



# RFID Applications

## Module III

### Syllabus :

Introduction, Concept and technology: RFID, transponder, RFID architecture, RFID applications i.e. Logistics and supply chain, Production, Monitoring and maintenance, Product safety, Quality and information, Access control and tracking and tracing of individuals, Payment, Loyalty, Household etc., Hardware, Hardware issues, Protocols : Pure aloha, Slotted aloha, Frame slotted aloha, Tree protocols, Tree splitting algorithms, Binary search algorithm, Bitwise arbitration protocols, Main query tree protocols.

## 3.1 Introduction

- In recent years' automatic identification procedures (Auto-ID) have become very popular in many service industries, purchasing and distribution logistics, industry, manufacturing companies and material flow systems.
- Procedure that exist to provide information about people, animals, goods and products in transit is Automatic identification.
- The technically optimal solution would be the storage of data in a silicon chip.
- The most common form of electronic data-carrying devices are used in everyday life is the smart card based upon a contact field (telephone smart card, bank cards).
- However, the mechanical contact used in the smart card is often impractical. A contactless transfer of data between the data-carrying device and its reader is far more flexible.
- In the ideal case, RFID systems (radio frequency identification) are called as, the power required to operate the electronic data-carrying device will also be transferred from the reader using contactless technology because of the procedures used for the transfer of power and data, contactless ID systems. RFID is a very valuable business and technology tool. It holds the promise of replacing existing identification technologies like the bar code.
- RFID can track inventory in the supply chain more efficiently, provide real-time in-transit visibility, and monitor general enterprise assets that can offers strategic advantages for businesses.

### 3.1.1 RFID

The term RFID refers to Radio Frequency Identification, a technology which uses radio waves to automatically identify items or people. RFID tag and a reader device are the most common uses.

### 3.1.2 Working of RFID System



In general terms, Radio Frequency Identification systems consist of an RFID tag (typically many tags) and an interrogator or reader. Waves are absorbed by the tag because the interrogator emits a field of electromagnetic waves from an antenna. The absorbed energy is used to power the tag's microchip and a signal that includes the tag identification number is sent back to the interrogator.

### 3.1.3 Benefits of RFID over Traditional ID Technologies Such as Bar-coding and Human Readable Formats

RFID technology can offer many benefits over more traditional approaches. Specific benefits are dependent on the type of RFID technology that is used and the application of the technology. Some benefits that may be recognized in utilizing RFID are :

1. Faster read rates
2. None line of sight reading
3. Multiple tag reads
4. Programmable and re-programmable tags
5. Enhanced security functionality

### 3.1.4 Key Differences between RFID Solutions

- Unsurprisingly the key difference between these solutions is the frequency at which the interrogator emits a field and at which the tags are operational.
- Through a combination of physical limitations and development profiles these technologies provide different functionality and benefits.
- For example, HF tags can typically only be integrated at a distance of up to 0.8m (2.6ft) whilst UHF tags can be read up to 15m (50ft) from a reader. This said, HF tags typically use larger silicon chips, which provide greater security functionality than current UHF solutions.

### 3.1.5 Passive and Active RFID Solutions

- Again the clue is in the terminology, passive RFID tags work on the basis that they absorb the power from the reader and use this to empower the microchip and re-emit a signal.
- Active tags contain a battery, which powers the chip and transmits to the interrogator. As a consequence, passive technology tends to be significantly lower cost but restricted to modest read distances, whereas active solutions are capable of reading over hundreds of meters.

### 3.1.6 Limitations

1. Traditional LF and HF tags do not function on metals and traditional UHF tags do not function on metals or polar liquids (such as water). This is due to tag detuning as a result of coupling between the tag and object to which it is attached.
2. The modern RFID tag technology that alleviates this issue offers a fundamentally different approach to passive UHF tag design, which alleviates this issue.

### 3.1.7 A Comparison of Different Identification Systems



Table 3.1.1

System parameters	Barcode	OCR	Voice Recognition	Biometry	Smart card	RFID Systems
Typical data quality (bytes)	1-100	1-100	-	-	16-64 k	16-64 k
Data density	Low	Low	High	High	very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very High	-	-	Possible (contacts)	No Influence
Influence of (optical) covering	Total failure	Total Failure	-	Possible	-	No Influence
Influence of direction and position	Low	Low	-	-	Unidirectional	No Influence
Degradation/wear	Limited	Limited	-	-	Contacts	No Influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorized copying /modification	Slight	Slight	Possible	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low ~4 s	Low ~3 S	Very low >5 s	Very low >5-10 s	Low ~4 s	Very fast ~0.5 s
Maximum distance between data carrier and reader	0-50 cm	<1 cm Scanner	0-50 cm	Direct contact *	Direct contact	0-5 m, microwave

### 3.2 Concept and Technology of RFID System

- RFID systems are closely related to the smart cards.
- Like smart card systems, data is stored on an electronic data-carrying device – the transponder. However, unlike the smart card, the power supply to the data-carrying device and the data exchange between the data-carrying device and the reader are achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields.
- The underlying technical procedure is drawn from the fields of radio and radar engineering. The abbreviation RFID stands for radio frequency identification, i.e. information carried by radio waves. Due to the numerous advantages of RFID systems compared with other identification systems, RFID systems are now beginning to conquer new mass markets.
- One example is the use of contactless smart cards as tickets for short-distance public transport.

- The operating principle of RFID systems is based on the remote exchange of electromagnetic waves. Specifically, the reader transmits a signal at a given frequency to one or more radio tags located in its reading field and they also transmit a signal back. The electromagnetic field feeds the label and activates the chip.
- To transmit the information recorded in the chip, the chip creates an amplitude or phase modulation on the carrier frequency. Once this information is received by the reader, it transforms it into binary code. The operation remains symmetrical in the opposite direction.
- The scenario of a radio frequency identification is therefore as follows :

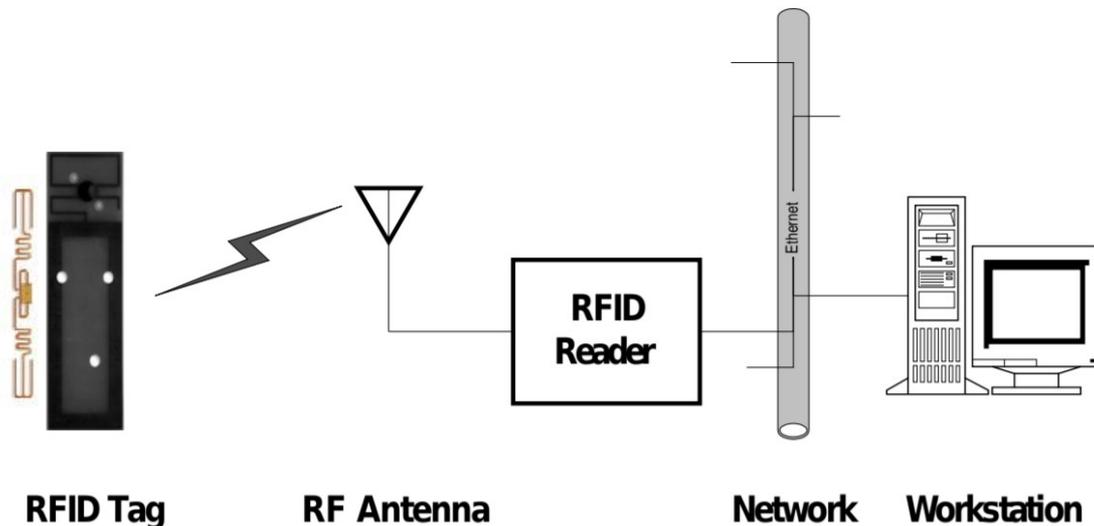


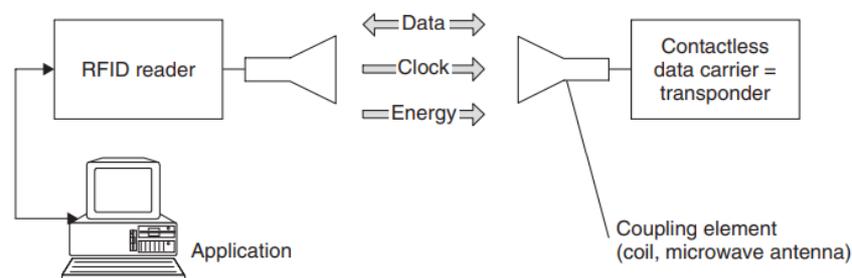
Fig. 3.2.1 : RFID system components

- The reader transmits energy by radio to activate the tag.
- It queries the tags nearby.
- It listens to the answers and eliminates duplicates or collisions between answers.
- Finally, it transmits the results obtained to the concerned applications.

### 3.3 RFID System Architecture Components

An RFID system is always made up of two components :

1. The transponder, which is located on the object to be identified;
2. The interrogator or reader, which, depending upon the design and the technology used, may be a read or write/read device. The data capture device is always referred to as the reader, regardless of whether it can only read data or is also capable of writing.

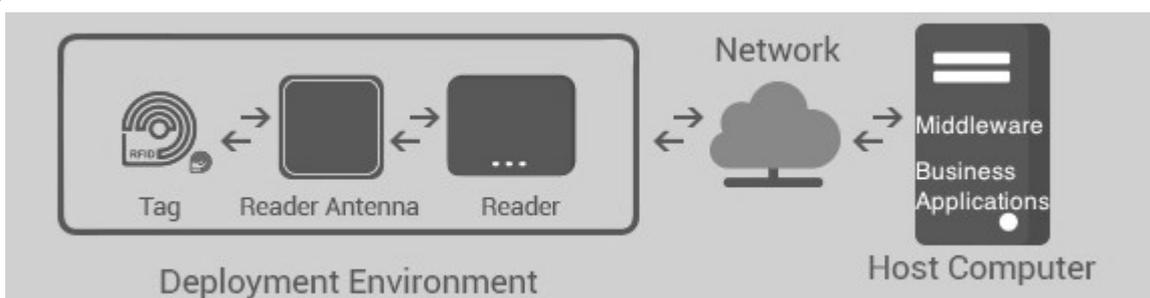


**Fig. 3.3.1 : The reader and transponder are the main components of every RFID system**

- Reader (also known as an Interrogator) – to read and write to tags.
- One or more reader antennas – transmits the reader power and commands to tags and receives data from tags.
- Cable to connect reader antennas to the reader (unless the antenna is integrated into the reader).
- Tags that are placed on or in an object.
- A software application to transfer data from the reader to the system that will process the data, usually referred to as the “middleware”.

#### **Additional components can include**

- **RFID Printer Encoder** : To print labels and encode RFID tags.
- **Barcode Scanner** : To scan barcode labels for association with the RFID tag.
- **Input / Output Devices** : Light stacks, sounds devices, triggers and sensors.
- System applications (that often encompass some or all middleware functions) and enterprise applications.

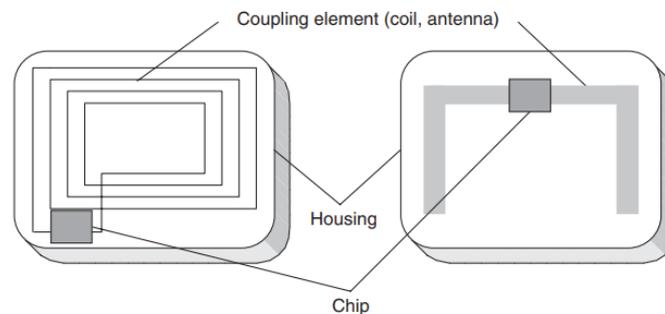


**Fig. 3.3.2 : Conceptual RFID system architecture**

#### 3.3.1 Transponder

- The transponder, which represents the actual data-carrying device of an RFID system, normally consists of a coupling element and an electronic microchip.
- When the transponder, which does not usually possess its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive.
- The transponder is only activated when it is within the interrogation zone of a reader.

- The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.



**Fig. 3.3.3 : Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna.**

### 3.3.2 RFID Tags

- **RFID Tag** : A microchip attached to an antenna and packaged so that it can be attached to an object. Programmed with a unique serial number, an RFID tag receives signals from a tag reader and sends signals back to the reader. When RFID tags enter the reader's field they immediately announce their presence by reflecting back a signal, which is useful in an environment where items are moving quickly. RFID tags can be active, passive or semi-passive.
- Passive, semi-passive, active tags
  - **Passive Tag** : Passive tags require no power source other than the one provided by the reader. Earlier, the reading operation of passive tags was limited to a distance of about 10 meters, but now, thanks to technologies used in communications systems, this distance can extend up to 200 meters. The reader sends energy to the tag, along with an interrogation signal that the tag responds to. Passive tags operate in read-only mode (like linear barcodes). In this case, the antenna captures some frequencies which provide enough energy to issue its unique identification code. The passive tags are programmed with data which is not modifiable, with a capacity of 32 to 128 bits.
  - **Battery Assisted Tag** : These RFID tags incorporate batteries and use the battery power to run the tag circuitry and sometimes an onboard sensor. They communicate with the tag reader using the same backscatter technique as passive tags though they have a longer read range because all of the energy gathered from the reader is reflected back to it. Also known as "semi-passive RFID tags."
  - **Semi-Passive Tag** : RFID tags where the battery operates the microchip's circuitry but is not used to send a signal to the tag reader. By "sleeping" until they receive a signal from the reader, semi-passive tags conserve battery life.
  - **Active Tag** : An RFID tag that uses a transmitter to return information as opposed to reflecting a signal back from the reader as a passive tags do. Most active tags are battery powered, though they may gather energy from other sources. Active tags can be read from up to 300 feet.
  - **Semi-active tag** : Semi-active tags do not use their battery to transmit signals. They act as passive tags at the communication level. However, the battery allows them, for



example, to store data during transport. These tags are used for the product shipments under a controlled temperature and to record the temperature of goods at regular intervals. These tags stay in the idle mode until they receive an activation message from the reader.

- **Quiet Tag** : RFID tags that are only readable with reader output at full power, or which can be read only at very close range.

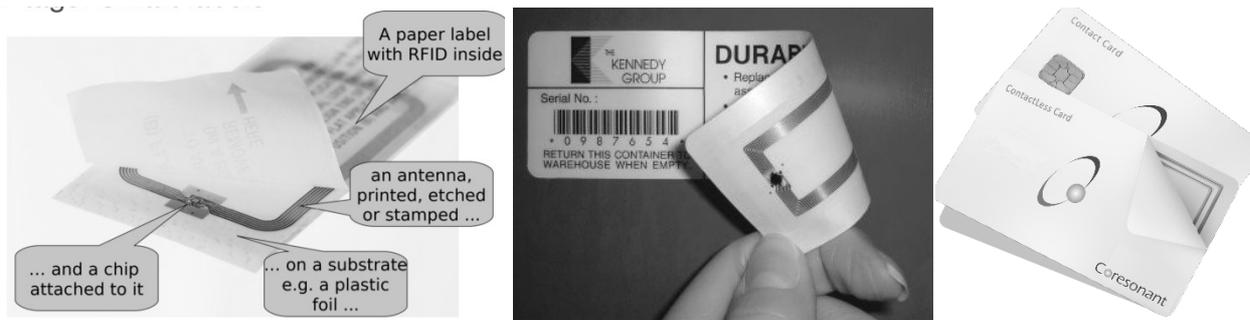


Fig. 3.3.4 : RFID tags : Smart label and card



Fig. 3.3.5 : Shows different types of RFID tags available in market

- Various frequencies - LF, HF, UHF, Microwave, UWB
  - Read distance is very much driven by the technology that is implemented (frequency of the RFID system) and the specific components that are put into use.
  - As a guideline :
    - (a) LF passive — 0-0.5m
    - (b) HF passive — 0-0.8m
    - (c) UHF passive — 0-15m
    - (d) Active — 50m+
- Performance dependent on environment, tagged materials and tag position
  - Environment
    - (a) A lot of metal - reflections, interference, diminished read range, or reading what's not desired - solved by shielding, tuning, antenna tilt.



- (b) A lot of water or aqueous liquids/moist materials (incl. wood) – detuning, absorption, diminished read range – design considerations like line of sight, tuning power, angling antennas and adding read points.
  - (c) Other readers in the environment – interference, diminished read range, data rate, tag reads – solved by dense reader mode, tuning power, gain, etc.
- Tagged materials – can interfere with tag operation due to detuning the tag
  - (a) Metals – tag is detuned to the point that it does not respond (the metal surface interferes with the tag’s antenna), in addition metal blocks signal.
  - (b) Aqueous liquids in thin containers, condensation or moist materials – tag is detuned.
  - (c) Solution – use tags specifically tuned/made for metals or moist materials – these are specifically tuned and /or offset from surface to ensure a proper performance.
- **Tag position** : Sometimes the tag can be placed in a position where the RF signal from the reader has hard time powering it. The tag must be (as much as possible) parallel to the surface of the reader antenna (perpendicular to the RF waves) and if linear antenna is use, the tag’s dipole has to be in the same plane.
- **Error Correcting Code** : Code stored on an RFID tag to enable the reader to determine the value of lost or scrambled data.
- **Far-Field Communication** : RFID tags farther than one full wavelength away from the tag reader are said to be “far field”, within one full wavelength away is “near field.” Far field signals decay as the square of the distance from the antenna, while the near field signals decay as the cube of distance. Passive RFID tags that use far field communications (UHF and microwave systems) have a longer range than tags using near field communications (low and high frequency systems).
- **Read Only tag** : RFID tag memory that cannot be altered unless the microchip is reprogrammed.
- **Read Write tag** : RFID tags that can store new data, often used on reusable containers and other storage assets. When the contents of the container are changed, new information is written to the tag.
- **EPC Global RFID Class Structure**

Class of Tag	Tag type	Description
<b>Class 1</b>	Passive identity tag	A simple, passive and read only non-volatile memory
<b>Class 2</b>	Passive functional tag	Extension of class 1 tag with up to 65KB of read-write memory
<b>Class 3</b>	Semi-Passive tag	Extension of class 2 tag with a built-in battery power to increase the read range
<b>Class 4</b>	Active Ad-hoc tag	A built-in battery power to activate the circuit and power the



		transmitter for broadcasts a signal to reader
<b>Class 5</b>	Reader tag	A built-in power, able to communicate with other class 5 tags and devices

### - RFID Characteristics

Air-interface frequency	ISO	Tagging mode	Effective read range	Transfer rate	Penetrating capability
<b>LF (125-135kHz)</b>	18000-2	Passive	Short read range (less than 0.5m)	Low	Can read through liquid but not metal
<b>HF (13.56MHz)</b>	18000-3	Passive	Medium read range (up to 1.5m)	Moderate	Can read through liquid but not metal
<b>UHF (860-930MHz)*</b>	18000-6	Passive	Medium read range (up to 5m)	Moderate to High	Cannot read through liquid or metal
<b>UHF (433MHz)</b>	18000-7	Active	Ultra long read range (up to 100 m)	High	Cannot read through liquid or metal
<b>Microwave (2.45GHz)</b>	18000-4	Active	Long read range (up to 10m)	Very high	Cannot read through liquid or metal

\* Due to the national difference of air frequency usage regulation, RFID in 868 MHz is generally used in European countries and 915 MHz is used for non-European countries.

### 3.3.3 Classification of RFID Systems Based on their Operating Frequencies

Sr.	Criterion	LF	HF	UHF	Microwave
1.	Frequency range	<135 kHz	13.56 MHz	860 - 930 MHz (1)	2.45 GHz
2.	Physical coupling	Inductively-coupled systems.		Backscatter systems.	
3.	tag to reader communication	A tag uses load modulation to retrieve its ID and uses AM during transmissions.			
4.	Tag	Passive		Active, passive,	Active, passive



Sr .	Criterion	LF	HF	UHF	Microwave
	characteristics			semi-passive	
5.	Communication boundary	Near Field		Far field	Far field
6.	Approximate read range (passive tags)	2 m	0.1 m - 0.2 m	4 m - 7m	1 m
7.	Standards specifications	ISO 18000-2	ISO 18000-3 Auto ID HF class 1	ISO 18000-6 Auto, class 1 ID class 0, Class 1	ISO 18000-4
8.	Antenna components	coil (>100 turns)	Coil (<10 turns) and capacitor.	Dipole antenna	Dipole antenna
9.	Antenna technology	Air-core or ferrite-core coil	Perforated, printed, etched	Perforated, etched, printed	Printed antenna, etched
10.	Effect on human body and water	None	Attenuation	Attenuation	Attenuation
11.	Effect of metal	Disturbance	Disturbance	Attenuation	Attenuation
12.	Data transfer rate	<10 kbit/s	<100 kbit/s	<100 kbit/s	<200 kbit/s
13.	Cost considerations	A larger antenna is required as compared to other RFID systems, resulting in high tag cost.	Less expensive than LF tags. Best suited for applications that require moderate range.	UHF tags are cheaper than LF or HF tags due to recent advances in IC design.	Microwave systems are expensive as compared to LF, HF and UHF RFID systems
14.	Typical RFID applications	Animal tagging, vehicle identification, and container tracking in waste management.	Access control, smart cards, item tagging, ticketing, document tracking, baggage control, laundries and libraries.	Baggage handling, toll collection and supply chain management.	Electronic toll collection, real time goods tracking and production line tracking
15.	No. of tags read per	Lowest	Low	high	Highest



Sr .	Criterion	LF	HF	UHF	Microwave
	second				
1 6.	Tag power consumption	Lowest	Low	High	Highest
1 7.	Passive tag size	Largest	Large	Small	Smallest
1 8.	Orientation sensitivity	Least	low	high	Most
1 9.	Bandwidth	Lowest	Low	High	Highest

### 3.3.4 Classification of RFID Systems According to Tag Types

RFID Systems	Passive	Semi-Passive	Active
<b>Tags</b>	Passive tags have no power source and on-board transmitter. They use the power emitted from the reader to energize and transmit their stored data to the reader.	Semi-passive tags use an on-board power source to activate a tag's microchip. However, for data transmissions, backscattering is used.	Active RFID tags have an on-board power source such as a battery or solar power. The power source is used to transmit data to a reader. Hence, they do not rely on the reader's emitted power for data transmissions.
<b>Transceiver on Board</b>	No		Yes
<b>Communication Model</b>	Reader talks first (RTF).		Tag talks first (TTF). The presence of a reader is not necessary for data transmissions.
<b>Communication Principle</b>	Either inductive coupling or backscatter (Near or far Field)	Backscatter (Far Field)	Neither backscatter nor inductive coupling. Tag generates electromagnetic waves on their own.
<b>Tag to</b>	Communication from reader to tags is achieved by		Tags have an on-board



RFID Systems	Passive	Semi-Passive	Active
<b>Reader Communications</b>	modulating electromagnetic or magnetic waves.		transmitter and does not rely on a reader's waves.
<b>Reader to Tag Communication</b>	Communication from reader to tags is achieved by turning electromagnetic or magnetic energy waves off for short gaps of time. Tags detect these gaps as commands sent by the RFID reader.		Tags are able to communicate independently, and do not rely on the reader.
<b>Operating Frequency</b>	LF, HF, UHF, Microwave	UHF	UHF, Microwave
<b>Tag size</b>	Thin, flexible		Large, bulky
<b>Read Range</b>	0.1m - 7m	60m - 80m	More than 100m
<b>Tag Cost (USD)</b>	0.15 - 1	0.75 - 2.00	10 - 100
<b>System Cost</b>	Lowest <-----> Highest		
<b>System Complexity</b>	Lowest <-----> Highest		

### 3.3.5 Antenna

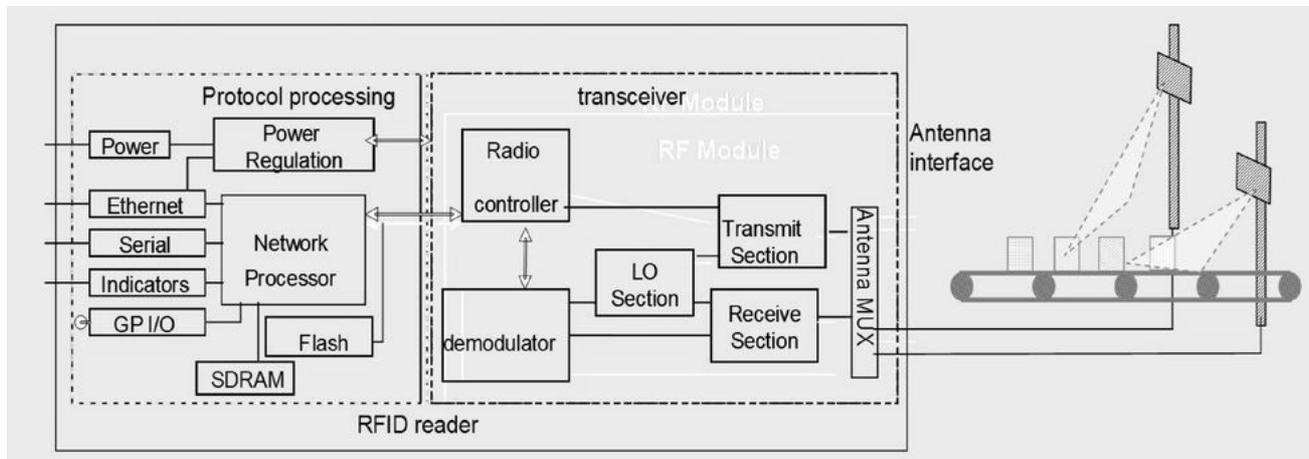
- **Antenna** : The conductive element to send and receive tag data. Passive low- frequency tags (135 kHz) and high-frequency tags (13.56 MHz) use a coiled antenna that couples with the coiled antenna of the reader to form a magnetic field. Readers have antennas that are used to emit radio waves. The RF energy from the reader antenna is “harvested” by the tag antenna and used to power the tag microchip to reflect back its signal back to the reader.
- **Dipole** : Antenna consisting of two straight electrical conductors or “poles”. The antenna is typically 1/2 wavelength from end to end. In an RFID transponder the antenna is connected to a microchip.
- **Dual dipole** : An antenna that contains has two dipoles. The goal of the dual dipole design is to reduce the tag's orientation sensitivity.
- **Folded dipole** : A dipole antenna in which the two poles are connected to each other, as well as to the microchip.
- **Antenna Gain** : The power ratio at the input of a loss-free reference antenna to that supplied to the input of the given antenna to produce, in a given direction, the same field strength at the same distance. Expressed in decibels. The higher the gain the more energy output. Higher gain antennas can read RFID tags from farther away.

### Types of Antenna



1. **Circular-polarized antenna** : A UHF reader antenna that produces radio waves in a circular pattern. As the waves move in a circular pattern, they have a better chance of being received, though circular-polarized antennas have a shorter read range than linear-polarized antennas. Used in situations where the orientation of the tag to the reader cannot be controlled.
  2. **Isotropic antenna** : Isotropic antennas radiate energy equally in all directions.
  3. **Linear-polarized antenna** : An antenna designed to focus radio energy from the reader in one orientation or polarity, thereby increasing the read distance and providing increased penetration through dense materials. In order to be read accurately, RFID tags designed to be used with a linear polarized antenna must be aligned with the reader antenna.
  4. **Patch antenna** : A square reader antenna made from metal or foil.
  5. **Slotted antenna** : An antenna designed as a slot cut into an electrical conductor connected to the transponder. Slotted antennas have the same orientation sensitivity as dipole antennas.
- **Inductive Coupling** : The transfer of energy from one circuit to another through mutual inductance. In RFID systems using inductive coupling, the tag reader antenna and the RFID tag antenna each have a coil which together forms a magnetic field so that the tag draws energy from the field to change the electrical load on the tag antenna. The change is picked up by the tag reader and read as a unique serial number.
  - **Conducted Power** : The RF power supplied by an RFID system to the antenna. It is measured at the cable to antenna connection. In the U.S., Federal Communication Commission regulations limit maximum conducted power to 1 watt.
  - **Effective Isotropic Radiated Power (EIRP)** : A measurement of RFID tag reader antenna output which is usually expressed in watts is known as EIRP.
  - **De-Tune** : When a UHF antenna is placed close to metal or metallic material, the antenna can be detuned to better receive RFID waves of a certain length from a reader so that the RFID tag can be read, but results in poor performance.
  - **Harvesting** : The way passive RFID tags gather energy from RFID reader antennas.
  - **Orientation** : Position of a reader antenna in reference to a tag antenna. In UHF systems reader antennas can be linear- or circular-polarized. When using a linear polarized antenna the tag and reader must be in alignment to achieve the maximal reading distance
  - **Key points about antenna**
    - Transmit the reader's interrogation signal
    - Receive the return signal from the tag
    - Come in various sizes and shapes
    - Are connected to the reader via a cable (unless integrated)
    - Size depends on frequency
      - (a) As frequency increases, wavelength and antenna size decrease
      - (b) By increasing antenna size, you can increase its read range
    - They are designed for a specific gain (higher the gain the narrower the beam and vice versa).

### 3.3.6 RFID Reader / Interrogator



**Fig. 3.3.6 : Block diagram of generic RFID reader**

- **Reader** : A device used to communicate with RFID tags, it has one or more antennas that emit radio waves and receive a signal back from the tag. Tag readers are also sometimes called interrogators.
- **RFID Scanner** : An electronic device, such as an RFID tag reader, that sends and receives radio waves. When combined with a digital signal processor that turns the waves into data, the scanner is called a reader or interrogator.
- **Shielding** : The use of a Faraday cage, Mylar sheet or metal barrier to prevent radio frequency noise from interfering with tag readers or to prevent readers from interfering with other devices.
- **Reader Field** : The area a tag reader can cover. Tags outside the field do not receive radio waves emitted by the tag reader and cannot be read.
- **Reader Module** : Reader electronics (digital signal processor and circuit board) can be placed in a dedicated device or an RFID label printer, for example.
- **Reader Talks First** : A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as “walking” a binary tree, “tree walking”, or “singulation”.
- **Read** : The process of retrieving RFID tag data by broadcasting radio waves at the tag and converting the waves the tag returns to the tag reader into data.
- **Read range** : The distance from which tag readers can accurately and reliably communicate with RFID tags. Active tags have longer read ranges than passive tags because they have their own power source for signal transmission. In passive tags the read range is controlled by frequency, reader output power, antenna design, and the method used to power up the tag. Low-frequency tags use inductive coupling which requires the tag to be close to the reader.



- **Read rate** : A specification describing how many tags can be read within a given period or the number of times a single tag can be read within a given period. Alternatively, the maximum rate that data can be read from a tag expressed in bits or bytes per second.
- **Singulation** : A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as “walking” a binary tree, “tree walking”, or “reader talks first”.
- **Types of RFID Readers**
  1. **Fixed Reader** : An RFID interrogator mounted to a permanent or non-mobile structure enabling users to read RFID tag numbers attached to movable items.
  2. **Agile Reader** : An RFID reader that reads tags operating at different frequencies or using different methods of communication between RFID tag and reader.
  3. **Intelligent reader** : A reader that can filter data, execute commands and perform functions similar to a personal computer.
  4. **Mobile Reader** : An RFID interrogator that is easily transported, allowing employees to read RFID tags attached to items in a warehouse or other setting along the supply chain.
  5. **Dumb Reader** : A tag reader with limited computing power that converts radio waves from a tag into a binary number, passing it to a host computer with little or no filtering.
  6. **Smart Reader** : A reader that can filter data, execute commands and perform functions similar to a personal computer.
  7. **Bi-static RFID reader** : A bi-static RFID interrogator or reader uses a one antenna to transmit energy to the RFID tag and a different antenna to receive reflected energy back from the tag.
  8. **Monostatic RFID reader** : An RFID reader that uses the same antenna to transmit RF energy to and receive RF energy from an RFID tag.
- **Input/output Port** : Connections on an RFID reader for external devices. An output device could be a panel that opens when a tag is read. An input device could be a photoelectric eye to turn on the reader when an object breaks the beam.
- **Interoperability** : The ability for RFID tags and readers from different vendors to communicate. Interoperability testing assesses the ability different systems to exchange information and use the data that has been exchanged.
- **Interrogation zone** : Area in which a tag reader can provide enough energy to power up a passive tag and receive back information. Also known as the read field or reader field. RFID tags located outside the interrogation zone do not receive enough energy from the reader to produce a signal.



- **Low-Level Reader Protocol (LLRP) Standard** : A standard to foster RFID reader interoperability and create a foundation for technology providers to offer capabilities that meet industry-specific requirements.
- **Anti-Collision** : A general term used to cover methods of preventing radio waves from one device from interfering with radio waves from another. Anti-collision algorithms are also used to read more than one tag in the same reader's field.
- **Monostatic** : An RFID reader that uses the same antenna to transmit RF energy to and receive RF energy from an RFID tag.
- **Multiple access Schemes** : Techniques to increase the amount of data that can be wirelessly transmitted within the same frequency spectrum. RFID readers may use Time Division Multiple Access (TDMA) so that they read tags at different times to avoid interference.
- **Multiplexer** : An technique that allows a reader to have more than one antenna and reduces the number of readers needed to cover a given area while preventing the antennas from interfering with each other.
- **Null spot** : An area in the RFID tag reader field that does not receive radio waves. This is a common issue with UHF systems.
- **Phantom read** : When a reader reports the presence of a tag that doesn't exist. Also called a false read or phantom transaction.
- **Excite** : Tag readers "excite" a passive tag when the reader transmits RF energy to activate the tag and cause it to transmit data back to the reader.
- **Forward channel** : Energy path from the tag reader to the RFID tag.
- **False read** : When a tag reader reports the presence of an RFID tag that does not exist. Also called a phantom transaction or false read.
- **Authentication** : In RFID, identify verification or authentication is used in two ways. In non-contact smart cards or other payment systems the RFID reader must ensure the transponder is a valid device and is not being used with the intent to commit fraud.
- The checksum code added to a data block on an RFID chip that is checked before and after data transmission from tag to reader to evaluate whether data has been corrupted or lost.
- **Concentrator** : A device that communicates with several RFID readers for the purpose of gathering data, which it then filters and passes on the information to a host computer.
- **Data transfer rate** : Number of characters that can be transferred from RFID tag to reader over a specified time. Baud rate defines how quickly readers can read information on a RFID tag, and is different from read rate, which refers to how many tags can be read over a specified time.
- **Duty cycle** : Length of time a tag reader is set to emit energy. European Union regulations permit tag readers to be on no more than 10 percent of the time.



- **Effective Radiated Power (ERP)** : A measurement of the output of RFID tag reader antennas used in Europe, usually expressed in watts.
- In RFID systems encryption is used to protect stored information or to prevent the interception of communications between RFID tag and reader.
- **Error correcting protocol** : A set of rules used by tag readers to interpret data from the RFID tag correctly.
- **Electronic product code** : A serial number created by the Auto-ID Center that will complement barcodes. The EPC identifies the manufacturer, product category and individual item.
- **ISO Protocols for RFID readers** :
  - o ISO 10536 : International standard for proximity cards.
  - o ISO 14443 : International standards for proximity smart cards.
  - o ISO 15693 : International standard for vicinity smart cards.
  - o ISO 18000 : International standards for the air interface protocol used in RFID systems for tagging goods in a supply chain.
  - o ISO 7816 : International standards covering smart cards physical and electrical characteristics and communication protocols.
  - o ISO/IEC 24730 : Standard that defines two air interface protocols and a single Application Program Interface (API) for Real-time Locating Systems (RTLS) for asset management. It is intended to allow for compatibility and encourages interoperability of products for the growing RTLS market.
- **Key points about reader** :
  - o Readers perform air interface functions
    - (a) Read/write data from/to tags via an antenna
    - (b) Anti-collision, filtering
    - (c) Work with one tag at a time, but very quickly
  - o Perform reader management functions
  - o Have firmware that runs the reader
  - o Often include a basic user interface with user application for reader configuration
  - o Communicate over the network with host computers
  - o Usually support multiple protocols (EPC and ISO)
  - o Can run light controls, motion sensors, electric eyes, horns and other I/Os
  - o Come in various form factors :
    - (a) Primary form factors are fixed and handheld,
    - (b) Fixed can be regular or integrated (these have integrated antenna),
    - (c) Handheld can be fully equipped handheld computers with a display but also be sled readers that are just RFID base and the computing is provided by a docked smart phone with an app.



- Fixed readers may have multiple antenna ports, usually 1 - 4 but sometimes 8 or 16.
- Bi-static, Mono-static
- Battery, AC, or Ethernet powered (POE)
- Dumb, Smart
- Serial or Ethernet (wired, wireless) connection, sometimes Bluetooth (handheld)

### 3.3.7 RFID Middleware

- Manages hardware devices and communicates between readers and business applications.
- Transfers, formats, filters and distributes data between the reader and the system application.
- It's a set of many different distributed software elements: Event Management, Data Conversion, Database Management, Data Consolidation, Data Reporting, etc.
- Refers to all the software laying between the on-device software and the business applications.
- Does not manage compliance with standards and regulations which is already managed by the reader firmware.

### 3.3.8 Advantages of RFID

The advantages of radio frequency tags compared to barcodes are :

1. Possibility to update information contained in an RFID;
2. Greater capacity for storing information;
3. Higher data recording speed;
4. Increased security for data access;
5. Greater flexibility in tag positioning;
6. Higher lifetime especially in terms of scalability;
7. Better protection against environmental conditions.

### 3.3.9 Disadvantages of RFID

There is no doubt that this technology has many advantages as described in the preceding section. However, RF tags also have constraints, the main ones are :

1. Particularly fluctuating cost;
2. Disturbance due to the physical environment;
3. Perturbations induced by tags among them;
4. Sensitivity to interference of magnetic and electric waves;
5. Unprintable;
6. Regulation constraints related to the impact on health.

## 3.4 Applications of RFID System

---



### 3.4.1 RFID in Supply Chain Management and Logistics

- Supply chain management and logistics are considered as the most fertile field as far as the applications of RFID is concerned.
- RFID in the supply chain plays a major role in enhancing the visibility right from the point of manufacturing, via supply chain, and most significantly from the back room to the floor, and ultimately to the exit door.
- RFID has a major say when it comes to inventory management, warehouse management, and retail sector. Let's see in detail about them all.

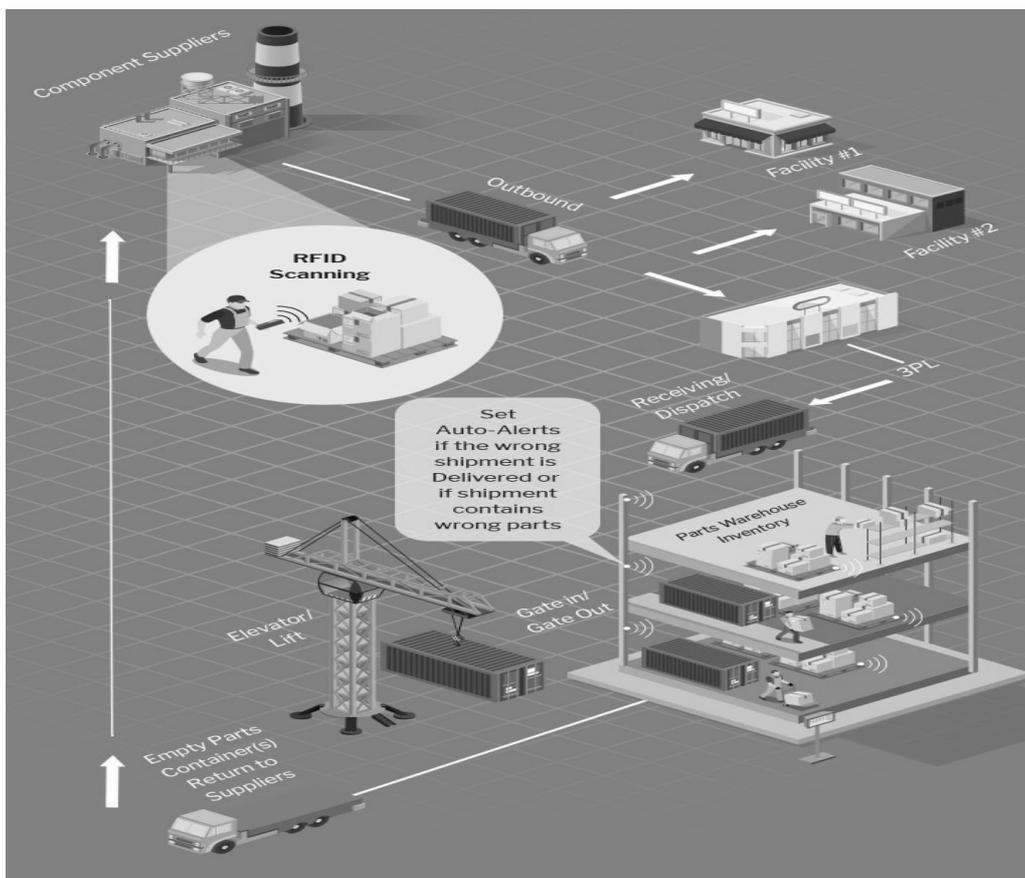


Fig. 3.4.1 : RFID in supply chain management

#### 1. Inventory management

- Inventory management is an important element of supply chain management. It includes various aspects like monitoring, administering, controlling, storing, and ultimately using the materials for the sale of a product.
- Inaccuracy in inventory management is inevitable and is prevalent in many industries.
- The inaccuracy is nothing but the mismatch between the inventory records and the actual amount of product available for the sale.



- RFID technology can provide numerous benefits to improve the inventory management system. RFID tags have the capability to read through an item.
- Moreover, the person can scan several items at a time. These properties of RFID help to speed up the inventory management process and reduces human errors thus rendering a highly accurate inventory records.

## **2. Warehouse management**

- Warehouses are simply storage area where you store different products received from the suppliers. These products are then distributed to the customers.
- Recently, RFID has emerged as a technology that supports warehouse management system for simpler supply chain and greater product intelligibility.
- With RFID technology you can automate important tasks which take place during receiving and shipping processes.
- RFID also increases efficiency of identification and validation activities along with reducing human errors.
- RFID ensures identification of products at an instant and greater control over items in the warehouse.
- Due to this the supply chains now have a greater information flow as compared to the material flow. This further reduces currency cost.
- Peer bits have developed a solution for warehouse management system using RFID technology. Click on the below video to see how it works.

## **3. Retail sector**

- RFID technology has already started to revolutionize the retail sector. Wal-Mart a behemoth in retail sector is experimenting with the passive RFID tags of passive types to meet high consumer demand.
- RFID increases the product visibility in the retail inventory that helps in better inventory control and customer experience.
- This is highly relevant in larger stores that have facility of customers searching for their chosen products online which the store has the current stock available for sale.
- Secondly, RFID provides enhanced product identification by storing distinctive identification number.
- And at last, it reduces the checkout times since RFID enables a shopper to scan entire content of a cart without even picking up a single item. Moreover, it helps in dynamic pricing, theft reduction, and employee tracking.

## **4. Benefits of RFID**

1. Adds flexibility and intelligence in the process to improve service levels.



2. Integrated automated receiving PCP in manufacturing enables you to continue without waiting for the receipt of the material.
3. It enables to control the expiry date, automatic filling of missing files, inventory and returns control, and expediting checkout.
4. Allows you to check shelves, boxes, and pallets on top without any eye contact.
5. Reduces the total cycle time order until the goods delivery.
6. Reduces the errors made in deliveries of customers' orders.
7. Allows you to read multiple tags and hence increases the reading speed instead of processing one bar code at a time.
8. Easy monitoring of all logistics operations along with increased security.
9. Increased speed and agility in locating materials.
10. Helps in avoiding tampering with recording of unique codes.
11. Makes it easy to manage products and materials with less manpower.

#### **5. Challenges in RFID implementation in supply chain management**

- RFID is a costly affair. RFID requires costly equipment whether it be a software or hardware. Moreover, talking about the tags be it active, passive, or semi-passive are a costly affair and has the capability to set the business backwards.
- The rates of RFID tags have lowered since 1970s, but still many companies are reluctant to adopt it due to its steep prices.
- Trouble with metals & liquids. RFID doesn't go well with metals and liquids as they both make it difficult to obtain proper reads on assets. In metals the radio waves bounces all over the place. Similarly, the liquid can absorb the signals from the RFID tags.
- Difficult to understand the technology. It's difficult to understand about the different tags and frequencies. Managers need to understand the technology well so that they can train their employees about its working.
- RFID collision course. Workers often come across reader and tag collisions. In reader collision, a worker faces the interferences from another reader in the field. Similarly, in tag collision, the workers face reading an abundant amount of tags at a time. It occurs when more than one tag reflects a signal that confuses the reader.

#### **3.4.2 RFID in Monitoring System**

- Perhaps the most important aspect of RFID related to service parts inventory management is the capability of monitoring the installed base and program usage within computer facilities or for capital equipment.
- Given the lack of information in these areas along with the high value of service parts, monitoring will almost certainly reduce the amount of service parts needed to achieve target service levels.



- Assuming that critical components contain RFID tags, either applied externally or integrated into the electronics, there are two basic ways of monitoring the installed base, intermittent or continuous.
- First, a technician could manually scan machines with an RFID reader to gain an accurate understanding of the installed base of components. This is essential information for projecting the number of probable failures for a span of time, thus improving the forecast.
- With a better forecast, the proper amount of inventory to meet a specific service level can be reserved.
- A second way of monitoring involves a continuous scan of the installed base using readers that are permanently fixed in the customer's facility.
- Besides confirmation of the installed base, sensors could be added that would monitor such variables as electric current draw to determine the time of usage for a component and confirm it is operational.
- Both methods, intermittent or continuous monitoring, allow the service parts supplier a means of linking directly to the customer with the longer-term prospect of gaining real-time information about critical components.
- The EPC global network and its ability to organize serial numbers to achieve unique identification will serve an important role in enabling this link so that specific information can be gathered for an individual component.

### 3.4.3 RFID in Maintenance and Repair Operations

- Beyond ability to gather information about the installed base and program usage, the EPCglobal Network and RFID technology also has potential to redefine repair operations in terms of productivity.
- Often customers return high value, non-functional components to a central facility for repair. After the repair work is completed, these components then re-enter the inventory of service parts for future use.
- Attaching a RFID tag to each component before shipping to a central repair facility would greatly improve the process of tracking.
- There are anecdotal accounts where considerable productivity can be achieved from knowing the precise location of high value components moving through the supply chain and within repair facilities.
- An unexplored area, the application of RFID to service parts inventory management represents a new opportunity to enhance productivity advances for both business and military applications.
- With a basic technology like RFID and the EPC global Network, the only limitation is the ingenuity of engineers and managers who must deal with day-to-day management of service parts inventory.



- Leading companies such as Boeing are beginning to implement RFID for service parts inventory management. Within ten years, the application of RFID in this area will become common practice.
- Since the memory size of RFID tags is continually increasing (in line with many other hardware devices) the ability to store information such as the maintenance history of a particular machine is now a realistic possibility.
- In this maintenance scenario, retrieval of the complete details of the asset (whether it be a machine, a spare part, a tool, a person or some other asset important to a company) is carried out via a database query web service.
- The query uses the tag's unique identifying number to retrieve details of the asset from a database server.

#### 3.4.4 RFID in Product Safety

- Chemical companies and industries that deal with high purity products such as pharmaceuticals and food are adopting process equipment tracking programs to minimize risk, reduce costs, and consolidate documents.
- Accurate records on equipment cleaning and maintenance are important parts of compliance and product safety, and automation can help to ensure the reliability and consistency of record keeping. RFID (radio frequency identification) tags are emerging as a technology to meet this need.
- If you toured five different processing facilities, there is a good chance you would find five different methods for tracking events that are critical to equipment degradation.
- Process equipment includes hose and hose assemblies, tubing, pumps, vessels, single-use/disposable components, bags, valves, filters, and other critical items.
- Precise, detailed records must be kept regarding the usage of these components to minimize contamination risks and assure product safety.
- Log books and hand-written charts requiring human entry are not uncommon, though they are prone to errors such as transposed numbers, incorrect dates, illegible handwriting, misread data, and misfiled documents.
- Other companies establish equipment replacement dates based upon a calendar method, opening themselves to operating inefficiencies and increased costs. These companies may be replacing process equipment before it is necessary.
- Timely access to a complete biographical history of any processing equipment in a production facility provides a comprehensive tool for equipment management and the required information for reordering.
- Such information can include the manufacture date, batch number, lot number, material specifications, material lot number, certificates of compliance, size specifications, and equipment description.



- What happens to a particular piece of equipment from the time it is installed to the time it needs replacement will have a direct impact on its life expectancy. These wear-related events include the date and number of cleaning cycles and the actual number of batches processed.
- By switching to a replacement method based upon actual usage, replacement decisions are based solely on the actual wear and condition of each individual part, thus providing a higher return on investment.
- The automation of process equipment tracking has been requested — and in some cases demanded — in order to provide concrete evidence of the standard operating procedures (SOPs) used to determine equipment replacement schedules. Benefits of such automated systems include the substantial risk reduction of contaminating a batch of product, equipment failure, and the costly repercussions associated with waste and production stoppages. This results in an increased degree of safety for the final product.
- Identification and tracking systems that ensure the dedication of equipment for specific applications, processes, and products are important.
- Maintaining records on process equipment's age and consistency of application provides assurances against substance contamination and cross-contamination of product lines.
- RFID solutions greatly help to simplify record keeping, improve accuracy, and most importantly increase product safety.

#### 3.4.5 RFID in Production or Manufacturing

For manufacturers, success hinges on the speed and accuracy of their manufacturing operations. UHF RFID provides instant and accurate tracking of information at every step inside the manufacturing plant, trimming wasted time and costs out of end-to-end manufacturing processes from receipt of raw goods to RFID-enabling supply, sequencing, assembly and shipping of final product. The net result is a leaner and more profitable manufacturing operation.

- End-to-end warehouse operations
- Quality assurance
- Line sequencing, raw material supply
- E-Kanban / replenishment
- Work-in-Process (WIP)/Just in time (JIT)

#### **Benefits**

1. Improve global inventory accuracy from raw to finished goods.
2. Improve product quality with increased automation of process and materials visibility.
3. Increase shipping and receiving accuracy.

#### 3.4.6 RFID in Retail Industry

Retailers need detailed inventory information to keep the right items on the shelves of the



store. But manual cycle counts are too costly to be performed frequently enough to provide current information. UHF RFIDs constant and accurate inventory information provides visibility into inventory levels, allowing retailers to make sure that customers find the products they want to purchase on the store shelves. And since the information is collected automatically, sales associates can spend more time with your customers instead of managing inventory.

- Inventory and cycle counting
- Receiving
- Replenishment
- Item locating
- Loss detection/prevention
- Demand forecasting

### **Benefits**

1. Achieve near 100% inventory accuracy
2. Maintain real time inventory information without any labor costs
3. Reduce out of stocks by as much as 80 percent & inventory cost by 59%
4. Minimize markdowns
5. Increase associate efficiency and associates are free to spend more time serving customers

#### 3.4.7 Access Control and Tracking and Tracing of Individuals

- RFID based People Movement and Monitoring System track the location and movement of people in organizations, events, factories, hospitals etc.
- Mainly used to find the exact location and time of a particular person not only for security purposes but also for access control and location tracking.
- Can also be used as check-in/check-out system for employees where attendance can also be stored for employees.
- Complete movement tracking for employees and monitoring the time of the movement.
- Unauthorized movement of a particular employee can be tracked and alerted accordingly. Each user can be identified by an RFID tag and 24×7 monitoring is possible with location control.
- People movement and monitoring System is used for :
  - o Tracking exact location of people.
  - o Access control after identifying the personnel.
  - o Time and attendance.



- Report generation.
- Zone Monitoring.

#### 3.4.8 RFID Based Contactless Payment System

- Contactless payment systems represent cashless payments that do not require physical contact between the devices used in consumer payment and POS terminals by the merchant.
- Radio frequency identification (RFID) devices can be embedded in the most different forms, as the form of cards, key rings, built into a watch, mobile phones.
- This type of payment supports the three largest payment system cards: Visa (Visa Contactless), MasterCard (MasterCard PayPass) and American Express (ExpressPay). All these products are compliant with international ISO 14443 standard, which provides a unique system for payment globally.
- Implementation of contactless payment systems are based on same infrastructure that exists for the payment cards with magnetic strips and does not require additional investments by the firm and financial institutions, other than upgrading the existing POS terminals.
- Technological solutions used for the implementation are solutions based on ISO 14443 standard, Sony FeliCa technology, RFID tokens and NFC (Near Field Communication) systems.
- The contactless smart chip includes a smart card secure microcontroller and internal memory and has unique attributes RFID tags lack i.e., the ability to securely manage, store and provide access to data on the card, perform complex functions (for example, encryption and mutual authentication) and interact intelligently via RF with a contactless reader.
- Applications using contactless smart cards support many security features that ensure the integrity, confidentiality and privacy of information stored or transmitted, including the following :
  - Mutual authentication.
  - Strong contactless device security.
  - Protection against transaction replay.
  - Support for biometric authentication.
  - Strong support for information privacy.

#### 3.4.9 RFID in Household Objects

- When you lose a small, important item, then the last thing you want to do is frantically search for it while you're about to head out the door. That's when RFID tags can come in handy.
- Paired with an app, RFID tags can be extremely useful. Already, there are several different companies that have employed RFID tags to create item trackers.
- For example, TrackR allows you to attach a coin-sized RFID tag to items before using an app to track it. There are also other, newly-developed apps. Find MyStuff, in particular, tells you exactly where your lost item is through the combination of a RFID chip and a ZigBee radio.



- UHF RFID tags could help address some of the challenges that robots face in unstructured environments and hasten the deployment of useful robots in homes and other environments.
- Behavior-based RFID search methods can be combined to find and navigate to UHF RFID tagged household objects in a realistic home environment without relying on training data or explicit Sensor models.

#### 3.4.10 RFID in Loyalty Program

- Since RFID technology has come out, it has been a boon to many different industries, most notably in the warehouse and shipping business where it can be utilized to keep track of inventory and ensure speed and accuracy.
- However, while the technology is excellent for back of house systems, it turns out that it can be beneficial on the customer side of things as well.
- In fact, if you are smart about implementing a strategic RFID system then you can even increase your customer service experience and generate more loyalty.
- While not every business can use RFID, some retailers are finding that it can be an easy way to set up customers with accounts that allow them to buy products without having to swipe a card or stand in line.
- Overall, convenience is always a big selling point, so customers will usually gravitate toward businesses that offer faster and simpler solutions to the shopping experience.
- If a person can visit a store and buy items without having to wait for a cashier, they will be much more likely to return instead of visiting a competitor that doesn't have such a system in place.
- Since convenience is the ultimate selling point, it shouldn't be too hard to get customers to sign up for reward services with your business that utilize RFID technology.
- When setting up the account, you can get information such as email address, physical address, age, gender, and so on. This data can be immensely helpful down the road as it will allow you to customize and tailor your marketing to reach specific demographics rather than a generic ad or coupon.
- Additionally, you can track the frequency of your customer's visits and see what kind of items or services they purchase the most, which will enable you to further tailor their experience over time.
- The more that you can make your clients feel appreciated, the more likely they are to return. In that regard, RFID is invaluable because it allows you to collect this data automatically without needing to pester individuals with surveys or questionnaires.

### 3.5 Issues with RFID System Hardware

---

#### 3.5.1 Technical Problems with RFID



## 1. Problems with RFID Standards

- In different ways by different manufacturers; global standards are still being worked on RFID has been implemented.
- Some RFID devices are never meant to leave their network (as in the case of RFID tags used for inventory control within a company), this can cause problems for companies.
- Consumers may also have problems with RFID standards. For example, ExxonMobil's SpeedPass system is a proprietary RFID system; if another company wanted to use the convenient SpeedPass (say, at the drive-in window of your favorite fast food restaurant) they would have to pay to access it - an unlikely scenario.
- On the other hand, if every company had their own "SpeedPass" system, a consumer would need to carry many different devices with them.

## 2. RFID systems can be easily disrupted

- Since RFID systems make use of the electromagnetic spectrum (like WiFi networks or cellphones), they are relatively easy to jam using energy at the right frequency.
- Although this would only be an inconvenience for consumers in stores (longer waits at the checkout), it could be disastrous in other environments where RFID is increasingly used, like hospitals or in the military in the field.
- Also, active RFID tags (those that use a battery to increase the range of the system) can be repeatedly interrogated to wear the battery down, disrupting the system.

## 3. RFID reader collision

- Reader collision occurs in RFID systems when the coverage area of one [RFID reader](#) overlaps with that of another reader. This causes two different problems:
  - **Signal interference** : The RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called Time Division Multiple Access - TDMA) can still result in the same tag being read twice.
  - **Multiple reads of the same tag** : The problem here is that the same tag is read one time by each of the overlapping readers. The only solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session.
- Reader collision occurs when the signals from two or more readers overlap.
- The tag is unable to respond to simultaneous queries.
- Systems must be carefully set up to avoid this problem; many systems use an anti-collision protocol (also called a singulation protocol). Anti-collision protocols enable the tags to take turns in transmitting to a reader.

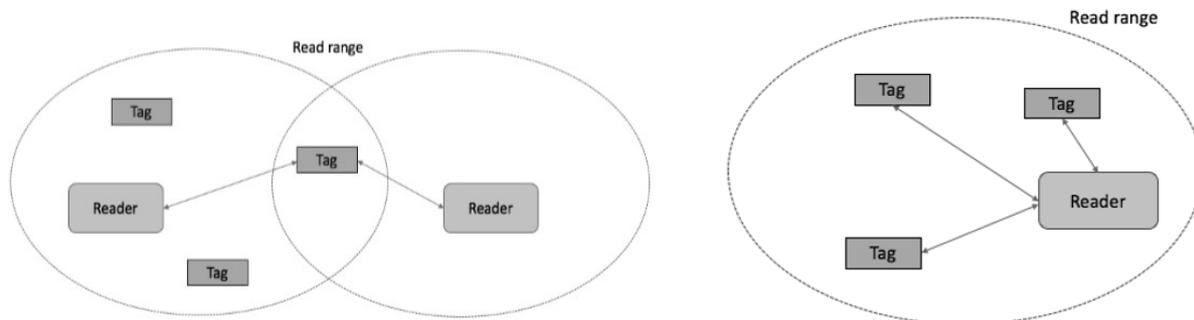


Figure 1. Reader collision.

Figure 2. Tag collision.

**Fig. 3.5.1 : Reader collision and tag collision**

#### 4. RFID tag collision

- Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time.
- Tag collision in RFID systems happens when multiple tags are energized by the [RFID tag reader](#) simultaneously, and reflect their respective signals back to the reader at the same time.
- This problem is often seen whenever a large volume of tags must be read together in the same RF field. The reader is unable to differentiate these signals; tag collision confuses the reader.

#### 5. Security, privacy and ethics problems with RFID

The following problems with RFID tags and readers have been reported :

- **The contents of an RFID tag can be read after the item leaves the supply chain.**

An RFID tag cannot tell the difference between one reader and another. RFID scanners are very portable; RFID tags can be read from a distance, from a few inches to a few yards. This allows anyone to see the contents of your purse or pocket as you walk down the street. Some tags can be turned off when the item has left the supply chain.

- **RFID tags are difficult to remove.**

RFID tags are difficult to for consumers to remove; some are very small (less than a half-millimeter square, and as thin as a sheet of paper) - others may be hidden or embedded inside a product where consumers cannot see them. New technologies allow RFID tags to be "printed" right on a product and may not be removable at all.

- **RFID tags can be read without your knowledge.**

Since the tags can be read without being swiped or obviously scanned (as is the case with magnetic strips or barcodes), anyone with an RFID tag reader can read the tags embedded in your clothes and other consumer products without your knowledge. For example, you could be scanned before you enter the store, just to see what you are carrying. You might then be approached by a clerk who knows what you have in your backpack or purse, and can suggest accessories or other items.

- **RFID tags can be read a greater distance with a high-gain antenna.**

For various reasons, RFID reader/tag systems are designed so that distance between the tag and the reader is kept to a minimum (see the material on tag collision above). However, a high-



gain antenna can be used to read the tags from much further away, leading to privacy problems.

- **RFID tags with unique serial numbers could be linked to an individual credit card number.**

At present, the Universal Product Code (UPC) implemented with barcodes allows each product sold in a store to have a unique number that identifies that product. Work is proceeding on a global system of product identification that would allow each individual item to have its own number. When the item is scanned for purchase and is paid for, the RFID tag number for a particular item can be associated with a credit card number.

### 3.6 Multi-Access Methods

- Each anti-collision protocol uses certain multi-access methods for identification in order to physically separate the transmitters' signals.
- Accordingly, they can be categorized into four different types: Space Division Multiple Access (SDMA), Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA)

Fig. 3.6.1 shows various multiple access and anti-collision procedures.

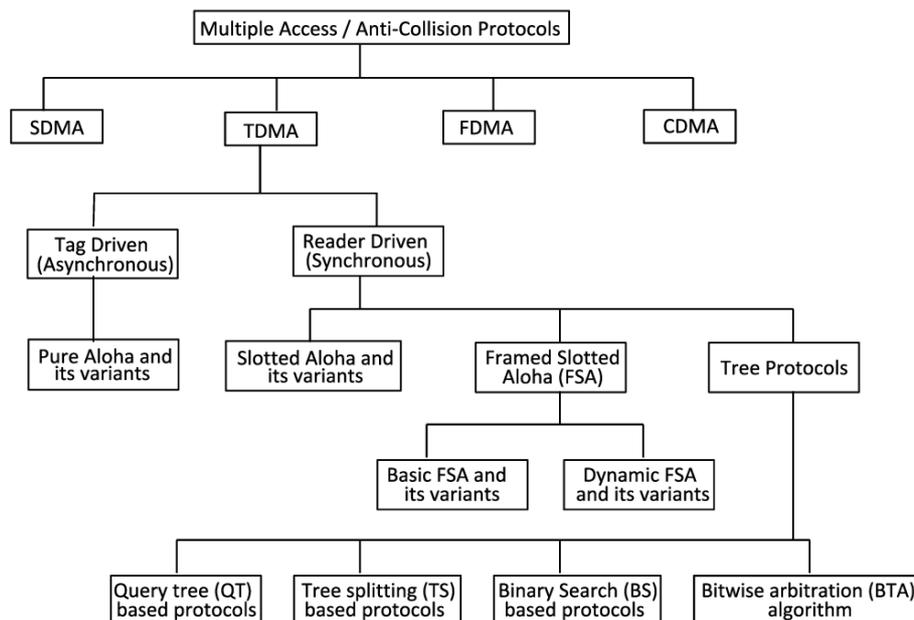


Fig. 3.6.1 : Multiple access / anti-collision protocols

#### 3.6.1 Space Division Multiple Access (SDMA)

- The term space division multiple access relates to dividing of the channel capacity into separate areas. Protocols based on this method can point the beam at different areas in order to identify tags.
- The channel is spatially separated using complex directional antennas. Another means of achieving this is through the use of multiple readers.



- As a result, the channel capacity of adjoining readers is enhanced. A huge number of tags can be read simultaneously as a result of the spatial distribution over the entire layout.
- This method is quite expensive and requires complex antenna design. The use of this type of method is restricted to a few specialized applications. This technique is shown in Fig. 3.6.2.

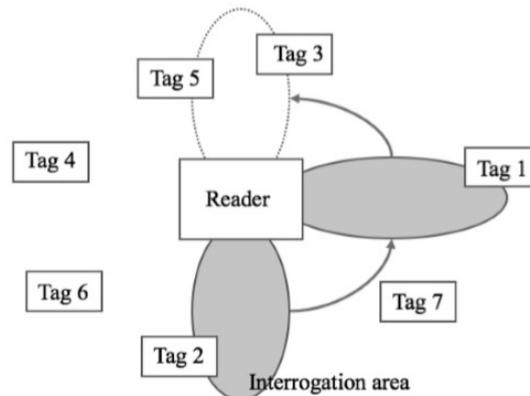


Fig. 3.6.2 : Space Division Multiple Access (SDMA) procedure

### 3.6.2 Frequency Division Multiple Access (FDMA)

- Tags transmitting in one of several different frequency channels requiring a complex receiver at the reader.
- Consequently, different frequency ranges can be used for communication from and to the tags: from the reader to the tags, 135 kHz, and from the tags to the reader, in the 433–435 MHz range.
- However, this technique is expensive and is only intended for certain specific applications. Fig. 3.6.3 shows FDMA procedure.

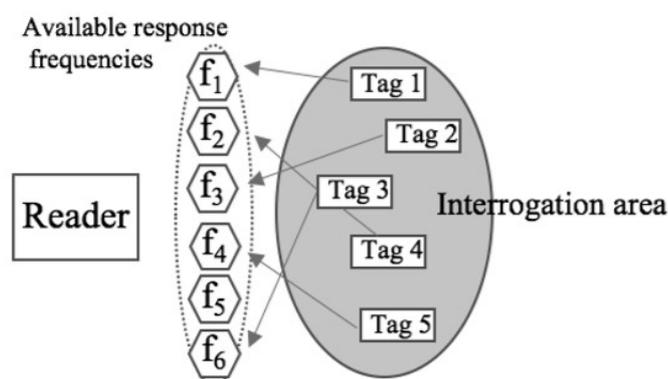


Fig. 3.6.3 : Frequency Division Multiple Access (FDMA) procedure

### 3.6.3 Code Division Multiple Access (CDMA)

- Requires tags to multiply their ID by a pseudo-random sequence (PN) before transmission.
- CDMA is quite good in many ways, such as the security of the communications between the RFID tags and the reader, and multiple tag identification.



- It adds great complexity and is expensive for RFID tags. Furthermore, this method consumes a great deal of power and can be classified as a group with elevated demands. Fig. 3.6.4 shows this procedure.

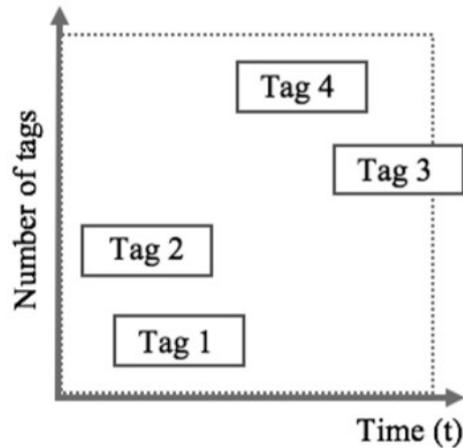


Fig. 3.6.4 : Code Division Multiple Access (CDMA) procedure

### 3.6.4 Time Division Multiple Access (TDMA)

- TDMA : Given that it is less expensive; this is the most widely used method. This method involves the largest group of anti-collision algorithms.
- The transmission channel is divided between the participants and ensures that the reader can identify a tag at different times in order to avoid interfering with another one.
- The space distributing characteristic of tags is not considered. The number of tags in the interrogation zone is reduced after every successful response.
- Another option involves the ability to mute all tags except for the transmitting tag. After that, the tags are activated one by one. TDMA is shown in Fig. 3.6.5.

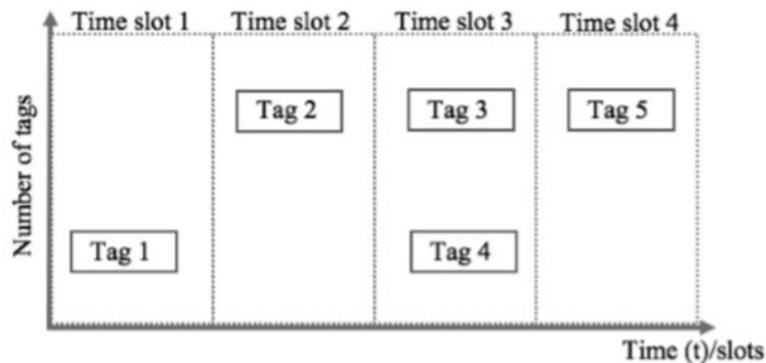


Fig. 3.6.5 : Time Division Multiple Access (TDMA) procedure

## 3.7 Protocols in RFID

- The operation of RFID systems often involves a situation in which numerous transponders are present in the interrogation zone of a single reader at the same time. In such a system -



consisting of a 'control station', the reader, and a number of 'participants', the transponders – we can differentiate between two main forms of communication.

- The first is used to transmit data from a reader to the transponders. The transmitted data stream is received by all transponders simultaneously.
- This is comparable with the simultaneous reception by hundreds of radio receivers of a news programme transmitted by a radio station. This type of communication is therefore known as broadcast.
- The second form of communication involves the transmission of data from many individual transponders in the reader's interrogation zone to the reader. This form of communication is called multi-access.
- Every communication channel has a defined channel capacity, which is determined by the maximum data rate of this communication channel and the time span of its availability.
- The available channel capacity must be divided between the individual participants (transponders) such that data can be transferred from several transponders to a single reader without mutual interference (collision).
- Tag collision in RFID systems happens when multiple tags are energized by the RFID tag reader simultaneously, and reflect their respective signals back to the reader at the same time. This problem is often seen whenever a large volume of tags must be read together in the same RF field. The reader is unable to differentiate these signals; tag collision confuses the reader.
- Different systems have been invented to isolate individual tags; the system used may vary by vendor. For example, when the reader recognizes that tag collision has taken place, it sends a special signal (a "gap pulse"). Upon receiving this signal, each tag consults a random number counter to determine the interval to wait before sending its data. Since each tag gets a unique number interval, the tags send their data at different times.
- In the context of RFID, anti-collision refers to different ways to keep radio waves from one device from interfering with radio waves from another device. RFID readers may make use of anti-collision algorithms to enable a single reader to read more than one tag in the reader's field.
- Reader collision occurs in RFID systems when the coverage area of one RFID reader overlaps with that of another reader. This causes problem of signal interference and multiple reads of the same tag.
- In an RFID environment, anti-collision protocols typically use the TDMA method. Protocols that use this method first select an individual tag from a large group using a specific algorithm and then the communication takes place between the selected tag and the reader.
- Significant increases in number of collisions in the identification process decreases the throughput and increases the number of transmitted bits.
- These protocols can be divided into three categories: Aloha-based protocols, tree-based protocols and hybrid protocols (which use a combination of the first two methods).



---

## 3.8 ALOHA Protocol

---

- **ALOHA** : ALOHA is a system for co-ordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.
- A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.
- Aloha means "Hello". Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.
- Aloha-based protocols use a random-access strategy in order to successfully identify the number of tags in an interrogation area.
- They belong to the group of probabilistic protocols because the tags transmit their own ID in randomly selected slots in a frame in order to reduce the possibility of a collision.
- However, there is no guarantee that all of the tags will be identified in the interrogation process. These protocols suffer from the well-known tag starvation problem, in the sense that a tag may not be correctly read during a reading cycle due to an excessive number of collisions with that same tag.
- Every frame consists of a certain number of slots, and the tags can only respond once per frame.
- In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.
- The ALOHA algorithm is a collision resolution algorithm based on Time Division Multiple Access (TDMA). There are three flavors of the original ALOHA algorithm: (Pure) ALOHA, Slotted ALOHA and Frame Slotted ALOHA.

### 3.8.1 Pure ALOHA Protocol for RFID

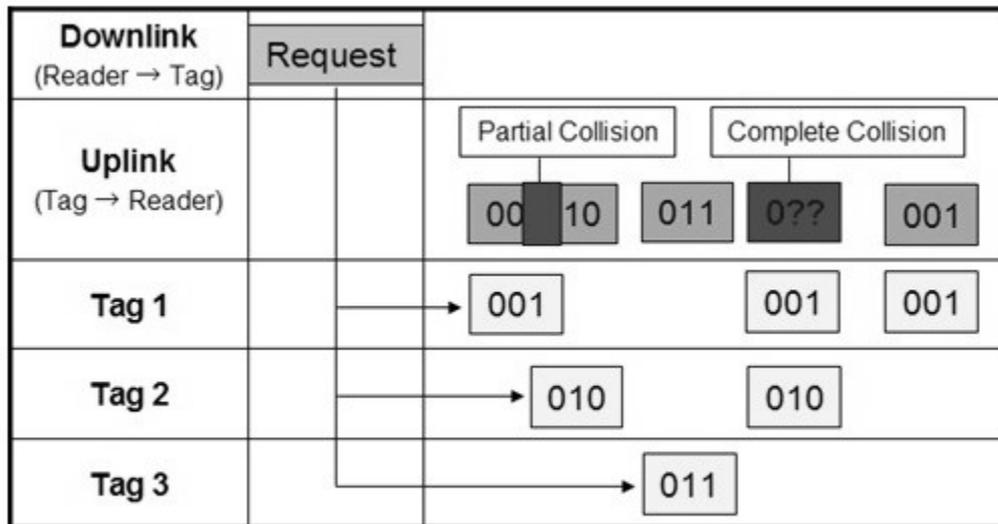


Fig. 3.8.1 : Pure ALOHA

- In Fig. 3.8.1, X and Y axis represents the read cycle and tags respectively. The read cycle is the time interval between neighboring two REQUEST commands and it can be repeated until all tags in the interrogation range are identified.
- A tag itself decides the data transmission time randomly as soon as it is activated.
- The transmission time is not synchronized with both the reader and the other tags at all.
- When the electricity is charged by the reader's electromagnetic wave tags transmit data after receiving the REQUEST command from the reader.
- If multiple tags transmit data imminently (whether earlier or later) then a complete or partial collision occurs.
- Retransmitting after random delay is the solution for a collision. During the read cycle the reader receives the data and identifies tags sent data without collision.
- When a read cycle is done then the reader broadcasts the SELECT command with the tag's unique identifier received from the tag.
- Once tags are selected the tags stop responding for the request command i.e. the selected tags keep silence until whether they receive other commands e.g. authenticate, read and write or the tag's power is off by being located out of the reader's power range.
- When the tag is reentered into the reader's interrogation range it restart transmitting its data to the reader. The advantage of this algorithm is simplicity.

### Protocol Flowchart for ALOHA :

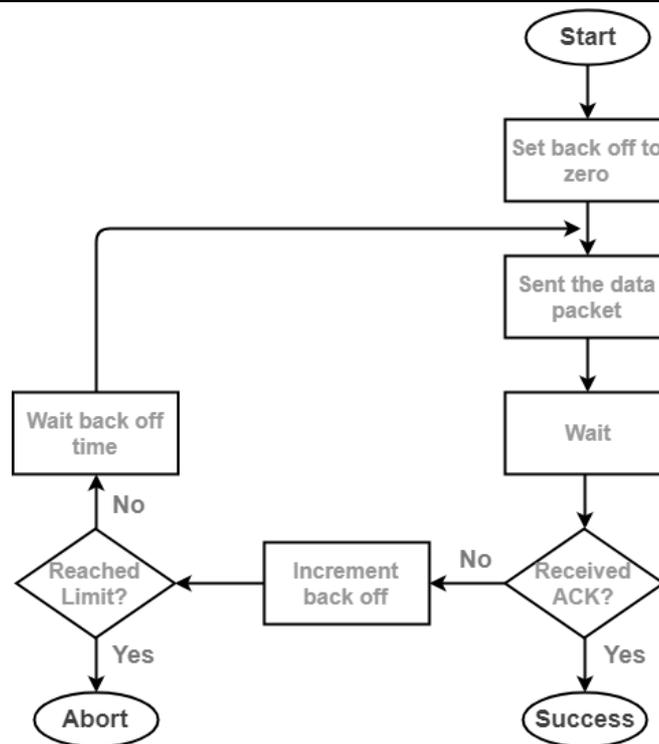


Fig. 3.8.2 : Flowchart of pure ALOHA

### Explanation :

Then, following 2 cases are possible-

#### Case-01

- Transmitting tag receives an acknowledgement from the receiving reader.
- In this case, transmitting tag assumes that the transmission is successful.

#### Case-02

- Transmitting tag does not receive any acknowledgement within specified time from the receiving reader.
- In this case, transmitting tag assumes that the transmission is unsuccessful.

Then,

- Transmitting tag uses a Back Off Strategy and waits for some random amount of time.
- After back off time, it transmits the data packet again.
- It keeps trying until the back off limit is reached after which it aborts the transmission.

### Efficiency

$$\text{Efficiency of Pure Aloha } (\eta) = G \times e^{-2G}$$

where  $G$  = Number of tags willing to transmit data

### Maximum Efficiency



For maximum efficiency,

- We put  $d\eta / dG = 0$
- Maximum value of  $\eta$  occurs at  $G = 1/2$
- Substituting  $G = 1/2$  in the above expression, we get
- Maximum efficiency of Pure Aloha =  $1/2 \times e^{-2 \times 1/2}$   
 $= 1 / 2e$   
 $= 0.184$   
 $= 18.4\%$

Thus,

Maximum Efficiency of Pure Aloha ( $\eta$ ) = 18.4%

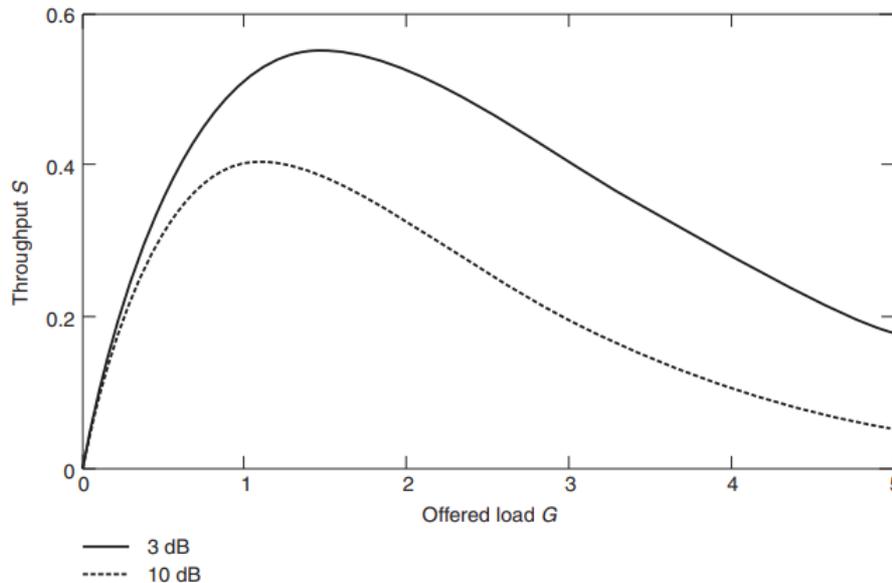
- The maximum efficiency of Pure Aloha is very less due to large number of collisions.

### 3.8.2 Slotted ALOHA Procedure

- In this, the communication time between the tags and the reader is slotted. Conventionally, the time from the point that the reader sends out a command to the point that the tags finish replying their information is called a time slot (slot for short).
- The time taken by the reader to identify a group of tags is conventionally called the reading time, and is measured in slots.
- One possibility for optimizing the relatively low throughput of the ALOHA procedure is the slotted ALOHA (S-ALOHA) procedure. In this procedure, transponders may only begin to transmit data packets at defined, synchronous points in time (slots).
- The synchronization of all transponders necessary for this must be controlled by the reader. This is therefore a stochastic, interrogator-driven TDMA anti-collision procedure.
- The period in which a collision can occur (the collision interval) in this procedure is only half as great as is the case for the simple ALOHA procedure.
- Assuming that the data packets are the same size (and thus have the same transmission duration  $\tau$ ) a collision will occur in the simple ALOHA procedure if two transponders want to transmit a data packet to the reader within a time interval  $T \leq 2\tau$ .
- Since, in the S-ALOHA procedure, the data packets may only ever begin at synchronous time points, the collision interval is reduced to  $T = \tau$ . This yields the following relationship for the throughput  $S$  of the S-ALOHA procedure:  
$$S = G \cdot e(-G)$$
- In the S-ALOHA procedure there is a maximum throughput  $S$  of 36.8% for an offered load  $G = 1$ . However, it is not necessarily the case that there will be a data collision if several data packets are sent at the same time: if one transponder is closer to the reader than the others, that transponder may be able to override the data packets from other transponders as a result of the greater signal strength at the reader.

- This is known as the capture effect. The capture effect has a very beneficial effect upon throughput behavior as shown in Fig. 3.8.3.
- Decisive for this is the threshold  $b$ , which indicates the amount by which a data packet must be stronger than others for it to be detected by the receiver without errors.

$$S = G \cdot$$



**Fig. 3.8.3 : Throughput behavior taking into account the capture effect with thresholds of 3 and 10 dB**

- The practical application of a slotted ALOHA anti-collision procedure will now be considered in more detail on the basis of an example. The transponder used must also have a unique serial number (i.e. one that has been allocated only once). In this example we use an 8-bit serial number; this means that a maximum of 256 transponders can be put into circulation if the uniqueness of serial numbers is to be guaranteed.

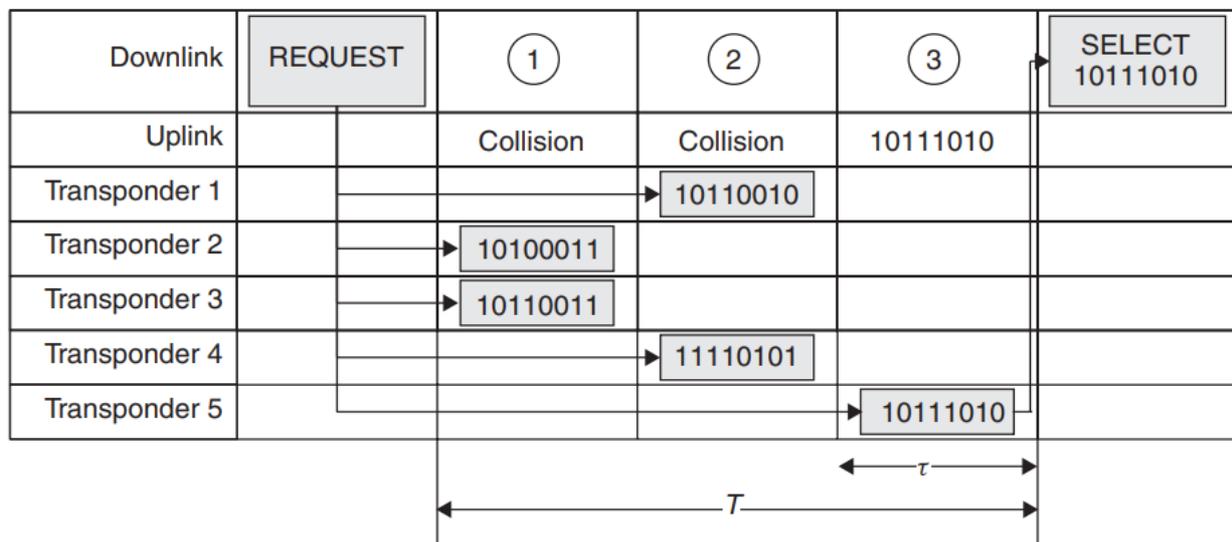
**Table 3.8.1 : Command set for anti-collision**

Command	Description
<b>REQUEST</b>	This command synchronises all transponders in the reader's interrogation zone and prompts the transponders to transmit their serial numbers to the reader in one of the time slots that follow. In our example there are always three time slots available



<b>SELECT(SNR)</b>	Sends a (previously determined) serial number (SNR) to the transponder as a parameter. The transponder with this serial number is thereby cleared to perform read and write commands (selected). Transponders with a different serial number continue to react only to a REQUEST command
<b>READ_DATA</b>	The selected transponder sends stored data to the reader. (In a real system there are also commands for writing, authentication, etc.)

- We define a set of commands in order to synchronize and control the transponders. A reader in wait mode transmits a REQUEST command at cyclical intervals. We now bring five transponders into the interrogation zone of a reader at the same time as shown in Fig. 3.8.4.



**Fig. 3.8.4 : Transponder system with slotted ALOHA anti-collision procedure**

- As soon as the transponders have recognized the REQUEST command, each transponder selects one of the three available slots by means of a random-check generator, in order to send its own serial number to the reader.
- As a result of the random selection of slots in our example there are collisions between the transponders in slots 1 and 2. Only in slot 3 can the serial number of transponder 5 be transmitted without errors.
- If a serial number is read without errors, then the detected transponder can be selected by the transmission of a SELECT command and then read or written without further collisions with other transponders.
- If no serial number were detected at the first attempt the REQUEST command is simply repeated cyclically. When the previously selected transponder has been processed, further transponders in the interrogation zone of the reader can be sought by means of a new REQUEST command.



### 3.8.3 Frame Slotted Aloha (FSA) Applied to RFID

The FSA protocol for RFID works as follows :

- Each tag that needs to be read should have a unique identification number.
- The RFID reader in the wait mode will send a Request command, and the tags in the reader range will recognize the Request command and respond to the reader by randomly selecting a slot in a frame to send the tag identification number to the reader.
- Collision occurs when more than one tag responds to the same slot. Collided tags need to be read again. If none of the tags responds, then the Request command will be repeated at cyclical intervals.
- If the reader identifies the tag identification number without errors (no collisions), then that detected tag can be selected subsequently using the Select command to perform the read/write operation.
- The throughput of pure Aloha is given by  $S = Ge^{-2G}$ , where  $S$  indicates the throughput and  $G$  indicates the offered traffic load. Maximum throughput is equal to  $1/2e$  where  $G = 0.5$ .
- Throughput of the FSA protocol is increased by having the tags begin transmitting data at predefined synchronous time slots. The collision interval of the FSA protocol is half that of the pure Aloha protocol.
- Therefore, the throughput of the FSA protocol is defined as  $S = G \cdot e^{-G}$  where  $S$  is throughput, and  $G$  is the offered load. The maximum throughput of the FSA protocol occurs when the offered load  $G$  is equal to 1; when  $G=1$ , then  $S = 1/e$ .
- The main inconvenience of FSA is slot wastage when the number of tags is small and the size of the frame is significantly larger.

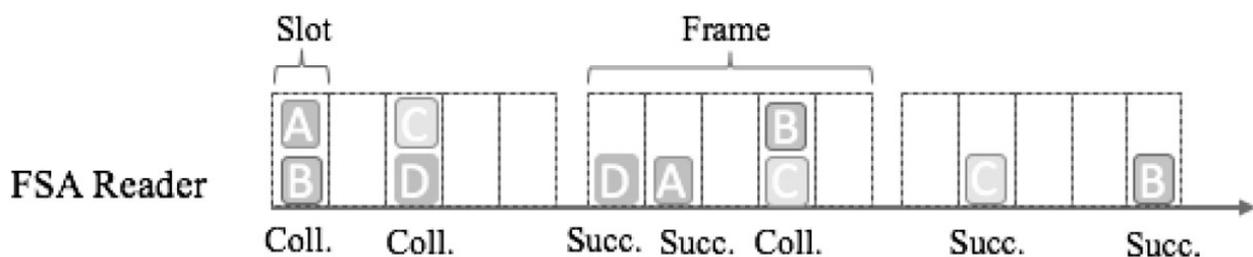


Fig. 3.8.5 : Example of FSA

### 3.8.4 A Comparison of Aloha Protocols

Table 3.8.2



Protocol Name	Pure ALOHA	Slotted ALOHA	Frame Slotted ALOHA
Protocol feature	Tags transmit after random time to the reader. In the case of a collision tags will retransmit after a random delay.	Tags transmit their ID in synchronous time slots. In case of a collision, tags retransmit after a random delay.	Each tag responds only once per frame.
Disadvantages	In a dense tag environment the number of collision increases significantly.	In a dense tag environment, the number of collision increases significantly. The reader requires synchronization with tags.	It uses a fixed frame size and does not change the size during the identification process.
RTF/TTF	TTF	RTF	RTF
Efficiency	18.4%	36.8%	36.8%
System cost	Very low	Low	Expensive
Complexity	Very simple	Simple	Medium
Tag Cost	Least	Medium	Most
Tag requirement	Timer	Random number generator, Timer, and Synchronization circuit	Random number generator, and synchronization circuit. Some tags in DFSA based variants also need to generate short pseudo IDs for identification or tag estimation.

### 3.9 Tree-based RFID Protocols

- One of the main features of tree-based protocols is that they are deterministic, since ideally, they are designed to identify the whole set of tags in the interrogation area.



- These protocols have simple design tags and work very well with a uniform set of tags.
- Tree-based protocols usually work with a muting capability since they need the identified tags to remain quiet after their identification.
- These protocols usually work using queries, which are broadcast commands transmitted by a reader to require the tags to respond. If a tag's ID does not match the query, the reader command is rejected.
- In tree-based RFID protocols, many protocols use binary tree algorithm. In this protocol, if a collision occurs in a timeslot, the colliding tags are randomly separated into two subgroups by independently selecting 0 or 1, until all tags are identified.
- The tags that select 0 transmit their IDs to an interrogator right away. If a collision occurs again, the collided tags are split again by selecting 0 or 1.
- The tags that select 1 wait until all the tags that select 0 are successfully identified by the interrogator. And if all the tags that select 0 are resolved, the tags that select 1 send their IDs to the interrogator. This procedure is repeated until there is no further collision.
- An example presented in Fig. 3.9.1 illustrates the process of the anti-collision scheme adopting the binary tree protocol. In the first timeslot, all tags select 0 or 1 randomly due to the collision. And tag 1 and 3 select 0. Both tags send their IDs at the next timeslot and are collided again. Tag 1 and 3 randomly select 1, no one selects 0, then at the following timeslot, it is empty. At the fourth timeslot, it is collided again.

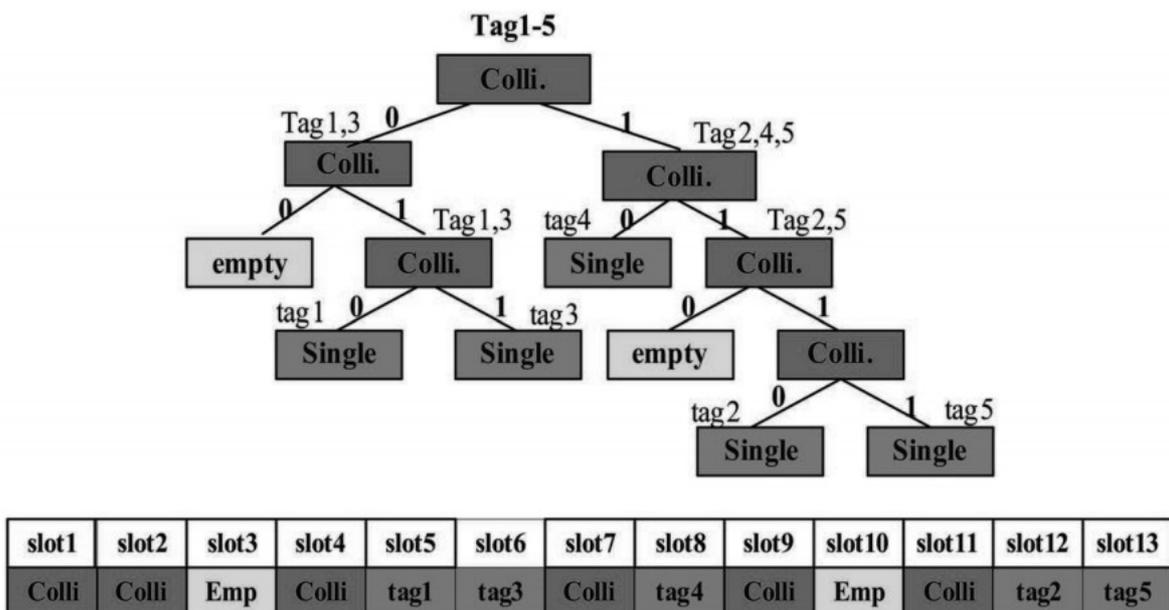


Fig. 3.9.1 : An example of binary tree algorithm

- Tag 1 transmits its ID at the fifth timeslot successfully by selecting 0, and the interrogator can then read the tag 3 because of no collision at the next timeslot.



- After the collision resolution of tag 1 and 3, tag 2, 4 and 5 are collided at the seventh timeslot. Next, tag 4 selects 0 and tag 2 and 5 select 1. Tag 4 sends its ID at the eighth timeslot. Thus tag 2 and 5 send at the twelfth and thirteenth timeslot, respectively.
- Due to the no further collision, an interrogator finishes an identification process. Table. 3.9.1 shows the procedure of query tree searching algorithm.

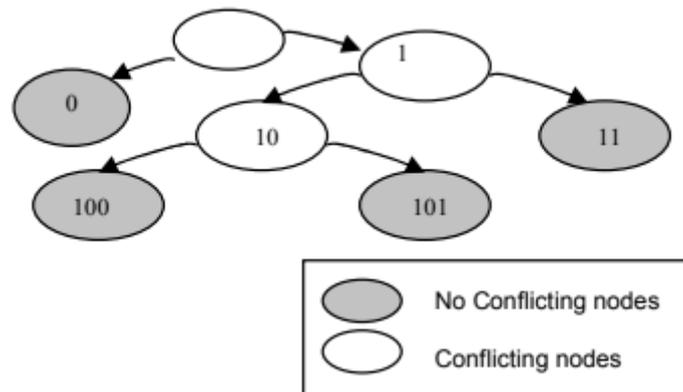
**Table 3.9.1 : Sequences of the query tree searching scheme**

		Interrogator						
		t1	t2	t3	t4	t5	t6	t7
Broadcast		0	00	000	001	01	1	
Tag1	0000							
Tag2	0010							
Tag3	0101							
Tag4	1100							
Interrogator	receive	xxxx	0xxx	00xx	0000	0010	0101	1100

- At  $t_0$ , the interrogator starts the anti-collision sequences by sending broadcast frame. Then at  $t_1$ , the interrogator sends '0' to receive a tag's UID of the first bit equal to '0'. At stage  $t_2$ , the interrogator sends '00' which is an accumulated UID stream that it is searching.
- By sending this accumulated UID stream, the tags are free for counting the stage information. Moreover, the only operations at tags are comparator or exclusive-OR operation. At stage  $t_3$ , the interrogator receives '00XX' where 'X' means a collision. It sends '000' firstly, and then receives the first complete tag information '0000'.
- Again the reader sends '001' which results an identification if UID '0010'. This algorithm takes 8 stages to get the whole 4 UID stream. The de-activation frame transmission is omitted for the simplicity.
- When the number of tag is small, tree-based protocols exhibit a reasonable performance. If the number of tags is large, at the early stage, they may experience poor performance because they might waste timeslots due to many collision slots until all tags are identified.

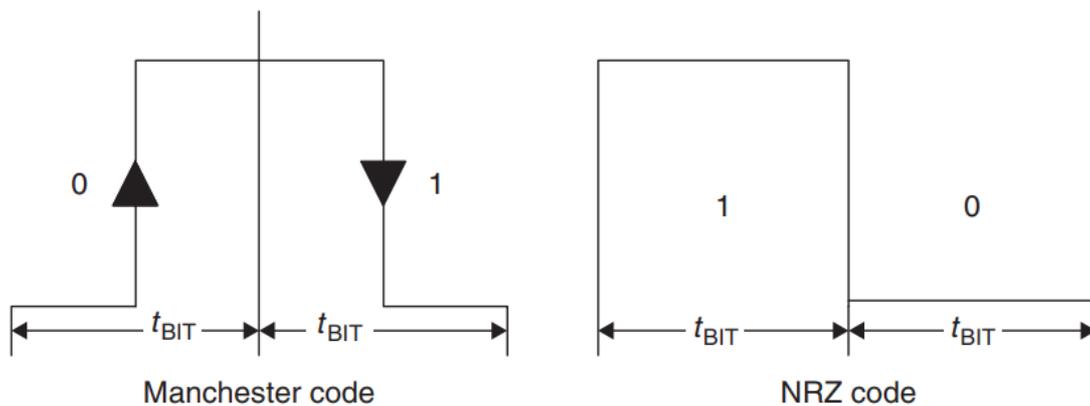
### 3.9.1 Binary Search Algorithm

- The fundamental idea of Binary Search algorithm is to divide the tabs into 2 subsets : 0 and 1.
- Firstly, enquiring the subset 0... If It can identify tab accurately if there is no conflict.
- The subset 0 will be divided into two lower levels of subsets : 00 and 01 if there is conflict, and so on. Until it identifies all the tabs of the subset 0. Then, enquiring the subset 1 according these steps in Fig. 3.9.2.



**Fig. 3.9.2 : Binary search algorithm model**

- Reader finally found the binary tree by repeated siftings. Binary algorithm is also known as Binary Tree Algorithm and Binary Tree Search Algorithm.
- The implementation of a binary search algorithm requires that the precise bit position of a data collision is recognized in the reader. In addition, a suitable bit coding is required, so we will first compare the collision behavior of NRZ (non-return-to-zero) and Manchester coding as shown in Fig. 3.9.3.
- The selected system is an inductively coupled transponder system with load modulation by an ASK modulated subcarrier. A 1 level in the baseband coding switches the subcarrier on, and a 0 level switches it off.

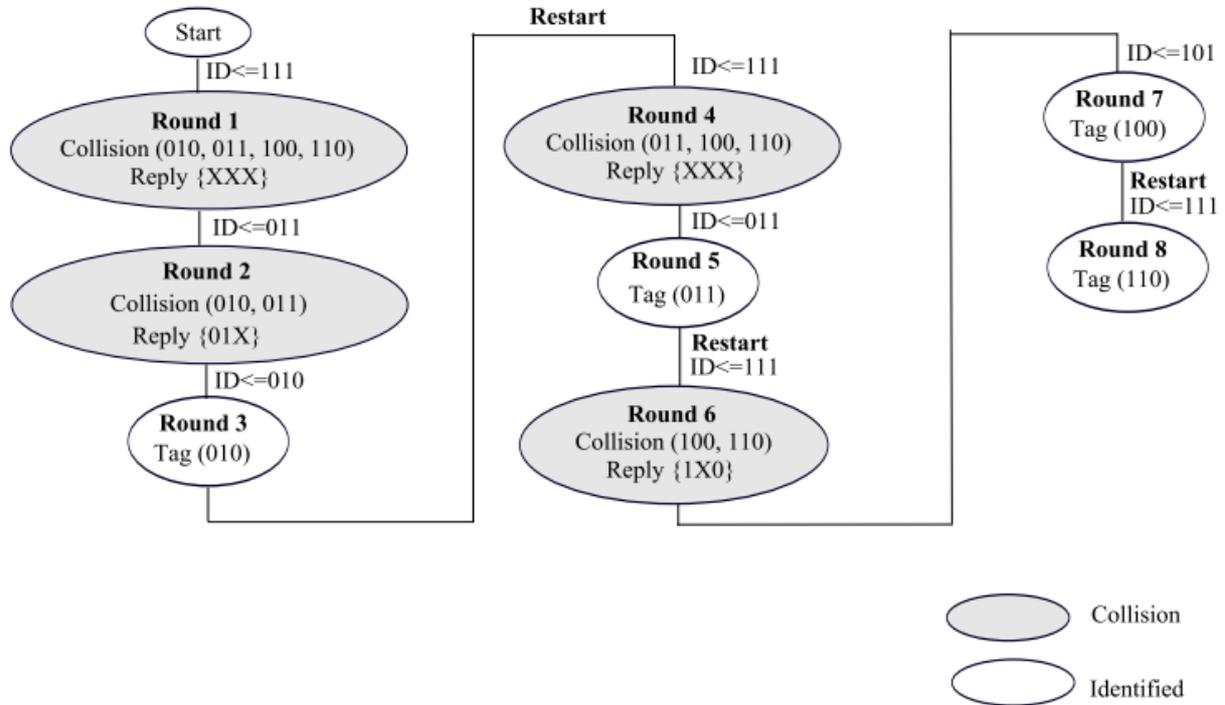


**Fig. 3.9.3 : Bit coding using Manchester and NRZ code**

- **NRZ Code**
  - The value of a bit is defined by the static level of the transmission channel within a bit window ( $t_{BIT}$ ).
  - In this example a logic 1 is coded by a static 'high' level; a logic 0 is coded by a static 'low' level.
  - If at least one of the two transponders sends a subcarrier signal, then this is interpreted by the reader as a 'high' level and in our example is assigned the logic value 1.



- The reader cannot detect whether the sequence of bits it is receiving can be traced back to the superposition of transmissions from several transponders or the signal from a single transponder.
  - The use of a block checksum (parity, CRC) can only detect a transmission error 'somewhere' in the data block.
- **Manchester code**
- The value of a bit is defined by the change in level (negative or positive transition) within a bit window ( $t_{\text{BIT}}$ ).
  - A logic 0 in this example is coded by a positive transition; a logic 1 is coded by a negative transition. The 'no transition' state is not permissible during data transmission and is recognized as an error.
  - If two (or more) transponders simultaneously transmit bits of different values then the positive and negative transitions of the received bits cancel each other out, so that a subcarrier signal is received for the duration of an entire bit.
  - This state is not permissible in the Manchester coding system and therefore leads to an error. It is thus possible to trace a collision to an individual bit.
- Binary Search algorithm involves the reader transmitting a serial number to tags, which they then compare against their ID. Those tags with ID equal to or lower than the serial number respond. The reader then monitors tags reply bit by bit using Manchester coding, and once a collision occurs, the reader splits tags into subsets based on collided bits.
- The construction of an ID binary tree for the example tag set A=010, B=011, C=100, and D=110.
- Initially, the reader starts reading with the maximum possible tag ID value, i.e., 111.
- Tags with an ID value less than 111 respond, resulting in the reply XXX. This indicates all three bits have experienced a collision.
- In the next slot, the reader transmits a new query by replacing the most significant collided bit (MSB) with a 0 and sets the other bits to 1, i.e., the new query becomes 011. The reader transmits a new query, 011, in the next slot, and all tags compare their ID with the received value. Communication in this slot again results in a collision (01X).
- In the second slot, the reader replaces the third bit of the command with a 0 and transmits the next query, 010. In the new interrogation round (slot 3) only Tag A has a value equal to or lower than 010, and therefore it is successfully identified.
- After this slot, the reader restarts the query value with the initial value 111 and transmits it. This procedure is repeated until all of the tags are identified.



**Fig. 3.9.4 : Example of the binary search algorithm**

- This protocol has two additional versions: Enhanced BS protocol (EBSA) and Dynamic BS protocol (DBSA).
- The main difference from EBSA is that it does not restart the reading procedure after a tag is identified, as in the basic version of BS. To reduce bit consumption, in the initial slot, the reader transmits only '1' instead of all '1's.
- In the DBSA version, the reader uses the knowledge from the last slot and reduces the number of transmitting bits. For example, if the reader has received 01X, it will request the tags to transmit only the last bit, since the initial prefix has already been identified.

**Table 3.9.2 : Example of the BS protocol**

Slot Number	Reader Command	Tag A (010)	Tag B (011)	Tag C (100)	Tag D (110)	Result	Type of Slot
Slot 1	111	010	011	100	110	XXX	Collision
Slot 2	011	010	011			01X	Collision
Slot 3	010	010				010	Success



Slot Number	Reader Command	Tag A (010)	Tag B (011)	Tag C (100)	Tag D (110)	Result	Type of Slot
Slot 4	111		011	100	110	XXX	Collision
Slot 5	011		011			011	Success
Slot 6	111			100	110	1×0	Collision
Slot 7	101			100		100	Success
Slot 8	111				110	110	Success

### 3.9.2 Tree Splitting Algorithms

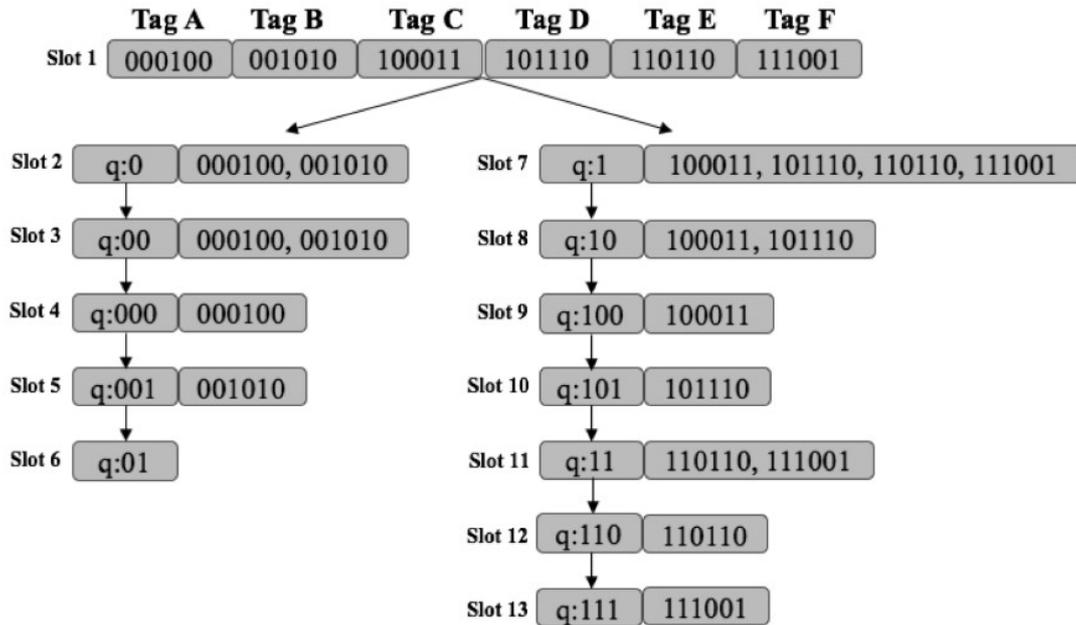
- We have seen that slotted Aloha has maximal throughput  $1/e$ .
- Now we will look at more sophisticated collision resolution techniques which have higher achievable throughput.
- These techniques also maintain stability without a complex estimation procedure like in pseudo-Bayesian slotted Aloha.
- The way they obtain this is by choosing different retransmission probability for different nodes, at each time slot during collision resolution the nodes are subdivided into two sets.
- A preliminary explanation as to how this is possible is to consider an algorithm that will make new arrivals wait until an ongoing collision has been resolved.
- Assuming a small attempt rate, it is most likely to have only two packets colliding. All other nodes will refrain from transmitting until they have observed that those two backlogged packets have been successfully transmitted.
- Each of the colliding packets could then be retransmitted with probability  $1/2$  leading to successful retransmission of one of them with probability  $1/2$  and the other could then be transmitted in next slot. With probability  $1/2$  another collision or an idle slot occurs.
- If so, the two packets would again be retransmitted with probability  $1/2$  until a successful transmission occurred which would be followed by the transmission of the remaining packet.
- The probability of two slots for retransmitting the packets is  $1/2$  since this happens if there is no further collision. Probability for three slots is  $1/4$ , probability for  $i$  slots is  $2^{-(i-1)}$ . The expected value for number of slots to send these two packets is thus  $\sum_{i=2}^{\infty} i \cdot 2^{-(i-1)} = 3$ .
- Thus we get a throughput of  $2/3$  for the period during which the collision is resolved.
- Various ways to choose whether to transmit or not in successive slots:
  - o Random choice ("flip an unbiased coin")



- Using arrival time of its collided packet
- Node identifier (in case of finite number of nodes)
- All alternatives have the property that the set of colliding nodes is split into subsets, one of which is transmitting in the next slot. If the collision is not resolved, then a further splitting into subsets is performed.
- We assume slotted channel, Poisson arrivals, collision or perfect reception, (0, 1, e) immediate feedback, retransmission of collisions, and an infinite set of nodes.
- When collision occurs in slot  $k$ , all nodes not involved in collision goes into waiting mode, the rest are split into two subsets.

### 3.9.3 Query Tree Protocol

- The query tree protocol (QT) is one of the most representative memory less protocols, in which the reader must provide the tags with a query and the matching tags must respond with their full ID.
- Tag response depends directly on the current query, ignoring the prior communication history.
- QT tags involve only simple hardware requirements because they only compare the reader query with their own ID and respond if it coincides.
- The identification process consists of more rounds in which the reader sends a query, and tags whose ID prefix match the current query respond with their whole ID binary value.
- In the case of a collision, the reader forms two new queries by appending  $q$  with a binary 0 or 1.
- New queries will be placed in a Last Input First Output stack (LIFO). If there is no response to a query, the reader knows that there is no tag with the required prefix, and the query is rejected. This kind of slot is called idle.
- If just one tag responds to the reader query, that tag will be identified. By extending the query prefixes until only one tag's ID matches, the algorithm can identify the rest of the tags.
- The identification procedure is completed when the LIFO stack is empty.



**Fig. 3.9.5 : Example of the QT protocol**

- Fig. 3.9.5 shows the QT protocol being used to read 6 tags (Tag A–Tag F). Each tag uses an ID length of  $k=6$  bits. Initially, the LIFO stack is empty, and the reader begins with a null string.
- After a collision occurs, the reader pushes queries 0 and 1 into LIFO stack. During the second round, the reader pops from the stack and transmits query 0.
- In the example in Fig. 3.9.5, tags 000100 and 001010 match the required prefix, which causes both to transmit and collide. The reader is unable to understand the messages from the tags.
- The reader then pushes into the stack queries 01 and 00. In the next round, the reader transmits query 00. Again, both protocols respond with their ID and a new collision occurs.
- In the stack, the following new queries are added: 001 and 000. The reader transmits query 000 and only one tag responds (000100). This tag is successfully identified and will not answer any of the following reader requests.
- The reader then transmits query 001 in slot 4, which matches tag 001010. In the next round, the reader pops and transmits query 01. For this query, there will be no response since no tags contain that prefix.
- In round 7 the reader transmits query 1 and the tag from the right side of the tree responds. Four tags will receive this query and a new collision occurs. The reader experiences a collision, since tags 100011, 101110, 110110 and 111001 responded to the query 1.
- As a result, queries 11 and 10 are pushed onto the stack. The identification process is repeated until round 13, in which the reader transmits the last query (111) from the stack. Overall, the reader uses 13 rounds to read 6 tags.

### 3.9.4 Smart Trend Traversal Protocol



- The Smart Trend Traversal protocol (STT) is a deterministic and memory less protocol that was created with the aim of reducing the number of collisions in the QT protocol.
- This protocol has the ability to dynamically issue queries according to an online, learned tag density and distribution. It proposes a combination of the QT protocol and the shortcutting method in order to skip a query that results in a collision. When the protocol detects the potential possibility of a collision, it will avoid it and move to the bottom level of the binary query tree. STT provides trend recognition.
- The reader keeps track of the tag density and distribution in order to issue subsequent queries, and consequently, minimizes the number of empty slots and collision slots.
- In this protocol, it is not necessary to have any prior knowledge of the network, and it outperforms the existing protocols. The ideal number of queries can be the total number of single nodes. The ideal queries group, referred to as the query traversal path (QTP), is denoted by  $Q = q_1, q_2, q_3, \dots, q_n$ , where  $q_n$  is the last query used in the identification process.
- It is difficult to achieve, but is desirable to get close to its value. The reader can calculate the subsequent queries depending on the tag response, which can be classified into three types :
  1. A collision occurs when the QTP is at too high a certain level and should be moved down by adding a longer prefix to the query. Consequently, the reader appends  $t$  bits of 0's to the last query, where  $t = s + n_{col} - 1$ . Let  $s$  denote the minimum increase, and  $n_{col}$  be the number of consecutive colliding slots.
  2. An idle slot occurs when no tag responds to a reader query. QTP needs to traverse up just one level, which can lead to a new collision. This rule will be applied only to the right side. If the empty response comes from the left side of the tree, QTP must move horizontally to the right. The reader will decrease the query length by  $m$  bits, where  $m = s + n_{emp} - 1$  and  $n_{emp}$  is the number of consecutive idle slots.
  3. Upon a successful response, a single node is visited, indicating that the tag has been successfully identified by the reader. Then QTP moves to the symmetric node if the query finishes with a 0, but it returns one level if the query finishes with a 1.
- The identification process of the STT protocol, which was explained above, is depicted in Fig. 3.9.6 with 4 tags.

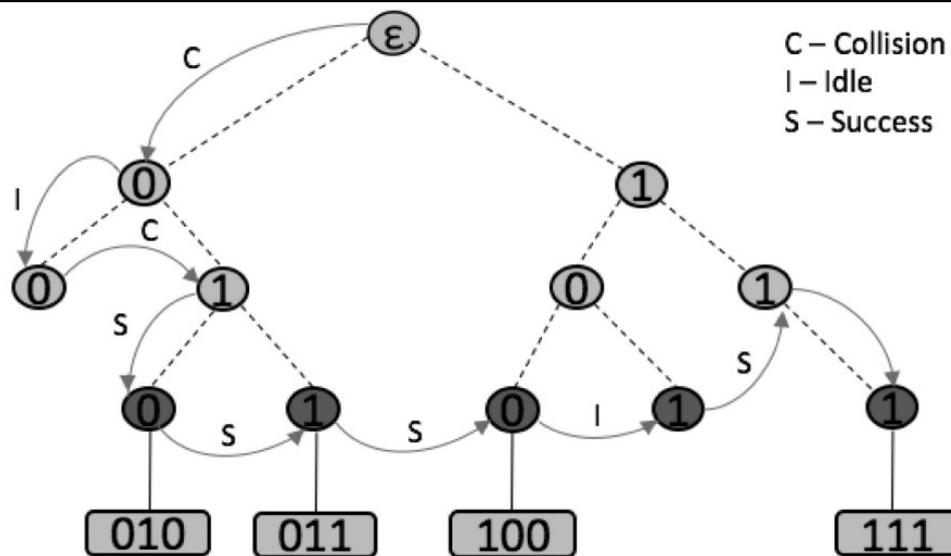


Fig. 3.9.6 : Example of STT protocol

- In conclusion, STT significantly reduces the number of collisions, the identification time, and the energy consumption as compared to the existing Aloha-based and tree-based protocols.

### 3.9.5 Window Based Protocols

- In the majority of tree-based protocols, tags respond with their full ID or with the bits from the last query, when the query sent by the reader matches the tag ID prefix.
- Fig. 3.9.7 shows an example of a communication slot between the reader and the tag. To reduce the number of bits transmitted by the tag, a window method has been proposed.
- In the identification process, many slots ultimately collide, resulting in a huge waste of bits. Protocols using the window method reduce the number of bits transmitted by the tags.
- The window is defined as a bit-string of length  $w_s$  bits transmitted by a tag in a slot. This bit-string is computed on the reader side, respecting the condition  $0 < w_s < k$ . It is shown in Fig. 3.9.8.
- Most tree-based protocols use a fixed tag response during the identification process, but some use different operational process methods with a dynamic response that is based on window synchronization.

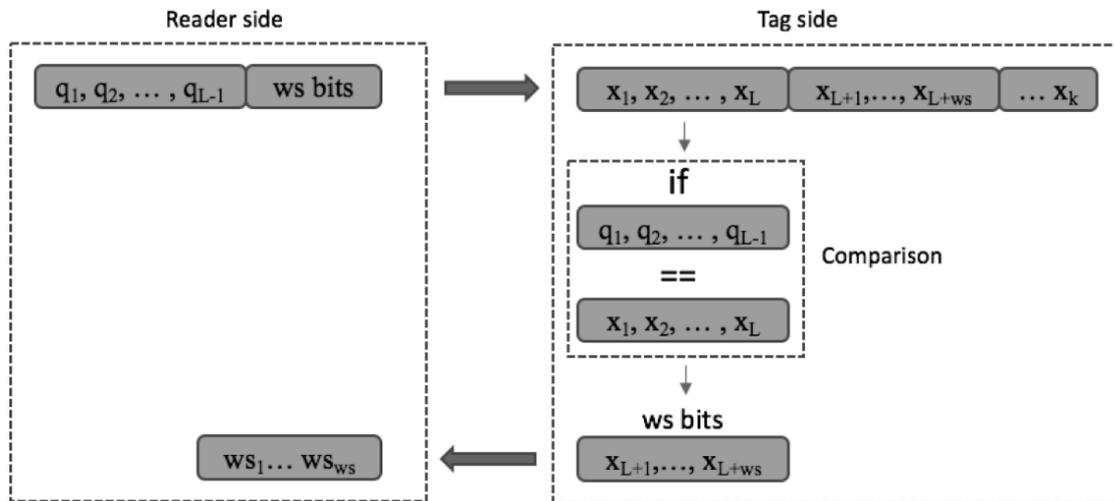


Fig. 3.9.7 : Example of a communication slot between the reader and one tag

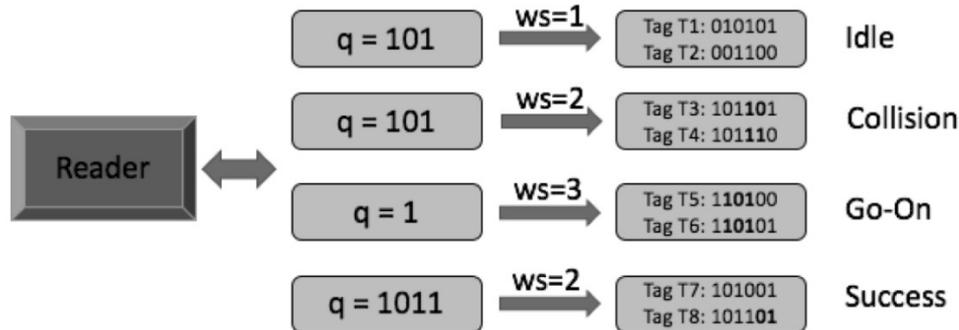


Fig. 3.9.8 : Window synchronized answer

### 3.9.6 Query Window Tree Protocol

- The Query Window Tree protocol (QWT) is a memoryless tree-based protocol that applies a dynamic bit window to QT. Tags respond directly depending on the current query.
- QWT tags compare their ID value with the query received and transmit a certain number of bits, managed by the reader. This reduces the complexity of passive tags, their energy consumed, and the identification time.
- A reader and tag flow chart for QWT are shown in Fig. 3.9.9 (a) and (b). When tags appear in the interrogation area, the reader will broadcast to them by transmitting a query length of  $L$  bits.
- Tags will respond if their ID prefix matches the query sent by the reader, but with the previously specified number of bits. One of the main features is that the total number of collisions is decreased by transforming potential collisions into partial successful slots. This is a new type of slot, called go-on slots.

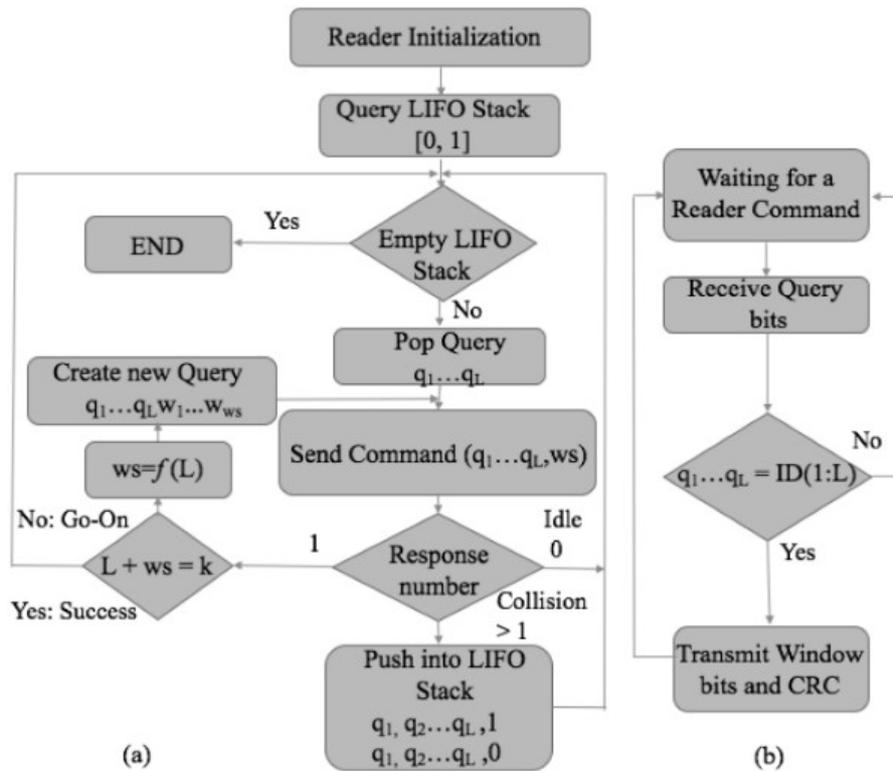


Fig. 3.9.9 : Flow chart of QwT protocol : (a) for reader; (b) for tags.

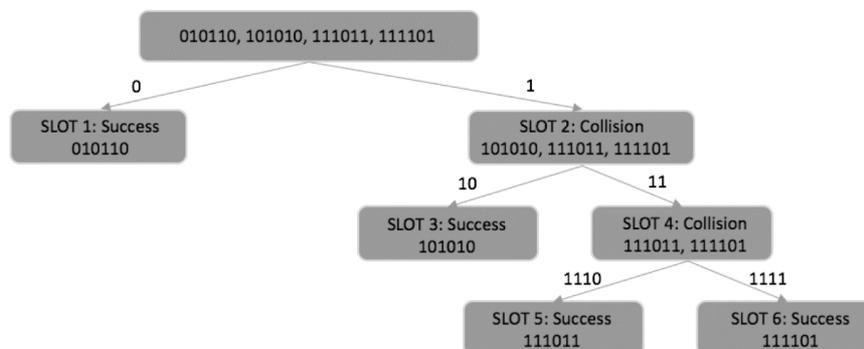
- The previously explained window methodology is implemented in the QWT protocol. The window allows tags to transmit only the bit-string instead of their full ID.
- If tags match a reader query, they will synchronously transmit the next adjacent was bits of the ID. This protocol uses cyclic redundancy check (CRC) in order to differentiate between the types of tag responses. Accordingly, the slot types that can occur in the QWT protocol can be classified into 4 groups :
  1. **Collision slot** : When the reader cannot differentiate the answer, they will create two new queries by appending '0' and '1' to the former query  $[q_1, q_2 \dots q_L]$ . The window size  $w_s$ , will remain unchanged, with the value used in the previous query.
  2. **Idle slot** : When there is no response, the reader will discard the query and retain the same  $w_s$  as that of the last command.
  3. **Go-on slot** : This occurs when at least one tag responds with a window and the reader is able to understand it. If  $L + w_s < k$  is not true, the reader will transmit a new query created from the former query and received window. During this query, the reader will append an updated  $w_s$  value.
  4. **Success slot** : This is a type of go-on slot where the reader successfully receives the last part of the tag ID and  $L + w_s = k$ . Then, the reader can save the tag, calculate the new  $w_s$ , and continue with the identification process.
- Using the QwT protocol, the reader computes  $w_s$  using the expression  $f(L) = k(1 - e^{-\beta L})$ ,  $0 < L \leq k$ , where  $\beta$  is an adjustable parameter. This heuristic function is used to provide dynamism to the

value of  $w_s$ . It can only be applied to the go-on and Success slots, since in a Collision or Idle slot,  $w_s$  will be held unchanged.

- The proposed protocol maintains the memoryless feature of QT in that it is an applied bit window procedure.
- It provides a decrease in the number of tag-transmitted bits, but increases the number of slots and reader-transmitted bits. Altogether, this tree-based protocol achieves significant energy savings and a reduction in identification time.

### 3.9.7 Collision Tree Protocol

- The Collision Tree protocol (CT) is an improvement of QT which uses bit-tracking technology in order to find which bits have collided as well as where they are.
- The reader, using the bit-tracking technology, can trace a collision to an individual bit and get the correct bits successfully. This feature works using Manchester coding, which can locate the conflicting bits based on voltage transitions.
- The basic features of this protocol is that it decreases collision slots and eliminates idle slots. This contributes to improved results in terms of latency and the number of bits transmitted.
- The advantage of this protocol compared to the QT protocol is that CT has no idle slots and reduces collision slots.



**Fig. 3.9.10 : Example of the CT protocol**

- Fig. 3.9.10 reveals how this protocol works in an environment with 4 tags. At the beginning of the identification process, the reader generates two queries '1' and '0' into a LIFO stack. Then, the reader pops query '0' from the stack and transmits it to the tags.
- In this case, one tag (010110) matches the query and responds with its ID, and the tag is identified. Then, the reader sends a new query from stack '1' and a collision occurs. Through bit-tracking, the reader can find the colliding bits and thereby resolve potential collisions.
- The reader pushes two new queries '11' and '10', and firstly transmits '10'. The second tag is identified (101010). On the next transmission, a collision once again occurs. The reader can trace the collision to the fourth bit.
- Two new queries are made: '1111' and '1110'. These are the last queries in the interrogation round because both tags (111011, 111101) are identified.



- From this example it may be noted that there are no idle slots and the number of collision slots and latency are reduced, which is the basic aim of the CT protocol.
- In conclusion, CT is a stable and efficient anti-collision protocol for RFID tag identification. The performance of CT is very dependent on the total number of tags in the interrogation area.

### 3.9.8 Bitwise Arbitration (BTA) Algorithms

- Unlike TS, QT, and IDS protocols, BTA algorithms operate by requesting tags to respond bit by bit from the most significant bit (MSB) to the Least Significant Bit (LSB) of their ID.
- The key feature of BTA algorithms is that bit replies are synchronized, meaning multiple tags responses of the same bit value result in no collision.
- A collision is observed only if two tags respond with different bit values. Moreover, the reader has to specify the bit position it wants to read.

### 3.9.9 A Comparison of Tree Protocols

Table 3.9.3

Criterion	Query Tree (QT)	Tree Splitting (TS)	Binary Search (BS)	Bitwise Arbitration (BTA)
<b>Protocol feature</b>	The reader transmits a query, and tags with prefix matching the query respond.	The algorithm performs collision resolution by splitting collided tags into disjoint subsets.	The reader sends a serial number to tags, and those with values less than or equal to the serial number reply.	Each tag responds in a bit by bit manner.
<b>Tag requirements</b>	Prefix matching and synchronization circuitry.	Random number generator, synchronization circuits, and counters to store state information.	Manchester coding scheme, synchronization circuits.	Synchronization circuits, ability to respond in a bit-by-bit manner.
<b>RTF/ TTF</b>	RTF (Reader-Talk-First)			
<b>Time complexity (1)(3)</b>	$O(n)$	$O(n)$	$O(\log n)$	$O(2k)$
<b>Message complexity (2)(3)</b>	$2.21k \log n + 4.19k$	$n \log n$	Not specified	$O(n(k + 1))$
<b>Tag cost</b>	Least -----> Most			
<b>System cost</b>	Least -----> Most			

(1) Time required to identify all tags.



(2) Number of messages tags need to transmit before they are identified successfully.

(3)  $n$  denotes the number of tags and  $k$  denotes the length of tag's ID.

### 3.10 Hybrid Protocols

---

- Hybrid protocols combine the advantages of tree-based and Aloha-based protocols to avoid their problems and provide better features in tag identification.
- Most of them first implement a tree-based procedure and tag estimation procedure in order to predict the number of tags.
- Therefore, the combined Aloha-based and tree-based protocol procedures are known for their high complexity and hardware demands. This kind of protocol can significantly increase performance as compared to the previous ones.
- Recent proposals include the Tree Slotted Aloha (TSA) and Binary Tree Slotted Aloha (BTSA). TSA uses a tree structure, and the tag's responses are organized in slots, as in FSA. In the BTSA protocol, tags randomly choose a slot after the reader query.
- Tree Slotted Aloha (TSA) is a probabilistic protocol created to reduce the number of collisions occurring in FSA. When more tags collide in a slot, FSA attempts to solve this problem in the next frame. However, in the new approach, if more tags collide in a frame, only those tags that are involved in that collision are queried in the next slot.
- The reader in the Binary Tree Slotted Aloha (BTSA) uses a dynamic frame length adjustment and BTSA algorithm. Each tag from the interrogation area randomly chooses a slot and transmit its ID. If the reader successfully identifies a tag it will not be activated in the subsequent slots. When a collision occurs, the collided tags are resolved by binary tree splitting, while the rest of the tags will wait until that process is successfully completed.
- Dynamic Binary Tree Slotted Aloha (dynamic BTSA) involves a dynamic frame adjustment and the basic BTSA algorithm. The advantage of this protocol is that the reader can adjust its frame size by judging only the first slot type in the identification process.
- Adaptive Binary Tree Slotted Aloha (Adaptive BTSA) offers an improvement to the Q protocol. This protocol adjusts the frame size based on the tags' responses in a current slot. Adaptive BTSA first uses features from the Q protocol. If there are numerous collisions in a frame, the reader ends the frame earlier and transmits a new command with a new frame length. If there are excessive idle slots, the reader once again ends the frame earlier and sends a new command with a smaller frame length.

### 3.11 A Comparison of Aloha, Tree-based and Hybrid Protocols

---

**Table 3.11.1**



Criterion	Aloha Protocols	Tree-Based Protocols	Hybrid Protocols
Protocol feature	They use random multi-access means to identify tags. In the case of collision, tags will be asked to send data later with a random time relay.	They identify the total number of tags in the interrogation zone. The reader controls every step of the protocol, using commands or queries to split colliding tags into subsets, and further repeatedly split those subsets until identifying all of the tags.	Tree-based protocols. They use two methods. The first uses randomized divisions in tree-based algorithms, and another uses tree strategies after a collision in Aloha algorithms.
Number of tags to reader commands	Low	High	Medium
Usage	Aloha protocols are commonly used in LF, HF and UHF RFID (18000-6C) systems.	Tree-based protocols are commonly used in HF, UHF and microwave (18000-6B and 18000-7) RFID systems.	Not implemented on any standard
Method	Probabilistic	Deterministic	Mixture (Aloha and Tree-based)
Tag starvation	Yes	No	No