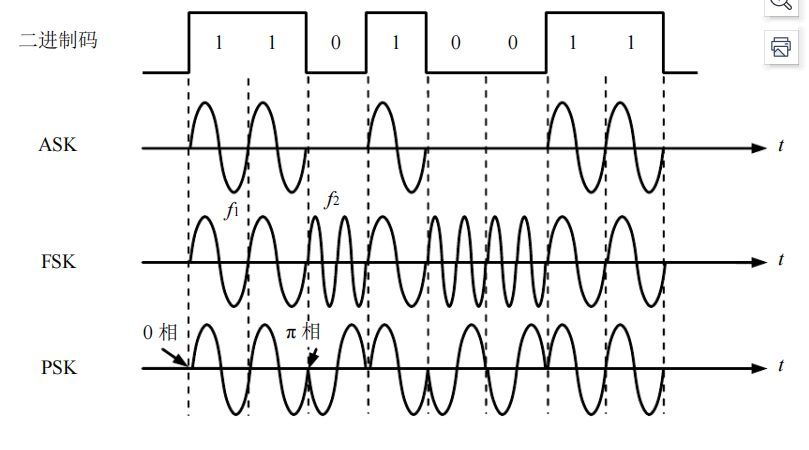
A16-bit CRC : checking the data integrity of data blocks

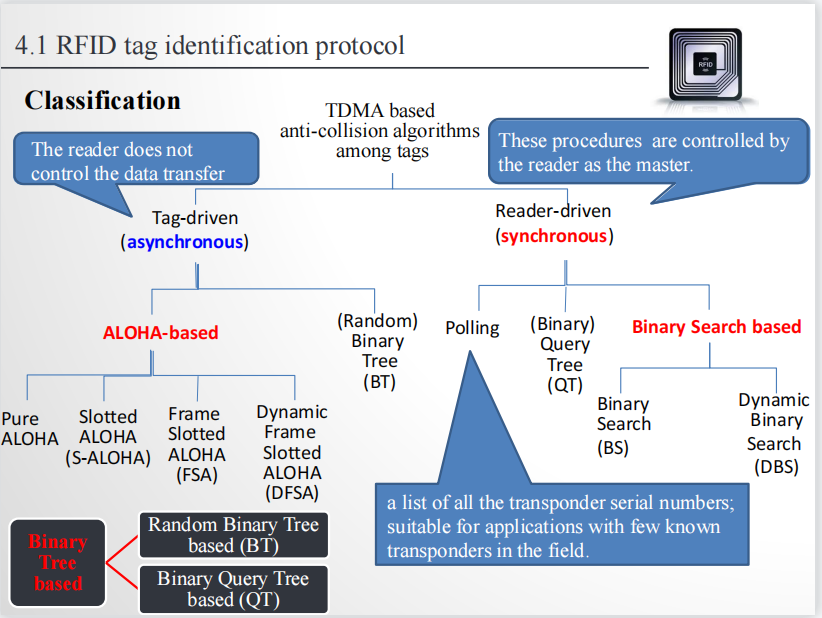
up to 4Kbytes in length

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

8-bit CRCs

**·ASK, FSK, PSK**





# Chapter 5

**·Concept of EPC global network**

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

**·Five basic services of EPC global network, interaction of different components of EPCglobal network**

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

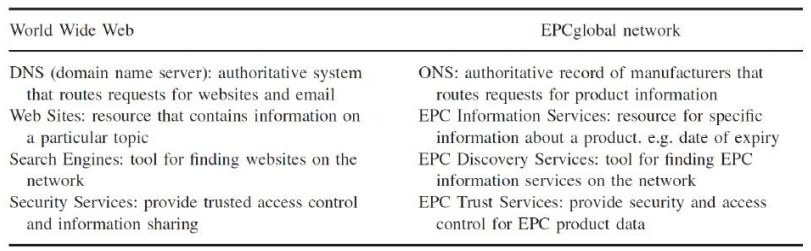
• allow users to find data regarding a certain EPC in the EPCglobal Network

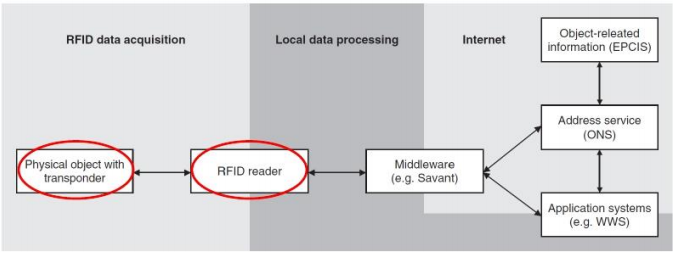
·Object Naming Service (ONS)

– EPC Information Services (EPCIS)

• allow users to exchange EPC-related data via EPCglobal

Network with their trading partners





**·EPC code**: Domain Manager Number + Object Class Number + Serial Number

**·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

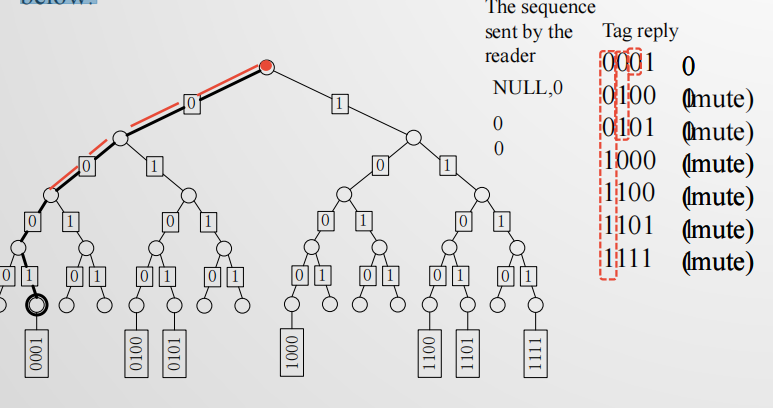
· registered by EPCIS with EPC Discovery Services ⑥

·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

**·Binary tree based variant algorithm for EPCglobal Class 0**



BT，tag随机选择0、1加到自己的寄存器里，tag 选01。这里： reader选择0，1发送给tag

QT:前缀逐渐扩大前缀，这里：每次只发送一个bit，

**·EPCglobal C1 G1: PingID; C1G2: four commands (是什么，分别干什么用的), two types of performance trade-offs**

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

**4 commands:**

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

**two types of 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 reader

to-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