An Empirical Study of UHF RFID Performance

Michael Buettner and David Wetherall

Presented by Qian (Steve) He

CS 577 - Prof. Bob Kinicki

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Terms

- Ultra-High Frequency (UHF)
  - UHF designates the International Telecommunication Union (ITU) radio frequency range of electromagnetic waves between 300 MHz and 3 GHz.
- Radio-Frequency IDentification (RFID)
- Electronic Product Code (EPC)
  - EPCglobal UHF Class 1 Generation 2 in this paper
  - EPCglobal (a joint venture between GS1 and GS1 US)

Characteristics

- Passive Radio Frequency Identification
  - small, inexpensive computer chip
  - remotely powered
  - interrogated for identifiers and other information

Comparison

- EPC Gen2 standard
  - defines readers and passive tags that operate at UHF frequencies
  - use "backscatter" communication to support read ranges measured in meters
  - high capability of data storage

- Early HF tags
  - based on inductive coupling that only provide read ranges of centimeters
  - active tags that require batteries to increase range

* Privacy

Richard Stallman at WSIS 2005 presenting his RFID badge wrapped with aluminum foil as a way of protesting RFID privacy issues.

Logo of the anti-RFID campaign by German privacy group FoeBuD.

http://en.wikipedia.org/wiki/Radio-frequency_identification

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Backscatter

1. A reader transmits information to a tag by modulating an RF signal
2. The tag receives both down-link information and the entirety of its operating energy from this RF signal.
3. The reader transmits a continuous RF wave (CW) which assures that the tag remains powered
4. The tag then transmits its response by modulating the reflection coefficient of its antenna.
5. The reader is able to decode the tag response by detecting the variation in the reflected CW,

UHF EPC

- Physical Layer
  - RFID tags communicate by "backscattering" signals that are concurrent with reader transmissions, and use a variety of frequencies and encodings under the control of the reader.
- MAC Layer
  - Readers and tags use a variation on slotted Aloha to solve the multi-access problem in a setting where readers can hear tags but tags cannot hear each other.

Physical Layer

- Down-link
  - Amplitude Shift Keying (ASK)
    - bits are indicated by brief periods of low amplitude
  - Pulse Interval Encoding (PIE)
    - the time between low amplitude periods differentiates a zero or a one
    - the reader can choose pulse durations
    - 26.7 kbps to 128 kbps.
- Up-link
  - partially determined by
    - down-link preamble
    - a bit field set in the Query command
  - frequency (40 to 640 kHz) & encoding
    - FM0
    - Miller-2
    - Miller-4
    - Miller-8

MAC Layer

- Based on Framed Slotted Aloha
  - each frame has a number of slots
  - each tag will reply in one randomly selected slot per frame
  - the number of slots in the frame is determined by the reader and can be varied on a per frame basis

Query Round & Circle

- Query Round
  - an individual frame
- Query Cycle
  - the series of Query Rounds between power down periods

Query Round: sequence

1. At the beginning, the reader can optionally transmit a Select command
   - limits the number of active tags by providing a bit mask
   - only tags with ID's (or memory locations) that match this mask will respond in the subsequent round
2. A Query command is transmitted which contains the fields:
   - determine the up-link frequency and data encoding, the Q parameter (determines the number of slots in the Query Round), and a Target parameter.
3. A tag receives a Query command, it chooses a random number in the range $(0, 2^Q - 1)$, where $0 \le Q \le 15$, and the value is stored in the slot counter of the tag. The tag changes its Inventoried flag.

Query Round: sequence (cont.)

4. If a tag stores a 0 in its slot counter, it will transmit a 16 bit random number (RN16) immediately.
5. The reader will echo the RN16 in an ACK packet after receiving it.
6. If the tag successful receives the ACK with the correct random number, the tag will backscatter its ID.

Query Round: sequence (cont.)

7. The reader will send a QueryRepeat command to cause the tag to toggle its Inventoried flag.
   – If the ID was not successfully received by the reader, a NAK command is sent which resets the tag so that a subsequent QueryRepeat will not result in Inventoried flag being changed.
   – A QueryRepeat signals the end of the slot.
8. On receiving the command, the remaining tags will:
   – decrement their slot counter
   – respond with a RN16 if their slot counter is set to 0.
   – The process then repeats, with the number of QueryRepeats being equal to the number of slots set using the Q parameter.

C1G2 Protocol

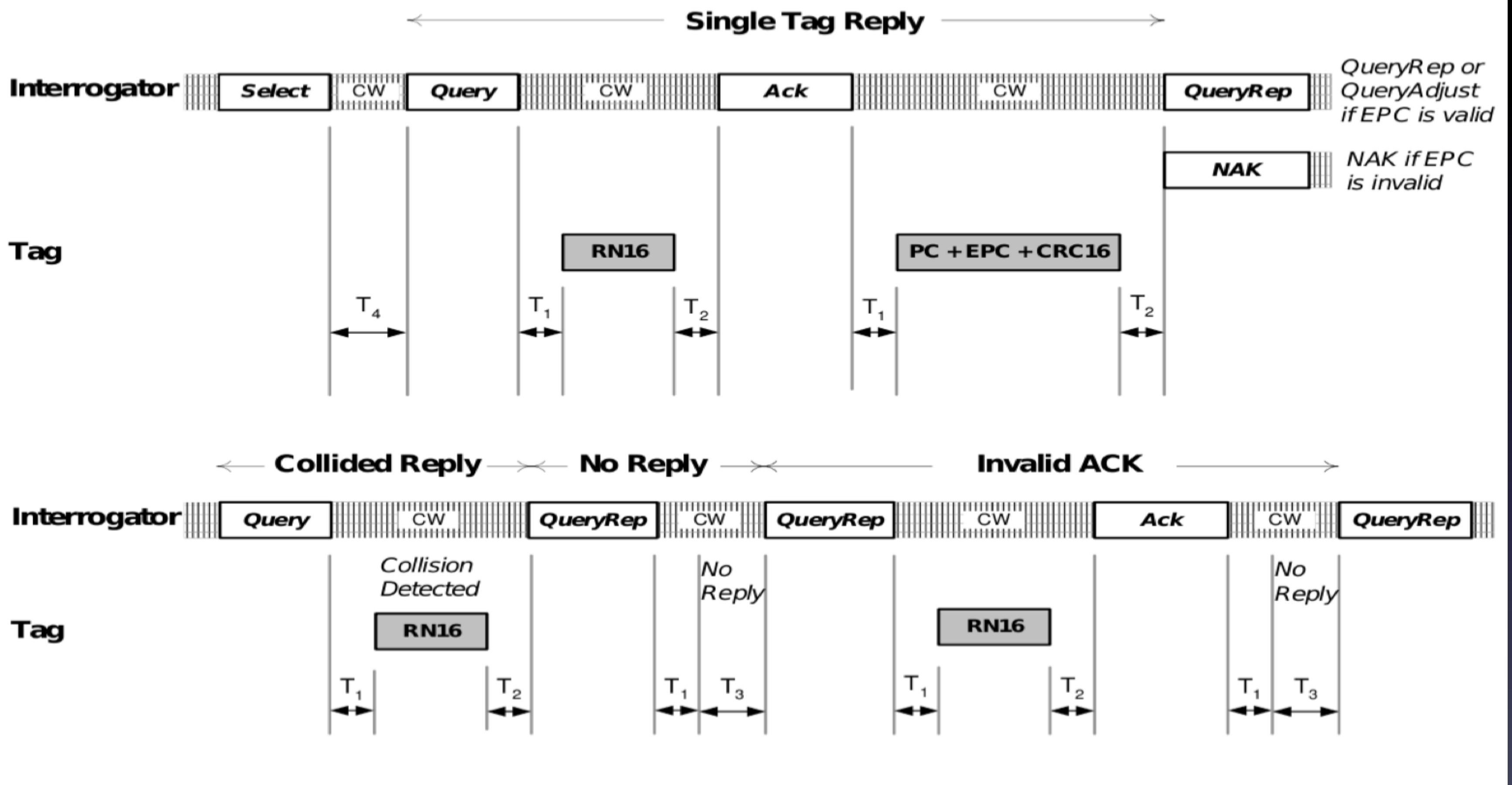


Figure 1: C1G2 Protocol (Courtesy of EPCglobal)

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Tools

Hardware

- Readers
  - Alien Technologies ALR-9800
  - ThingMagic Mercury5e Development kit
- Tags
  - Alien 9460-02 “Omni-Squiggle” tags

Software

- Software
  - Universal Software Radio Peripheral (USRP) platform
  - GNURadio

RFID Readers

Mode	Reader(kbps)	Tag(kHz)	Tag Coding
HS	128	250	FM0
STD	26.7	250	FM0
DR	26.7	250	Miller-4

Assessment

- How well do commercial readers perform?
- What protocol factors degrade reader performance?
- What causes tags to be missed during a read?
- What can be done to improve performance?

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Experiment Settings

- A standard office setting with cubicles of 42 inch height
  - Experiment 1: 30′ x 22′ x 10′
  - Experiment 2: 40′ x 24′ x 13′
- 16 tags were adhered to a sheet of poster board in a 4 x 4 grid, with tags spaced approximately 6 inches apart.

Overall Performance

Read Rate - Distance

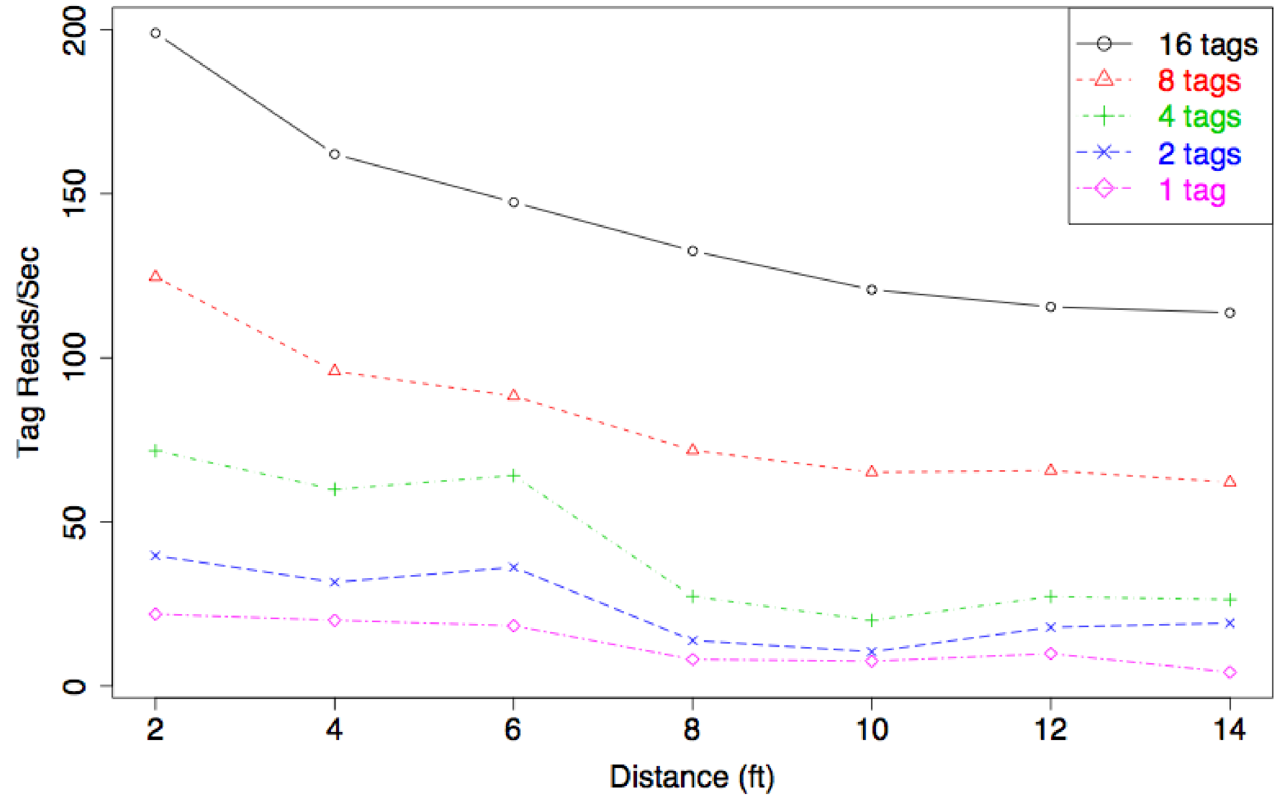


Figure 2: Read rates for High-Speed mode.

Overall Performance

Average Cycle Time – Number of Tags

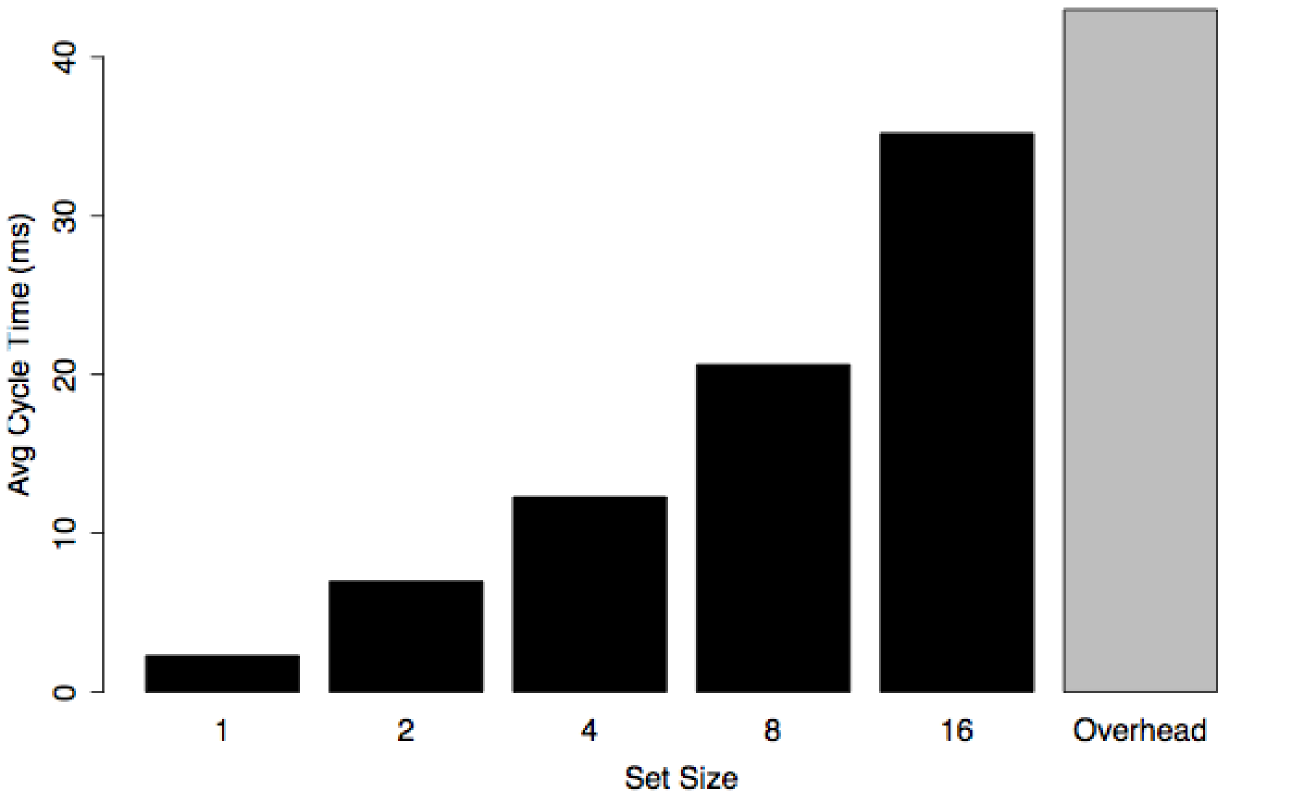


Figure 3: Cycle times and overhead for HS mode at 2 feet

Overall Performance

Read Rate - Coding Scheme

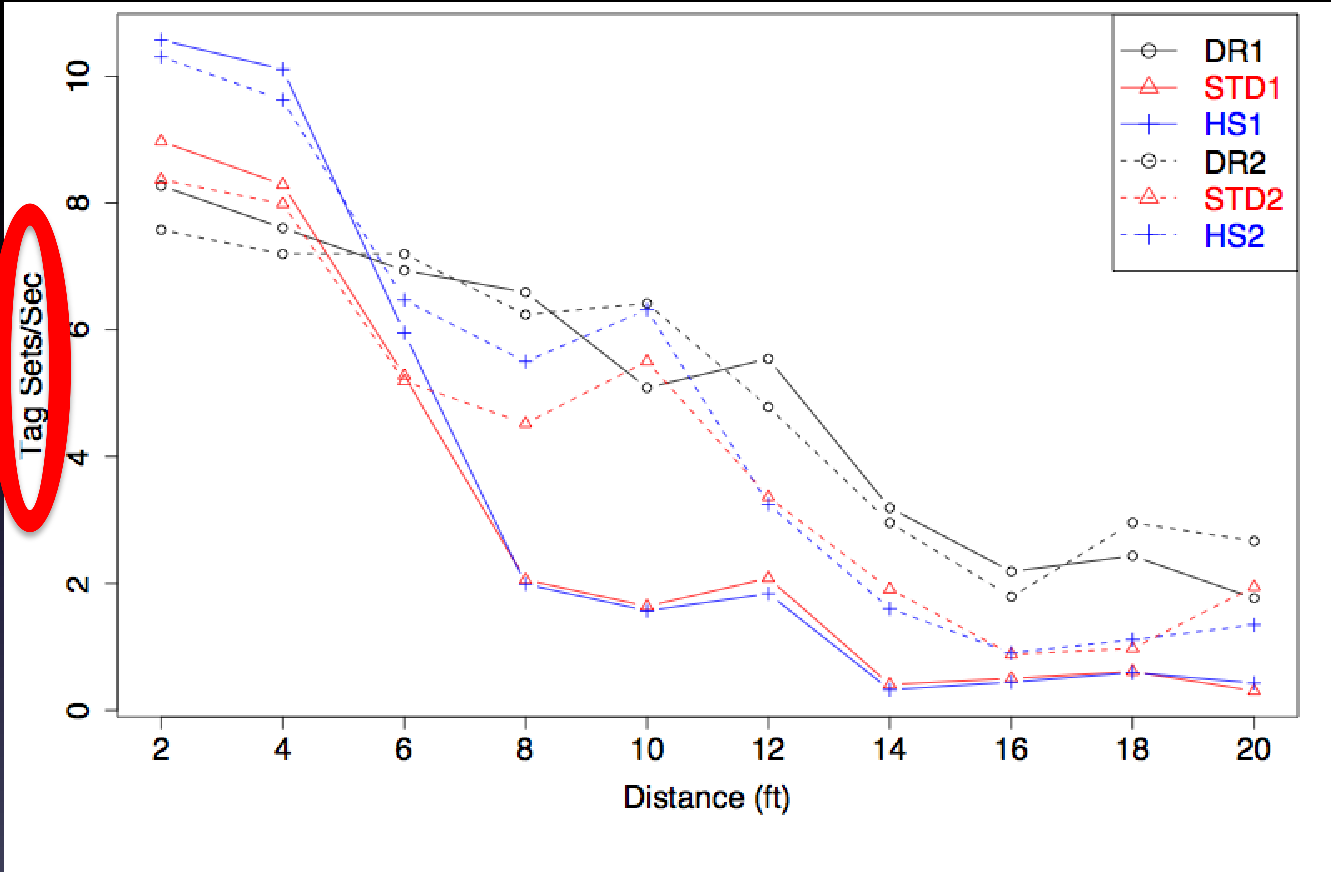
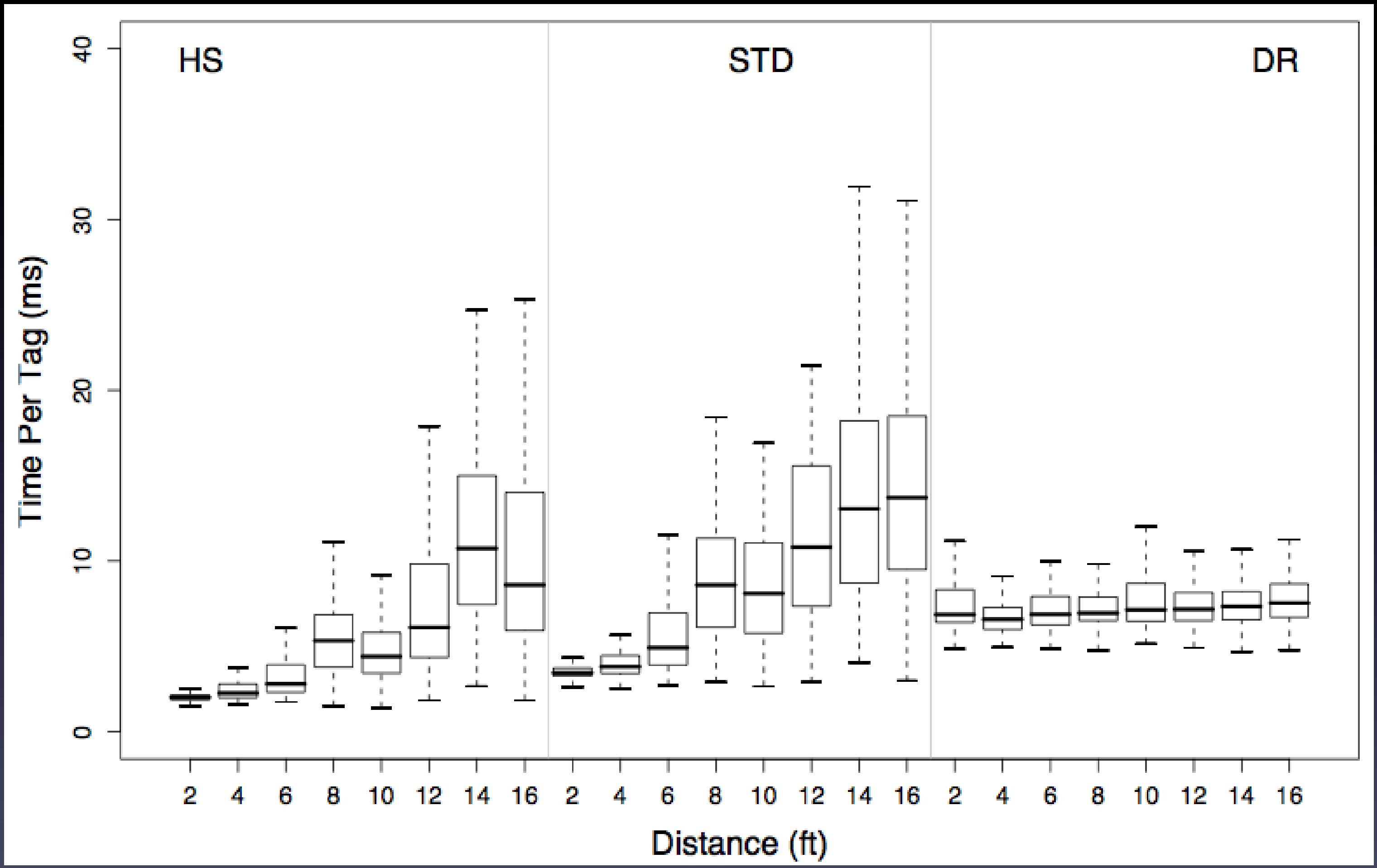


Figure 4: Tag set read-rate for varying coding schemes.

*1 : Experiment 1 *2 : Experiment 2

Cycle Duration



Error Rates

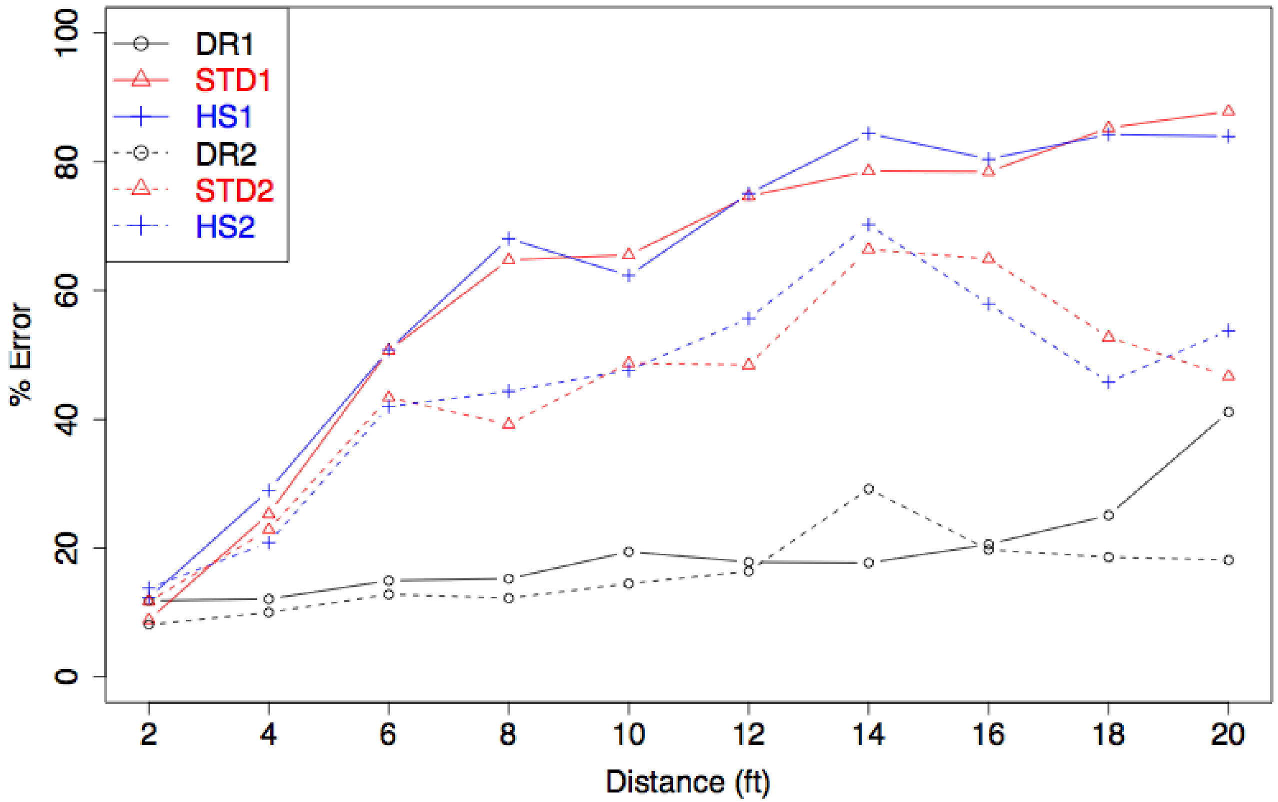


Figure 6: Error rates

Effects of Errors

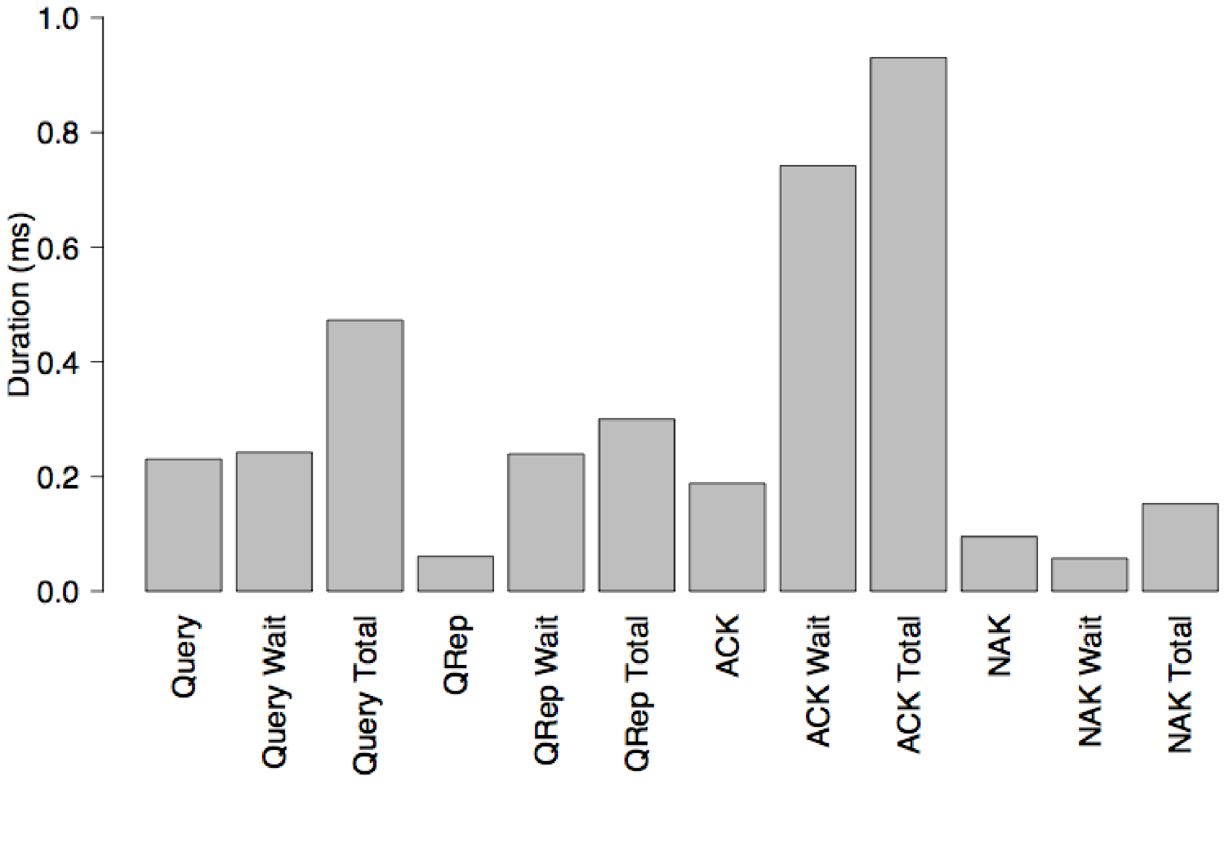


Figure 7: Duration of each command

Effects of Errors (cont.)

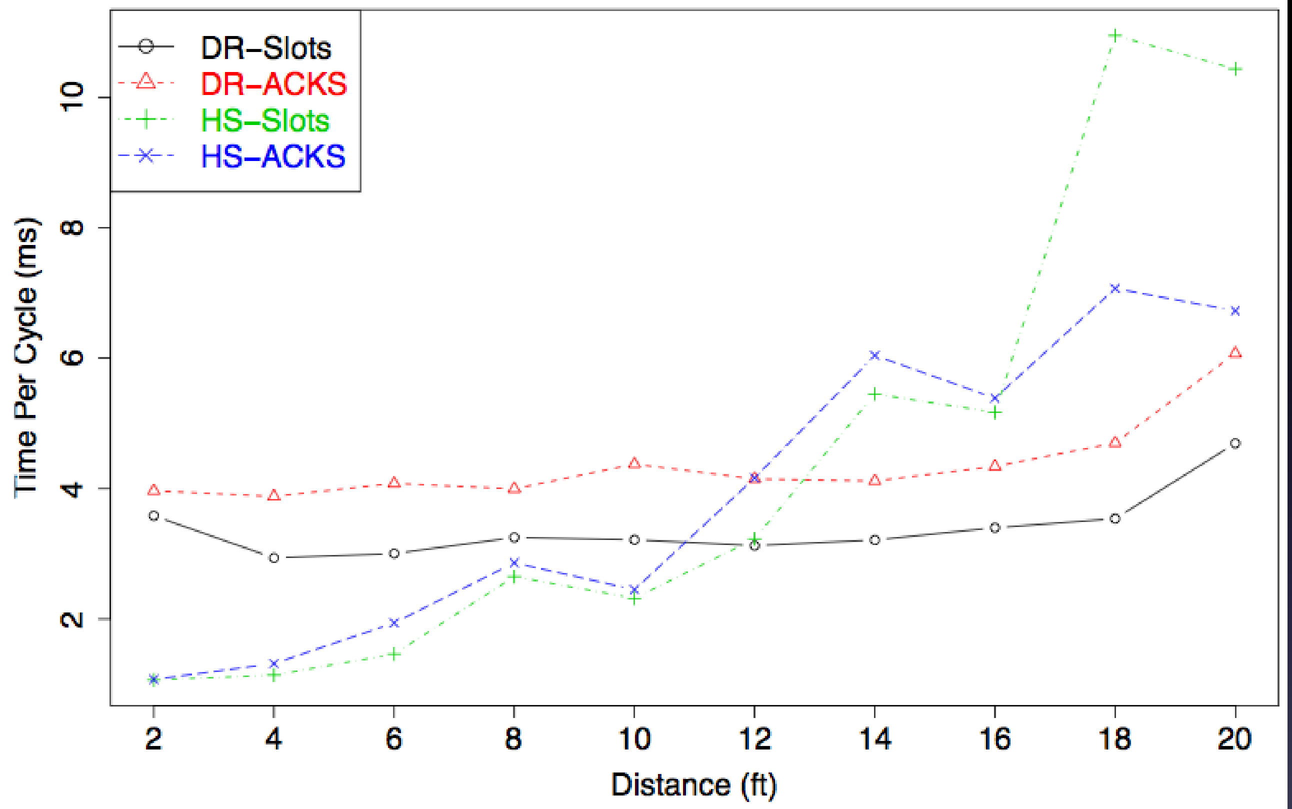


Figure 8: *ACK* and slot times per cycle

Number of Cycles

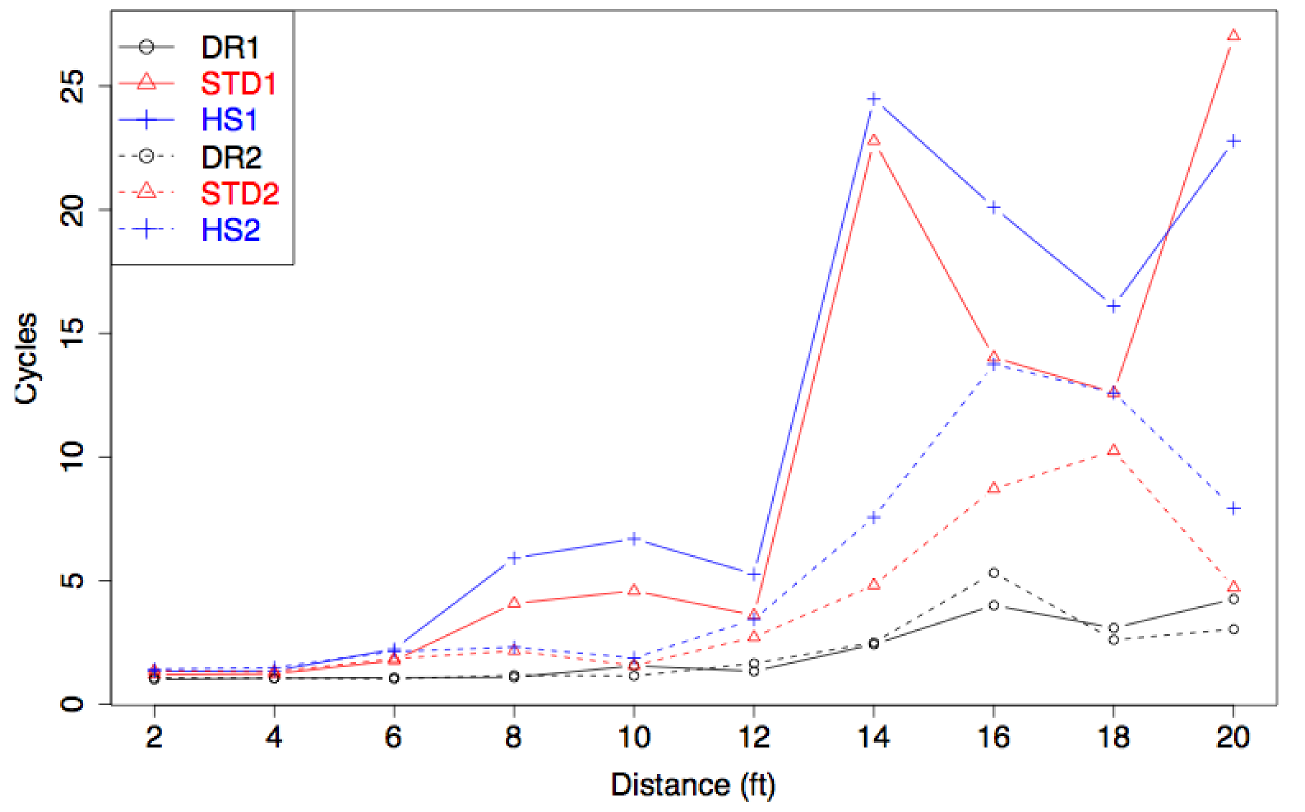


Figure 9: Number of cycles for different coding schemes

the average number of cycles needed to read all tags in the set

Hit Rate of DR Mode for Each Tag

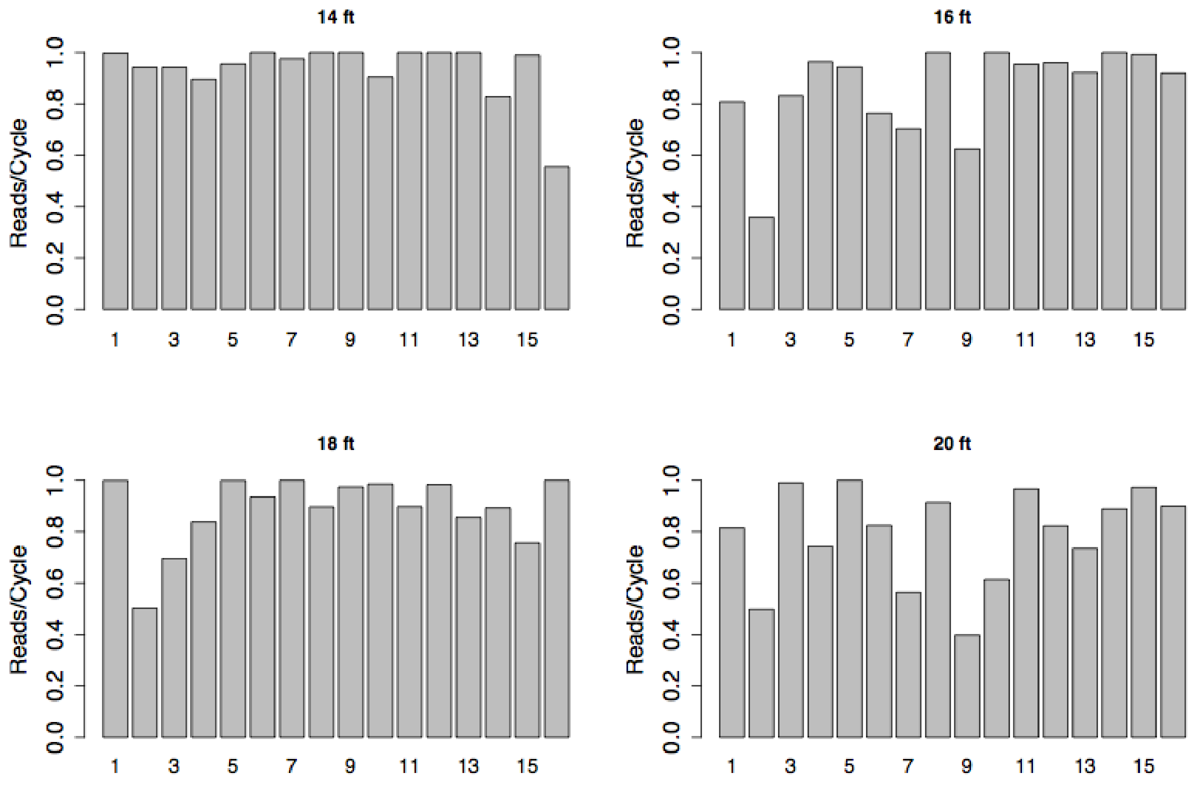


Figure 10: Hit rate for each tag using DR mode

Effects of Frequency Selective Fading

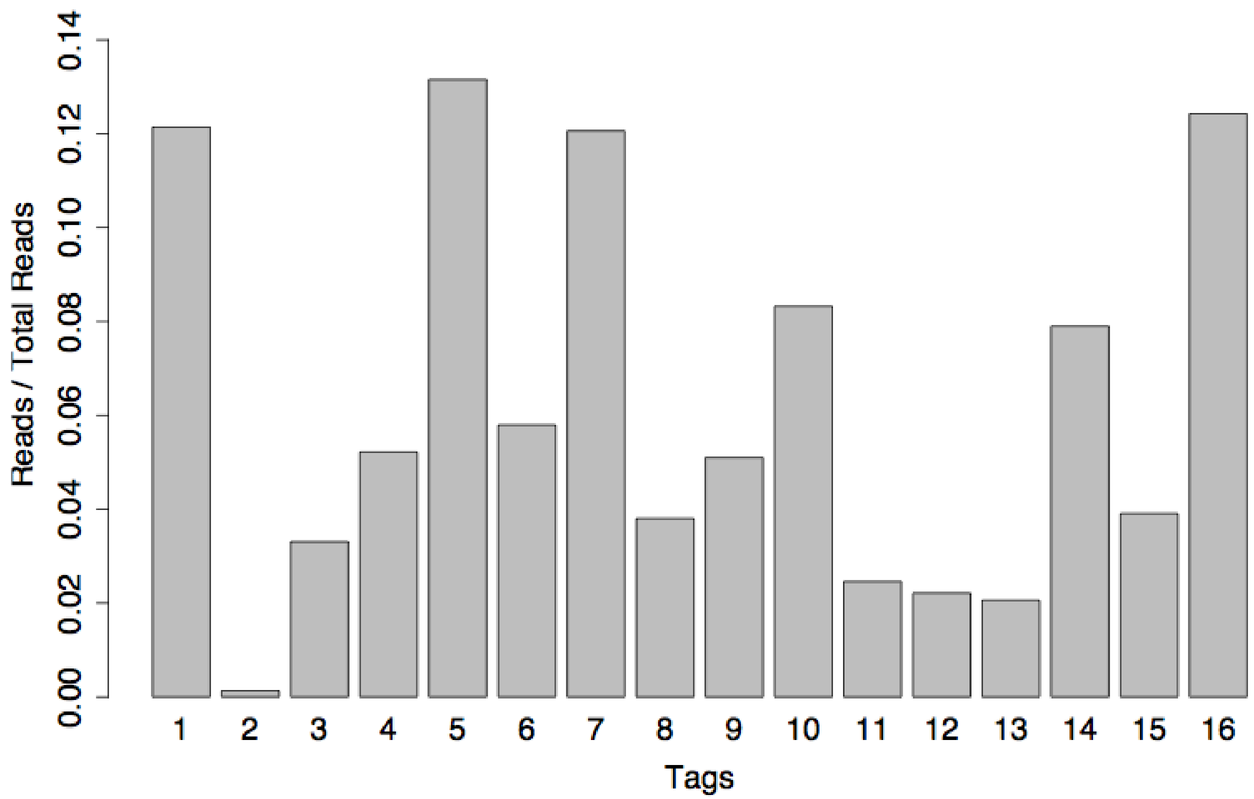


Figure 11: Hit rates for tags at 18 Feet

ThingMagic reader in the same location and setup as Experiment1.
15 minute experiment, in which each tag responds on all 50 channels at least once

Effects of Frequency Selective Fading
(conts.)

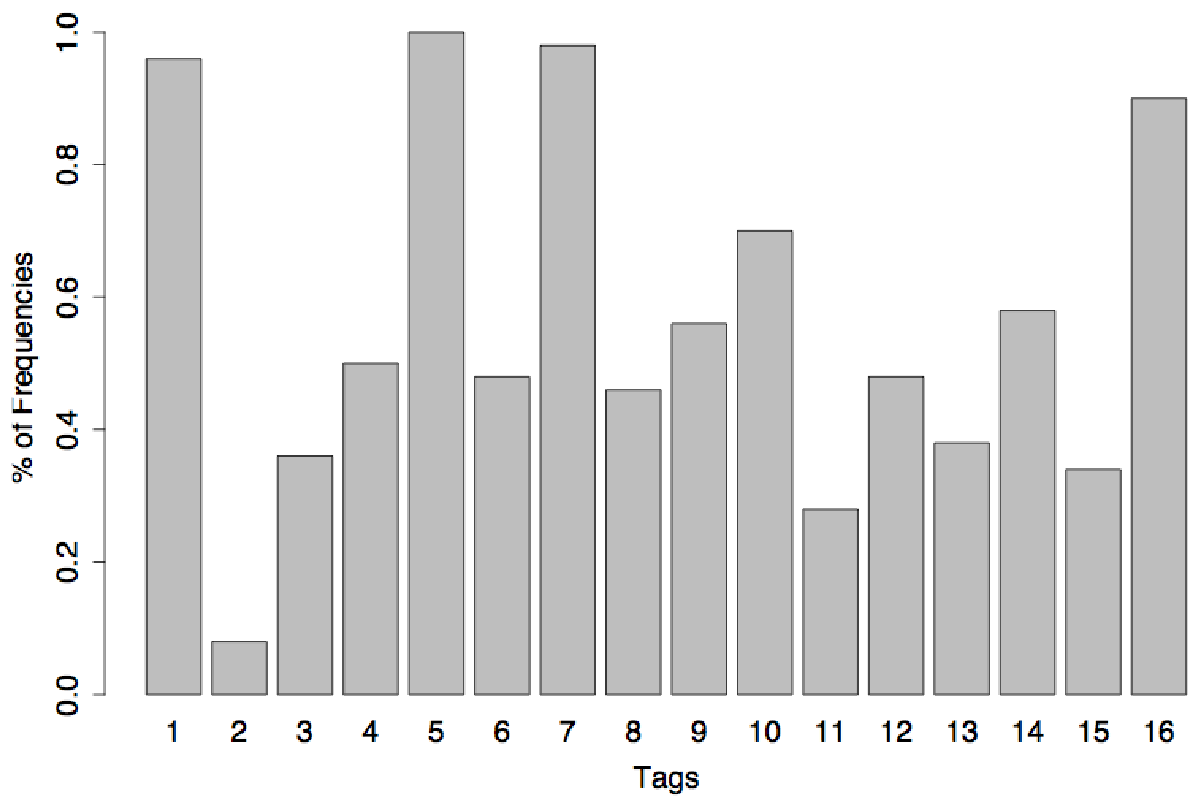


Figure 12: Frequency response of tags at 18 feet

Effects of Frequency Selective Fading (conts.)

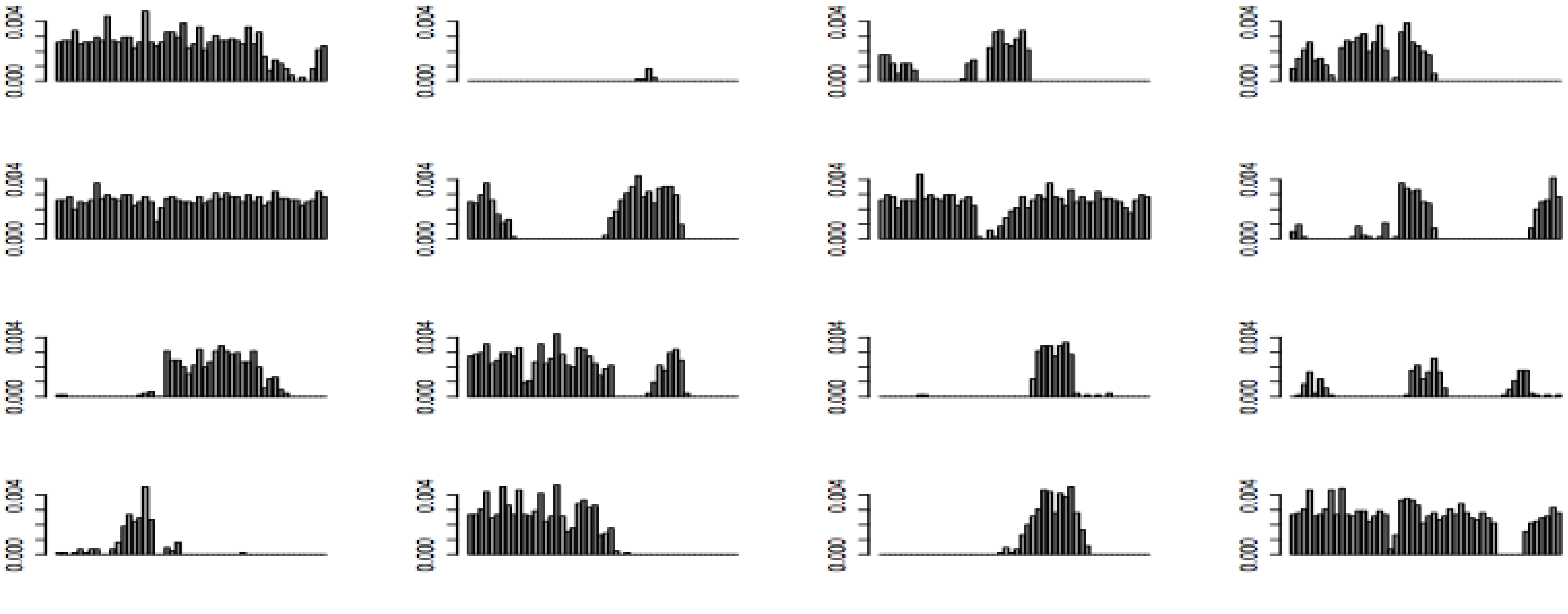


Figure 13: Frequency response of each tag at 18 feet

Summary

- Size of the tag set
  - affects performance, largely because larger tag sets are more efficient with respect to inter-cycle overhead.
- Up-link encoding
  - Slower but more robust up-link encodings are more effective at greater distances, as the overhead is quickly outweighed by reduced error rates.
- Multipath environment
  - Different multipath environments result in different error rates as distance increases, and these effects are location specific.
- Errors
  - increase both the variance and overall duration of cycles by increasing the number of ACKs and the number of slots.
  - also result in missed tags when a reader "gives up" during a cycle.

Summary (cont.)

- ACKs as well as Query and QueryRepeat commands
  - account for a significant amount of overall time
  - the ACKs because they are long and Query* because they are numerous.
- Lower down-link rate
  - result in fewer cycles needed to read the complete tag set, likely because more tags are able to power up.
- Frequency selective fading
  - is a dominant factor in missed reads, particularly at greater distances.

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Physical Layer

- Reducing Slot Times
  - As the Q algorithm results in many empty slots, having the reader truncate the listen time for empty slots would reduce overall cycle times.
- Reducing Missed Tags Due to Fading
  - The variation in frequency response can be smoothed by channel hopping at a more rapid rate.

Reducing Slot Times

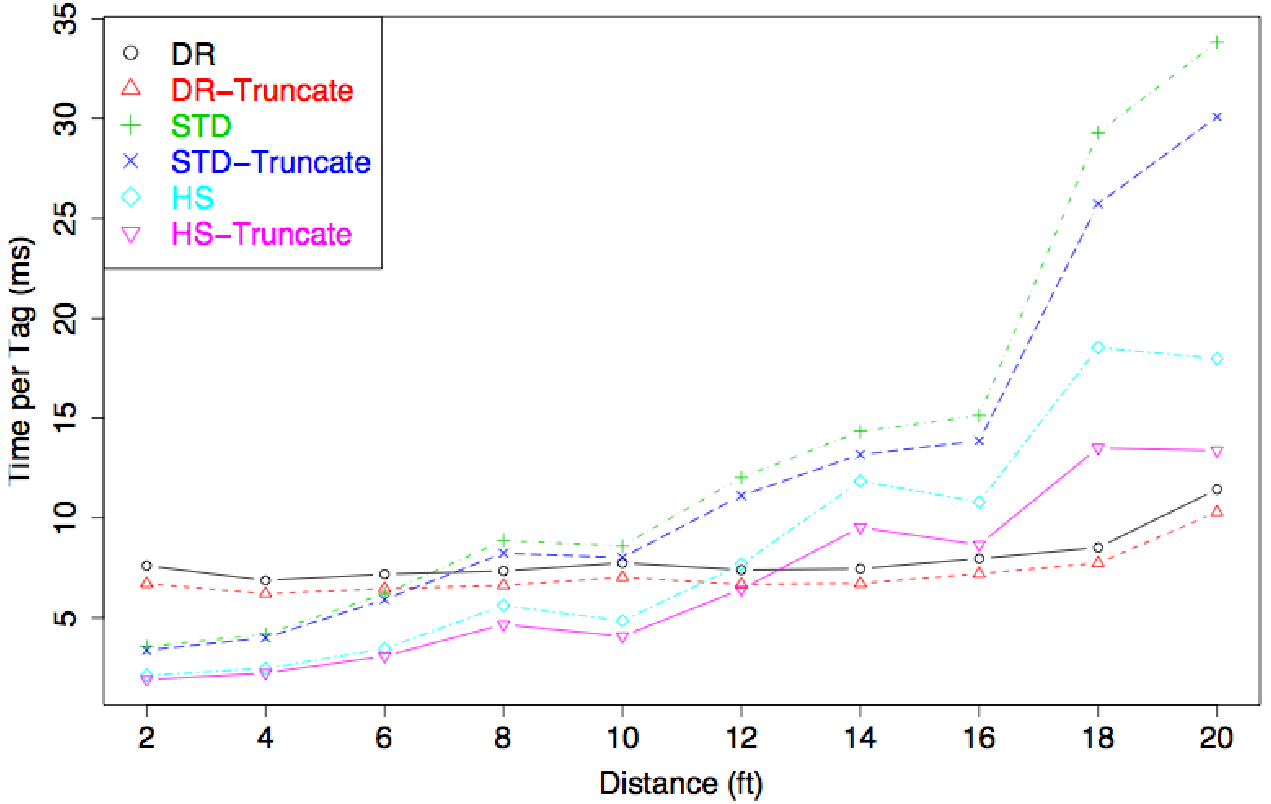


Figure 14: Read time with reduced listen period

Reducing Missed Tags Due to Fading

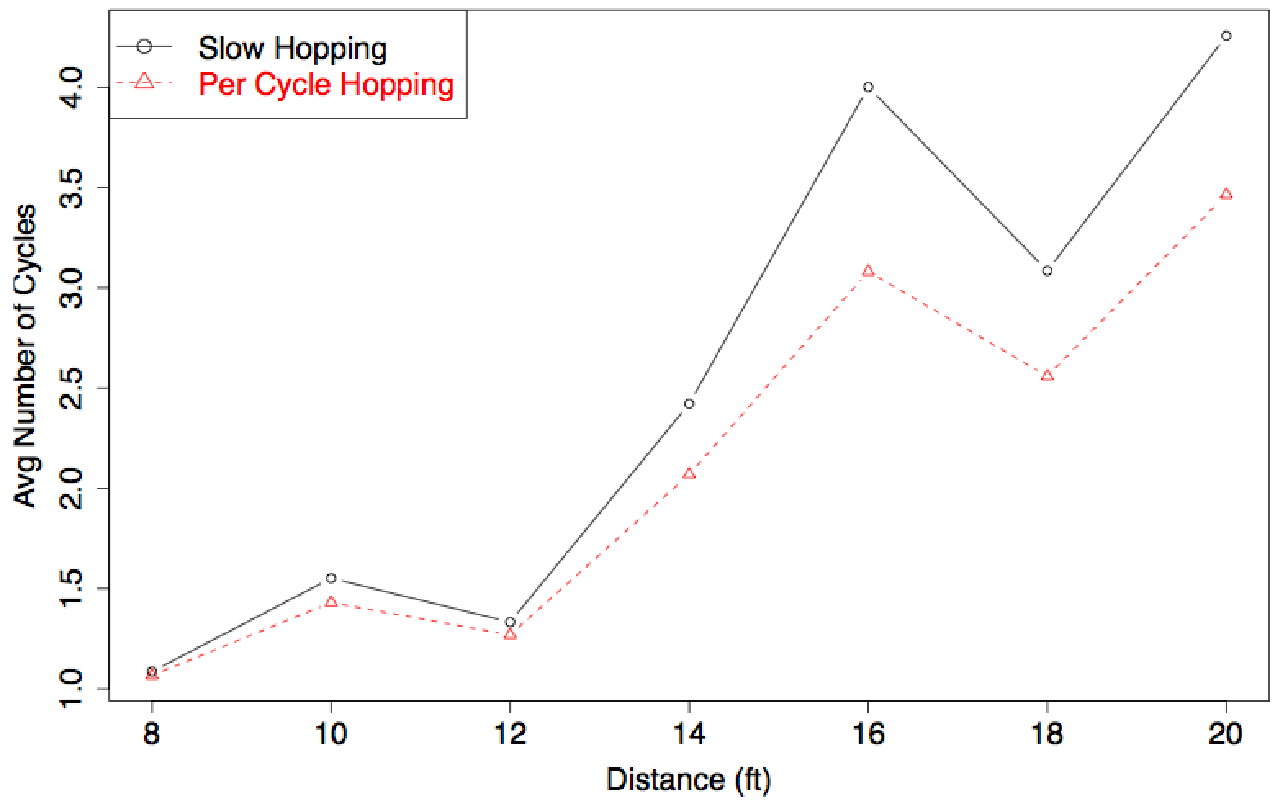


Figure 15: Effects of per cycle frequency hopping

Physical / MAC Layer Coordination

- Reducing ACKs
  - retrying ACKs even once is likely to have very little benefit when using these modes at larger distances
  - a more appropriate response would be to not waste time on retries, but instead change the physical layer parameters used in the next round
- Hybrid Reader Modes
  - combining the positive attributes of HS and DR mode has the potential to increase performance significantly

Reducing ACKs

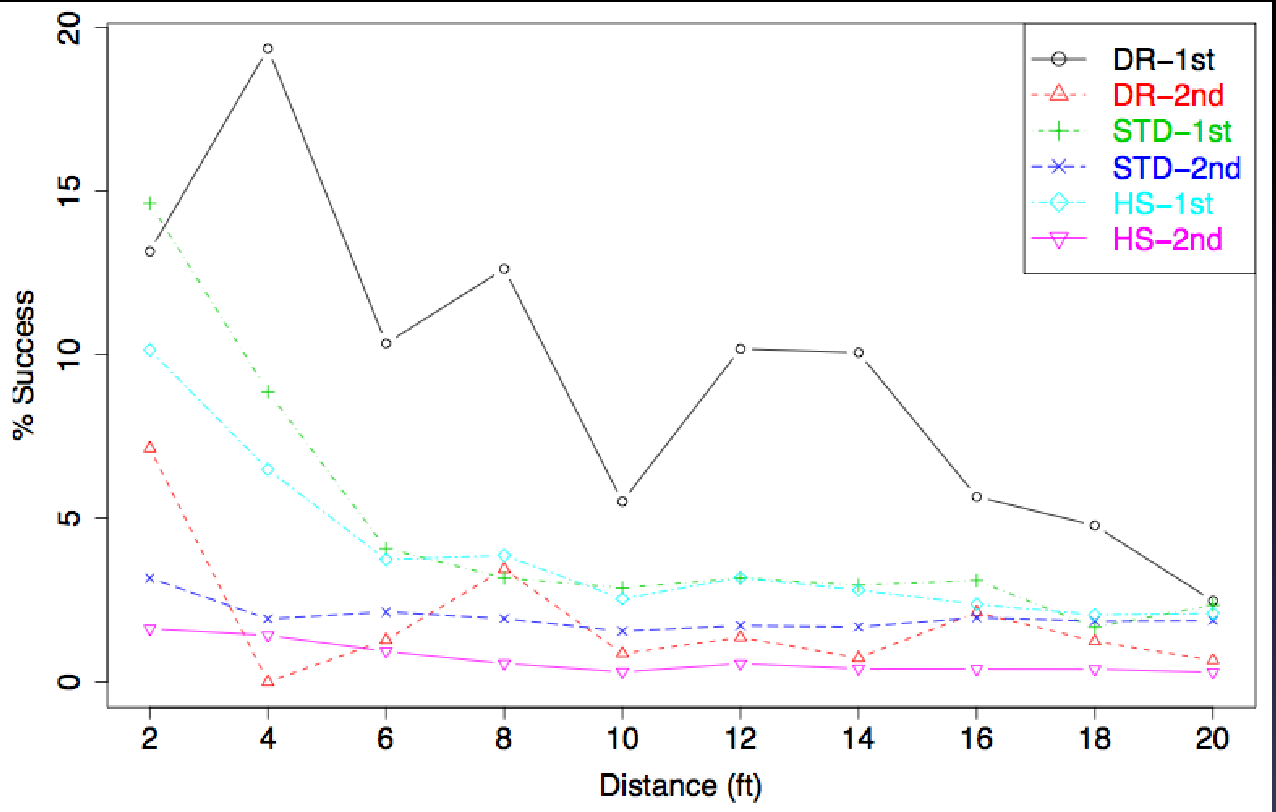


Figure 16: Chance of reading a tag on an ACK retry

Hybrid Reader Modes

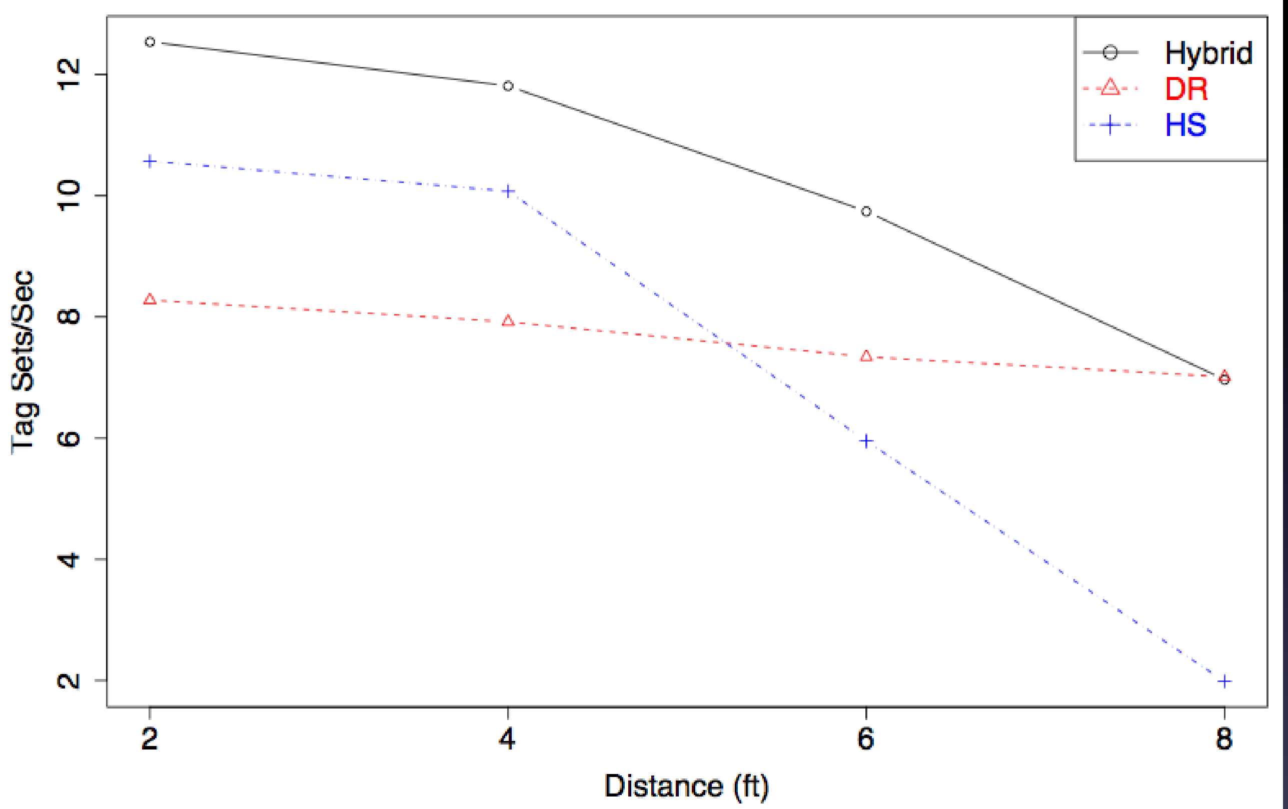


Figure 17: Effects of intra-cycle mode change

Overview

- Introduction
- Background Knowledge
- Methodology and Tools
- Experiment & Result
- Enhancement
- Conclusion

Conclusion

- First detailed, low-level measurement study of EPC C1G2 UHF reader technology in a real world setting.
- RFID physical and MAC layers should be considered in conjunction rather than separately as is done at present.
- Found physical layer effects are significant factors that degrade the overal(l) performance of commercial readers.
- Suggests that better physical layer implementation choices can improve performance while remaining standards compliant.
  - reducing the listen time for empty slots
  - increasing the rate of frequency hopping

Thanks

Q & A