RFID Security: An Overview

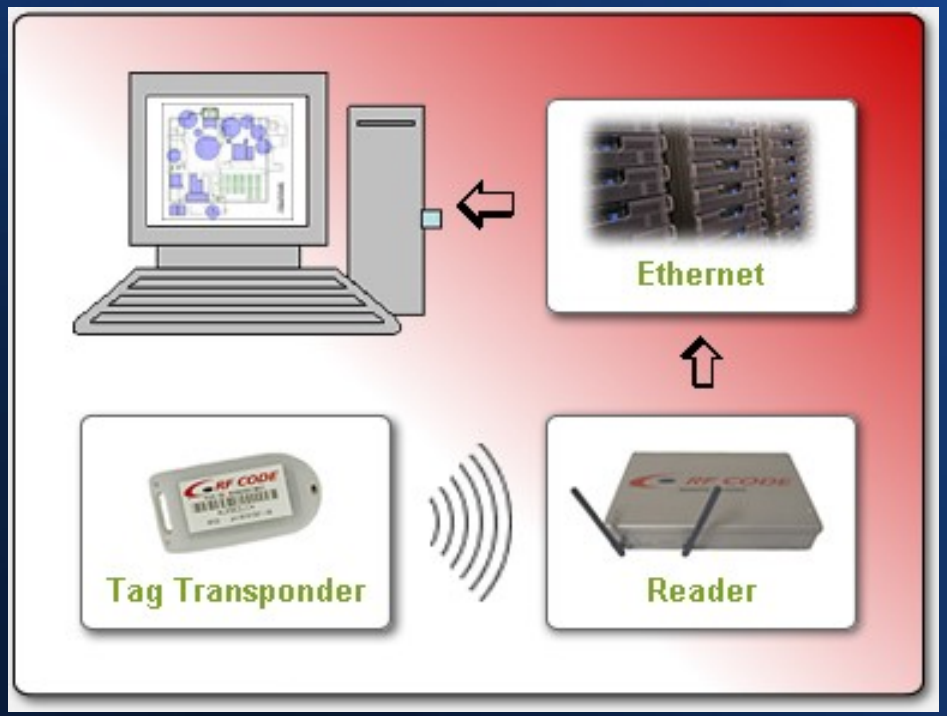
Date: 09 Feb, 2011

Talk By:

Vivek Vardhan Bilangi

Introduction

RFID is a communication technology - uses Radio Waves for data transmission.



Two Primary Components

1. RFID Tag
2. RFID Reader

Introduction

- RFID Reader - communicates with the Tag and retrieves information from the Tag.

- RFID Tag - microchip capable of wireless communication with the Reader.

Introduction

- Two types of RFID Tags - Active Tags, Passive Tags.
- Passive Tags - derive power from the Radio Waves.
- Active Tags - dedicated power source (battery) onboard.

- Active Tags can initiate communication with the Reader.
- Passive Tags cannot initiate communication with Reader.

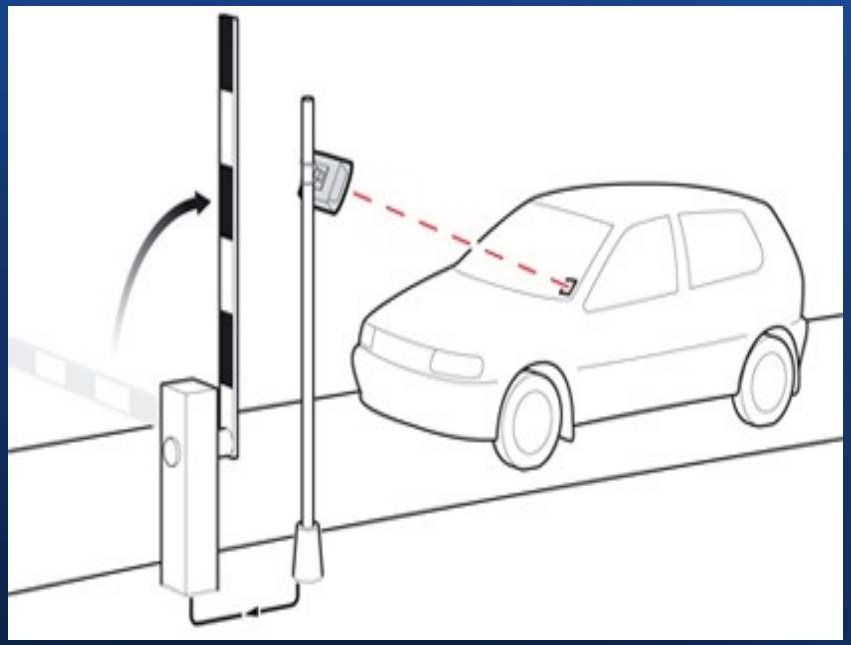
Pros of RFID Systems

- RFID Technology is extremely inexpensive.
- Passive Tag costs $0.10
- Compared to Barcodes, it is more accurate in object tracking, notification and identification.
- The Readers can be either static or mobile.

Areas of Application

- RFID technology is used in a wide variety of areas and is deemed to be pervasive in the future.
- Current Areas of Use:
  1. Retail Sector
  2. Animal Tracking & Management
  3. Library Management
  4. Transportation Sector, Electronic Parking Tickets etc.

Areas of Application



Electronic Parking Tickets

Security Threats

- Invasion of Privacy:

  1. Discloses valuable and sensitive information about the location and product without being queried.

  2. Careful observation of the queried data can reveal info about the product and the tag owner.

  3. Gives away info to anyone who queries the tags without any discrimination.

Security Threats

- Tag Counterfeit - Easy to manufacture duplicate tags due to the low production costs involved.

- Denial of Service (DoS):

  1. Intentional jamming of the RFID communication channels.
  2. Prevents the Reader - Tag communication.

Security Threats

- Eavesdropping & Traffic Analysis:

  1. Third parties can eavesdrop on RFID communication channels.

  2. Encrypting the information is irrelevant since trends and patterns are important, not data.

  3. More messages exchanges between the Reader and Tag implies more communication.

Security Threats

- Reader Collision Problem:

  1. More of a communication issue in multiple Readers and Tags than a direct security threat.

  2. Caused due the close proximity operation of Readers and Tags.

  3. However, can lead to the loss of data, data mining by third parties and retrieval of data by unauthorized personnel.

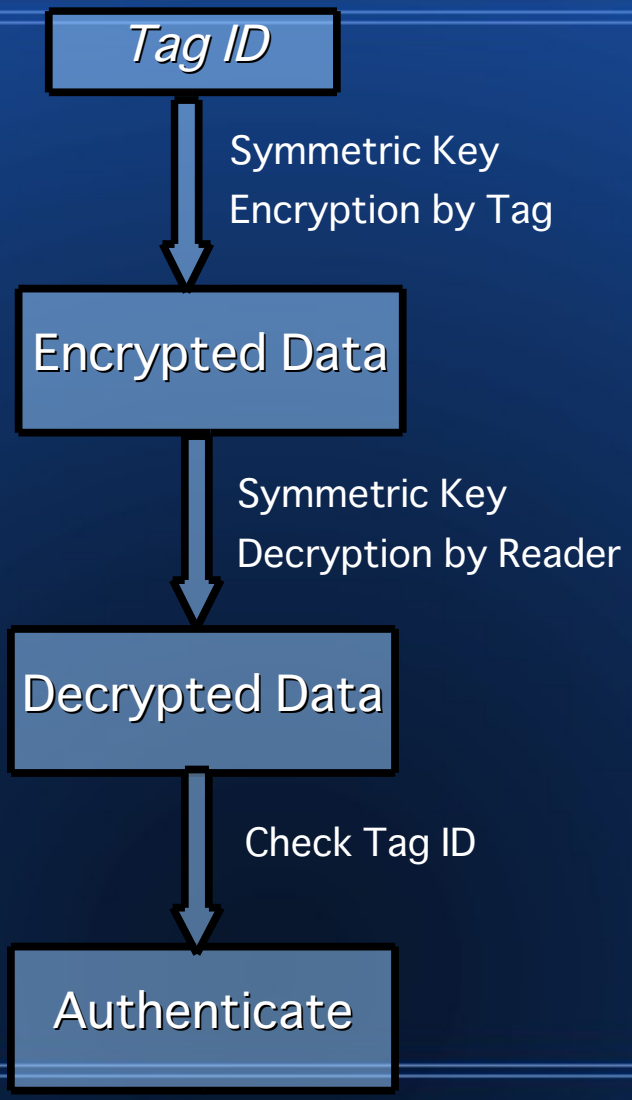
Proposed Solutions - General

- Faraday Cage - A solid cage or mesh - made up of conducting material - blocks static interference.

- Active Jamming - Similar to DoS but intentional jamming of radio signals to block out unauthorized Readers.

- Bill of Rights - A framework of self administered rules for companies involved in RFID technologies.

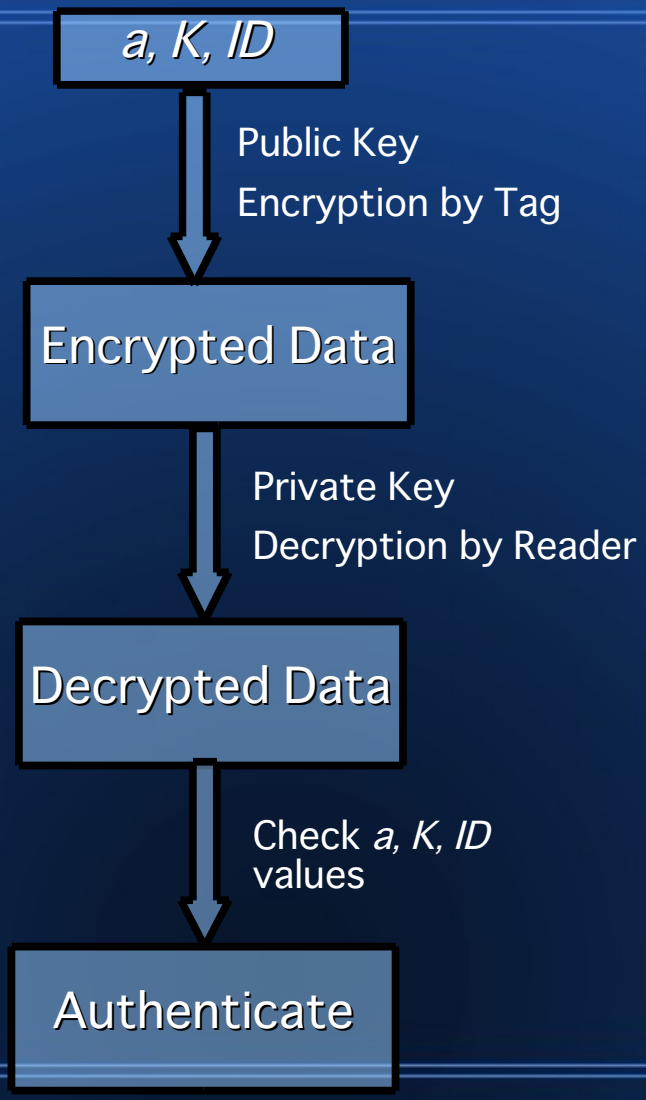
Proposed Solutions - Classic Crypto



- Symmetric Key Encryption:

1. A 128 bit AES encryption implemented on the hardware to enable RFID Tag authentication.
2. Can be used by the RFID Tags to authenticate themselves to the Readers.
3. Can be successfully implemented within the necessary available power for the RFID Tag, which is 9 μA.

Proposed Solutions - Classic Crypto



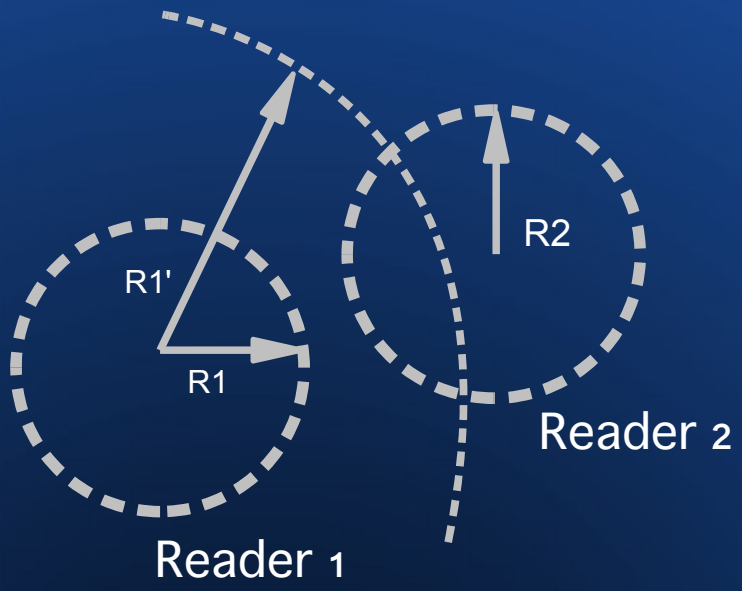
- Public Key Encryption:

1. System sends a random number *"a"* and to the RFID Tag.
2. Tag encrypts its *ID*, a pre-generated number *K* and *"a"* using its public key and transmits back to the Reader.
3. Reader decrypts using its private key.
4. Checks the value of *"a"* and compares *ID* and *K* with the values stored in its database.

Reader Collision Problem

- Caused due to the interference of signals from one Reader with another Reader.
- Interference caused due to multiple Readers working in close proximity to the RFID Tags.
- Interference is of two types:
  1. Reader to Reader Interference
  2. Multiple Reader to Tag Interference.

Reader Collision Problem



R_1 = Read range for reader 1

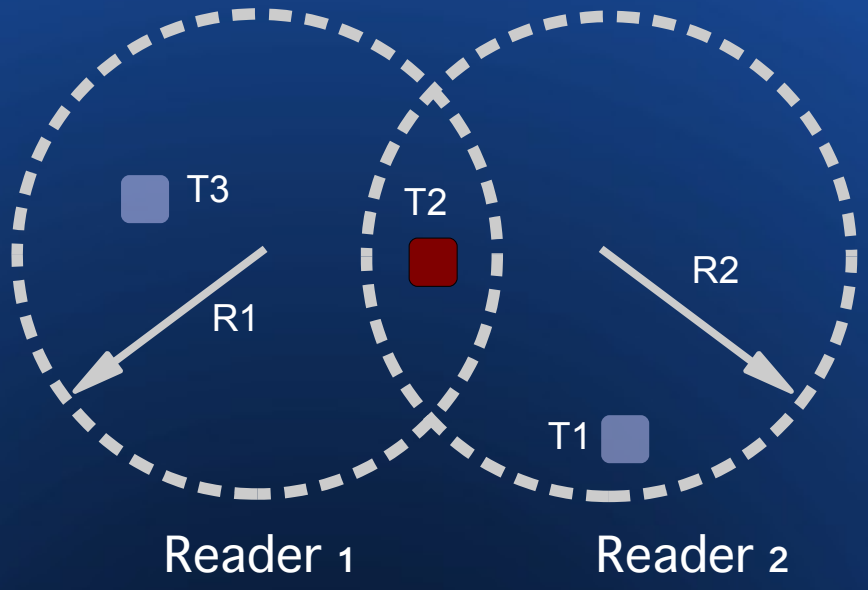
$R_{1'}$ = Interference Range for Reader 1

R_2 = Read range for Reader 2

- Reader to Reader Interference:

1. Occurs when 2 Readers are in operating in proximity.
2. Both the Readers have the same frequency, but different power levels.
3. Higher operating power for one Reader increases the range of the Reader causing interference.
4. Interference - *Reader Jamming*.

Reader Collision Problem



R_1 = Read range for reader 1

R_2 = Read range for Reader 2

T_1 = Tag 1; T_2 = Tag 2; T_3 = Tag 3

T_2 = Tag in conflict

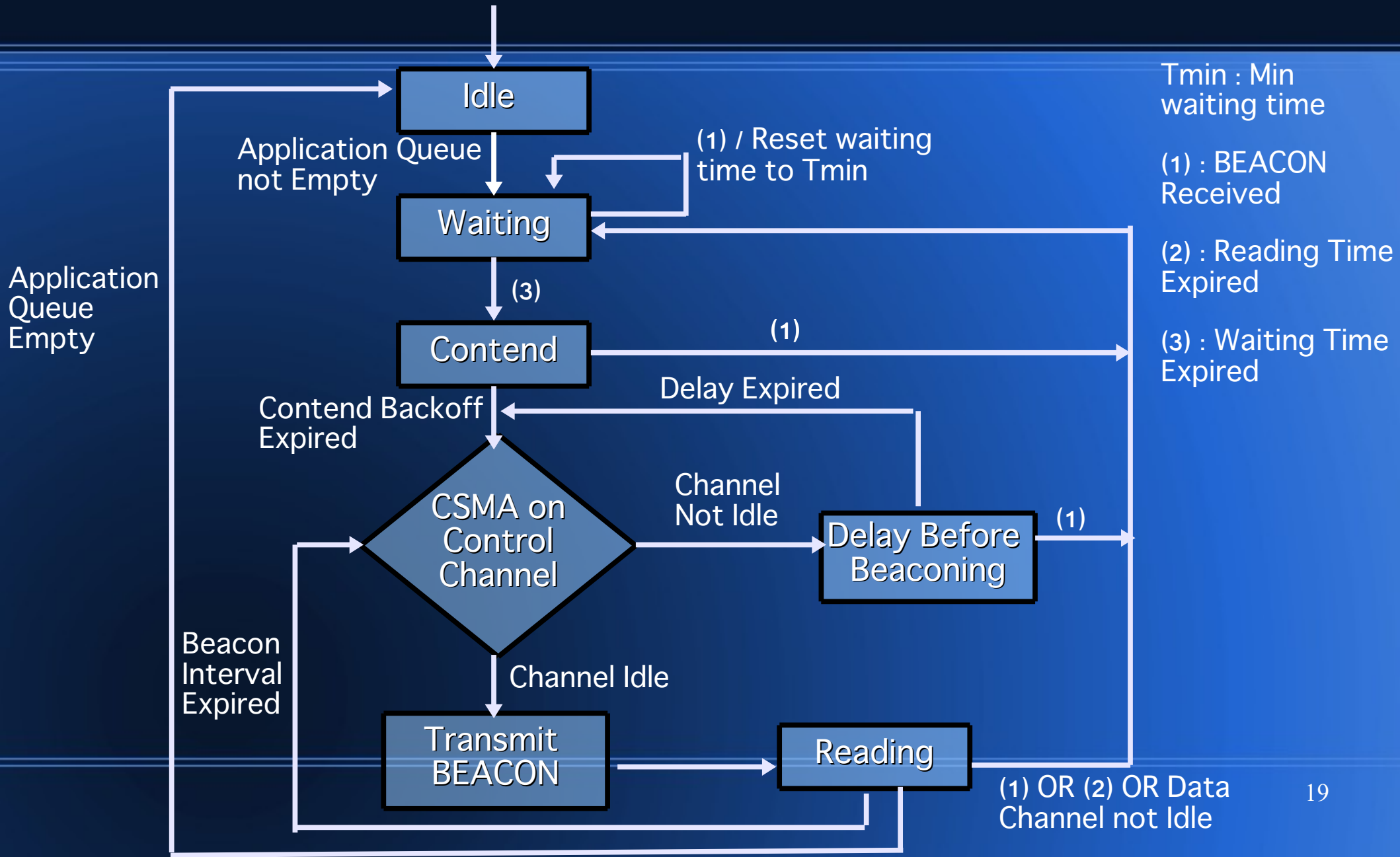
- Multiple Reader to Tag Interference:

1. Tag can communicate with only one Reader at a time.
2. Problem - when 2 Readers located at the same distance try to read a Tag.
3. Read ranges overlap - hence the Tag is not read by any of the Readers.
4. Overlapping region - *Dead Zone*
5. Interference - *Tag Jamming*.

Solution - Pulse Protocol

- Beacon Transmitting Mechanism for notification.
- Reader reads Tags on the Data Channel.
- Beacon broadcast on a separate Control Channel.
- Others Readers read the Control Channel first to sense any broadcast beacons.
- If no beacon sensed, Reader sends beacon.
- Keeps periodically sending a beacon in intermittent time intervals, as long as it is reading.

Pulse Protocol - Flow Chart



Pros of Pulse Protocol

- Takes place completely at the Readers end. Tags not involved.
- The Control Channel is sub-band of the Data Channel frequency.
- Splits the communication between the Readers and Tags into two different channels to prevent interference:
  1. Reader - Reader Comm. - Control Channel.
  2. Reader - Tag Comm. - Data Channel.

Conclusion

- Reader Collision problem not a direct security threat, but a problem which leads to a lot of security issues.
- Pulse Protocol solves Reader Collision problem with a greater efficiency as compared to other solutions like CDMA, TDMA, FDMA, CSMA.
- Pulse Protocol has a better throughput i.e. number of Tags identified by the Reader is higher.
- Pulse Protocol has a higher efficiency i.e. lesser collisions during transmissions.

THANK YOU