



Securing Off-The-Shelf RFID systems

Project Presentation

by

Mehmet Arikkan

Ferit Erin

Ali Kumcu



Overview

- Overview of RFID systems
- Our solutions to problems addressed
 - Design
 - Implementation
- Test bed
- Sample runs
- Performance Graphs



RFID Systems

- **R**adio **F**requency **ID**entification Systems
- Readers, Tags, and host machines
- Will replace bar-codes in the future
- Little computational power
 - A few thousand gates
 - **No cryptographic functions available**

4/26/2004

CS 590D - RFID Security

3



Security and Privacy Concerns

- Tags should not compromise **privacy**
 - **Unauthorized Reader Detection Problem**
 - Avoid long-term tracking associations between tags and holders (KILL TAG)
 - Private tag contents must be protected by access control (Encryption)
- Eavesdropping, traffic analysis, spoofing, DoS are some of the attacks

4/26/2004

CS 590D - RFID Security

4



Our Proposals

- **Screaming Shelves** → Keep profiles of read tags, update profiles and determine if tags are present or not
 - Server does the profiling so that we can have multiple readers
 - Tolerant to physical anomalies
- **Unauthorized Readers** → Detect collisions, determine if this collision results from an authorized reader or not



SCREAMING SHELVES



Screaming Shelves

- Screaming Shelves → Client – Server architecture
 - Client reads the tags with “detect interval”, a.k.a delta
 - Client sends to server IDs of read tags
 - Server updates tag profiles and sends them back to client
 - Client renders the profiles on the screen and issues visual and audible warnings

4/26/2004

CS 590D – RFID Security

7



Tag Profile (relevant fields)

- **tagID** → unique 32-bit ID number of the tag represented as string
- **slidingWindowSize** → size of the sliding window array
- **slidingWindow** → array representing last N reads; 1 is for read, 0 for not-read
- **slidingWindowCount** → count of 1's in slidingWindow array
- **recentSuccessRatio** → $\text{slidingWindowCount} / \text{slidingWindowSize}$
- **warningThreshold** → threshold to issue a warning

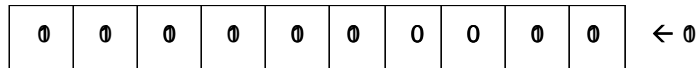
4/26/2004

CS 590D – RFID Security

8

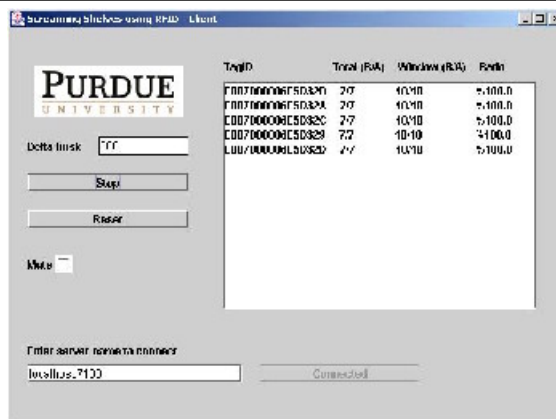
Sliding Window

- Data structure to keep track of the status of the latest N read attempts



Count: 3
 Last read: 0
 Window shifted left

Screaming Shelves – Tags present



- All tags are present.
- Client reads them successfully.

SS Demo – Tags missing

TagID	Total (RA)	Window (RW)	Ratio
E007000006F032E	1678	1070	638.0
F007000006F032A	1176	670	569.0
E007000006F032C	1678	1070	638.0
F007000006F032B	1678	1070	638.0
E007000006F032D	778	470	604.0

- Some tags are removed.
- Alarm is raised.

4/26/2004

CS 590D – RFID Security

11

UNAUTHORIZED READERS

4/26/2004

CS 590D – RFID Security

12



Unauthorized Readers - Refresher

- In the current scheme, there is no authentication between the reader and the tags
- ANY reader could read ANY tags!
- This brings up privacy implications
- How do you detect an unauthorized reader?

4/26/2004

CS 590D - RFID Security

13



Unauthorized Readers cont'd

- Since there is no authentication, we cannot know which reader is trying to read which tag
- Our approach is to use the Reader Collision problem for our purpose
- A reader is able to detect a collision with another reader

4/26/2004

CS 590D - RFID Security

14



Reader Collision

- Two or more readers that are trying to read the same tag
- There is a probability that no reader will succeed (analogous to Ethernet Collision)
- It is a different problem than tag-to-tag collision:
 - Reader collision: many readers – one tag
 - Tag-to-Tag collision: one reader – many tags
- Tag-to-Tag collision is handled by the anti-collision protocols in the standard

4/26/2004

CS 590D – RFID Security

15



Our Approach

- We have *detector* readers that continuously scan for tags in their coverage area
- The backend server keeps track of the “profile” of the tags
- If an unauthorized reader tries to read a tag in the coverage area, it will cause a collision with the *detector*.
- This collision is registered in the backend server and a warning is issued.

4/26/2004

CS 590D – RFID Security

16



Our Approach cont'd

- What if an *authorized* reader tries to read the tags in the coverage area?
- In that case the backend server will register two collisions, one from the *detector* and another one from the *authorized* reader.
- The backend server will silence the *detector* for a split second to give the *authorized* reader a chance to complete operation.
- The *detector* is turned on immediately after *authorized* reader completes its request.

4/26/2004

CS 590D - RFID Security

17



Unauthorized Readers

- There are 3 clients serving our purpose
- **Detector client** → Tries to read the tags, and detects a reader collision
- **Authorized reader** → Reads the tags and records the time stamp for last read attempt
- **Unauthorized reader** → Persistently tries to read the tags, but don't record anything on the server

4/26/2004

CS 590D - RFID Security

18

Server

- For every tag, if it becomes "missing" (i.e. in the sliding window), checks for authorized reader condition

- **Condition**

If $(t_{curr} - t_{last}) > (1 - W_{thres}) * SWS * T_{interval}$

Then

there exists an *Unauthorized Reader*

t_{curr} : current time

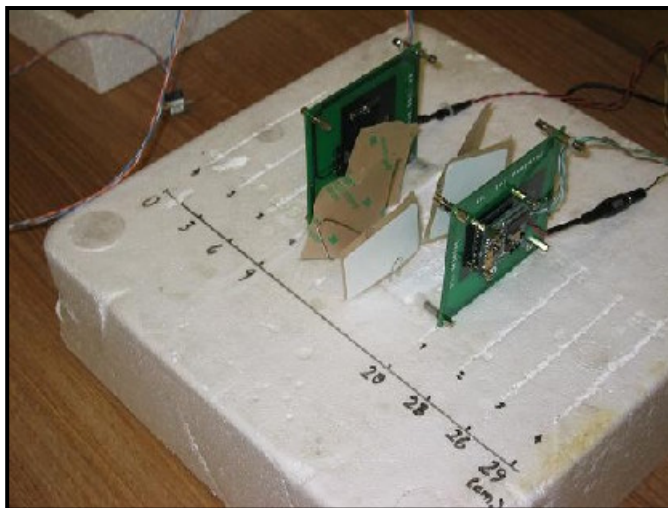
t_{last} : last time stamp

W_{thres} : warning threshold

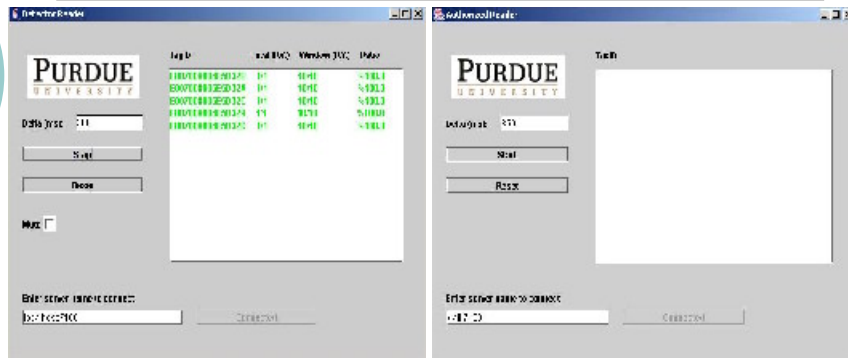
SWS : sliding window size

$T_{interval}$: detect interval

Test bed using SkyeTek Reader and TI tags



Authorized Reader – Startup



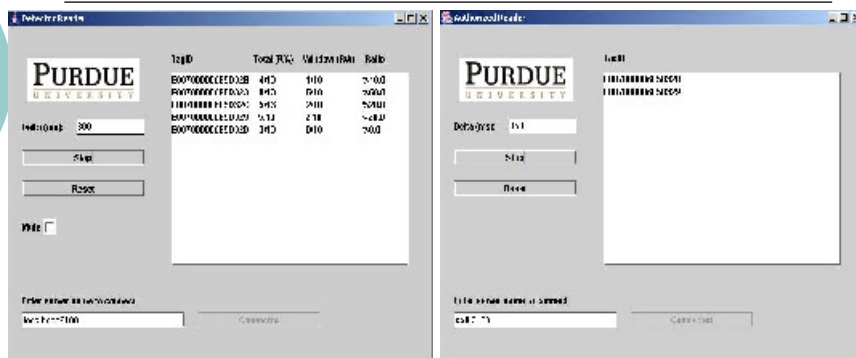
- Detector started.
- Authorized Reader is not started yet.
- Detector successfully reads tags.

4/26/2004

CS 590D – RFID Security

21

Authorized Reader – Detector & Reader



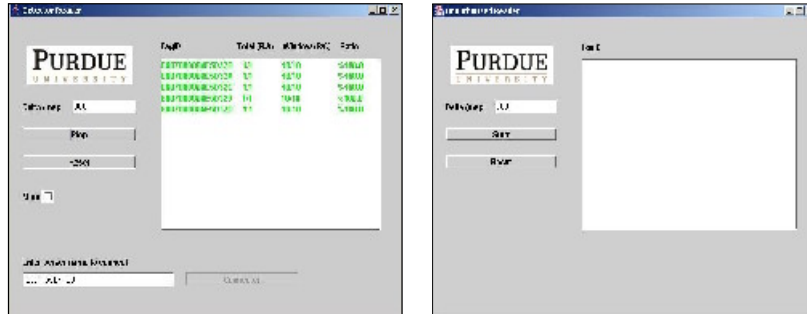
- Authorized Reader started, but cannot read all of the tags.
- Detector's success ratio decreases.

4/26/2004

CS 590D – RFID Security

22

Unauthorized Reader - Startup



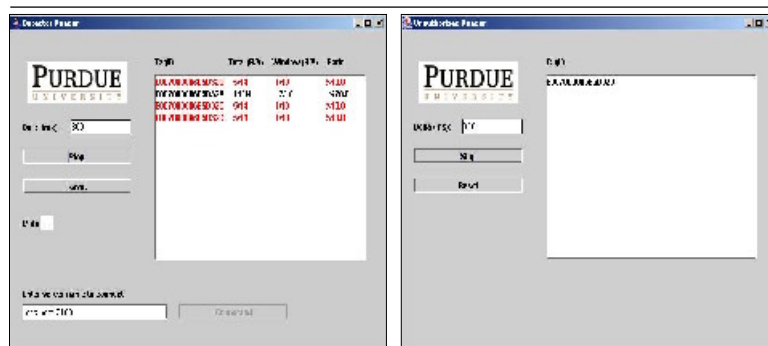
- Detector successfully reads.
- Unauthorized reader not started.

4/26/2004

CS 590D – RFID Security

25

Unauthorized Reader (cont'd.)



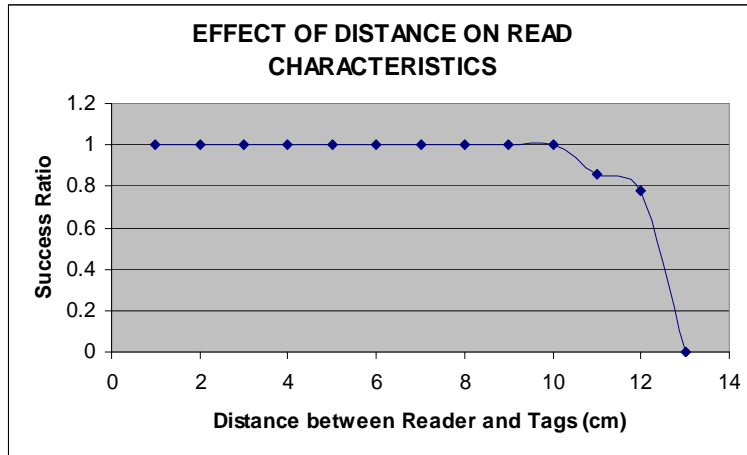
- Unauthorized Reader Started.
- Collision causes detector to fail reading some tags
- Detector understands there is no authorized reader, does not pause and issue a WARNING
- Unauthorized Reader unable to read all the tags

4/26/2004

CS 590D – RFID Security

26

Performance Graphs - 1

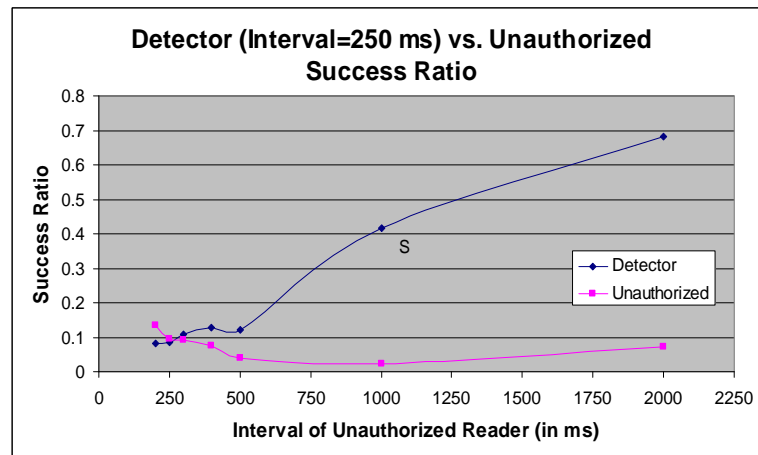


4/26/2004

CS 590D - RFID Security

27

Performance Graphs - 2

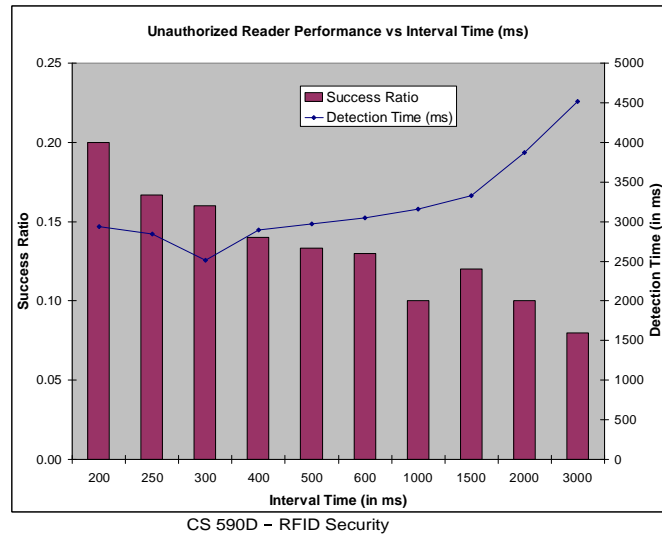


4/26/2004

CS 590D - RFID Security

28

Performance Graphs - 3



4/26/2004

29

Thank You

- Question or Comments welcome!
- You can reach us at

rfid@cs.purdue.edu

4/26/2004

CS 590D - RFID Security

30