COMP Annul Research Day (CARD) 2012

Fast Cloned-Tag Identification Protocols for Large-Scale RFID Systems

@IEEE/ACM IWQoS’12

Kai Bu, Xuan Liu, and Bin Xiao

Department of Computing

The Hong Kong Polytechnic University

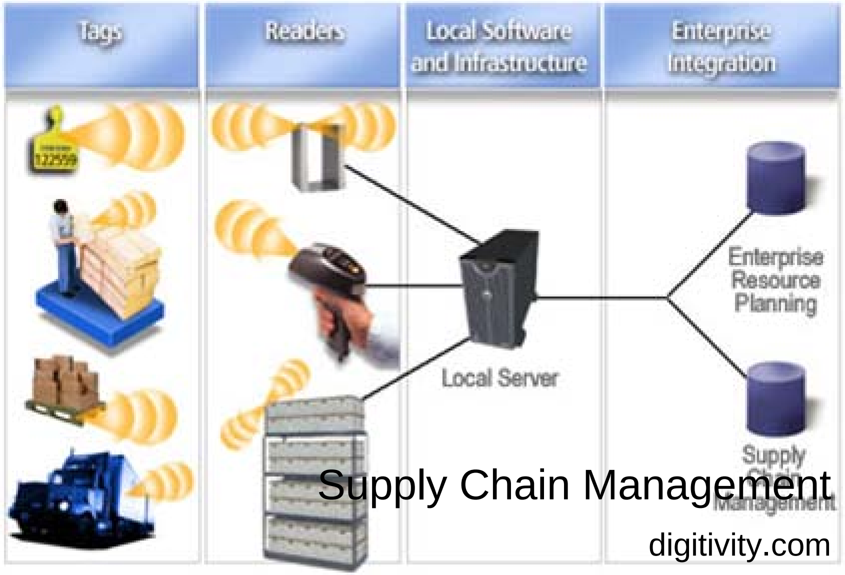
Content

- RFID Cloning Attacks
- Existing Solutions and Limitations
- BID
- S-BID
- ES-BID
- Preliminary Results
- Conclusion

RFID Getting More and More Popular

- RFID: Radio-Frequency Identification
- RFID systems

  back-end server + reader(s) + tags
- RFID applications



Supply Chain Management

digitivity.com

Baby Tracking for Healthcare

gaorfidassettracking.com

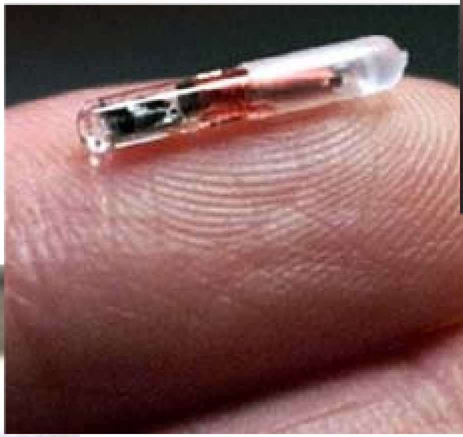
RFID’s Pros and Cons [cont.]

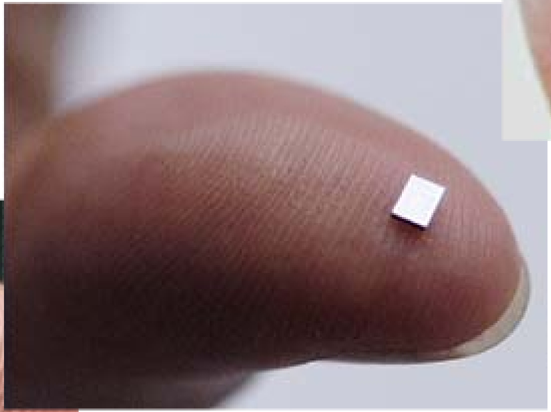
- Pros

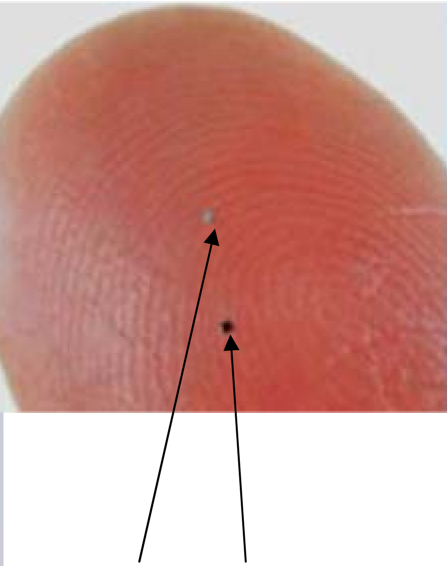
  small size

  low cost

  …







0.4×0.4 mm

RFID powder

RFID’s Pros and Cons

- Cons

  broadcast communication is vulnerable to a range of malevolent attacks (e.g., overhearing, replay, cloning…);

  hardware constraints limit the application of too sophisticated security strategies (e.g., cryptography…)

- ***The Cloning Attack***

RFID Cloning Attacks

- Cloning attacks

  the attacker compromises tags and produces their replicas *(cloned tags)*
- Cannot simply authenticate cloned tags as they clone all valid information such as ID, key…
- Significant financial losses to commercial RFID applications

  e.g., $200 billion counterfeit products in 2005

How to deal with cloning attacks in RFID systems?

Existing Solutions: Prevention

- Prevention

  uses techniques such as cryptography and encryption to make tags hard to compromise
- Limitation

  cannot be supported by most off-the-shelf low-cost tags due to hardware constraints

No prevention protocols claim to completely overcome cloning attacks!

Existing Solutions: Identification

- Identification

  Identifies cloned tags, rather than prevents cloning attacks

- Trace-based identification

  uses *tag traces* that consist of rag related data (e.g., ID, ownership, and *location*) distributed among the supply chain partners.

- Limitation

  partners are reluctant to share tag traces *due to business concerns*;

  tag traces may not even exist *before tags are transported/distributed.*

Cloned-Tag Identification **without tag traces**?

Innovative yet Practical Applications

- Identify cloned tags
  before injecting tagged objects
  into supply chains

hariri91.posterous.com

- Identify cloned tags
  for scenarios using
  RFID-enabled card scanning
  systems

Prior Art and Limitations

- Prior Art: SYNC [1]

  the reader reads (then writes) a random key to a tag per read operation;

  identifies a cloned tag if ID and Key mismatch.

- Limitations

  time-consuming transmission of tag IDs;

  privacy leakage in privacy-sensitive applications.

[1] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," *Pervasive Computing*, vol. 5538, pp. 291-308, 2009.

A suite of protocols to be proposed…

Problem Formulation

- System

server: registration of tags info (e.g., ID, key…);
communicates with readers;
reader: communicates with server;
communicates with tags;

“Reader”

tags: communicates with readers;
attacker: launches cloning attacks.

- Assumptions

error-free channel;

normal responses: cloned tags do not emit extra responses or always keep silent.

- Formulation

to identify all the IDs of cloned tags (if any) as fast as possible.

BID

- Idea

  the reader broadcasts tag IDs one after another;

  identifies cloned tags exist if multiple responses received – ***collision*** *occurs when multiple responses*
- Up to 30% time reduction over SYNC
- Limitation: similar to SYNC's

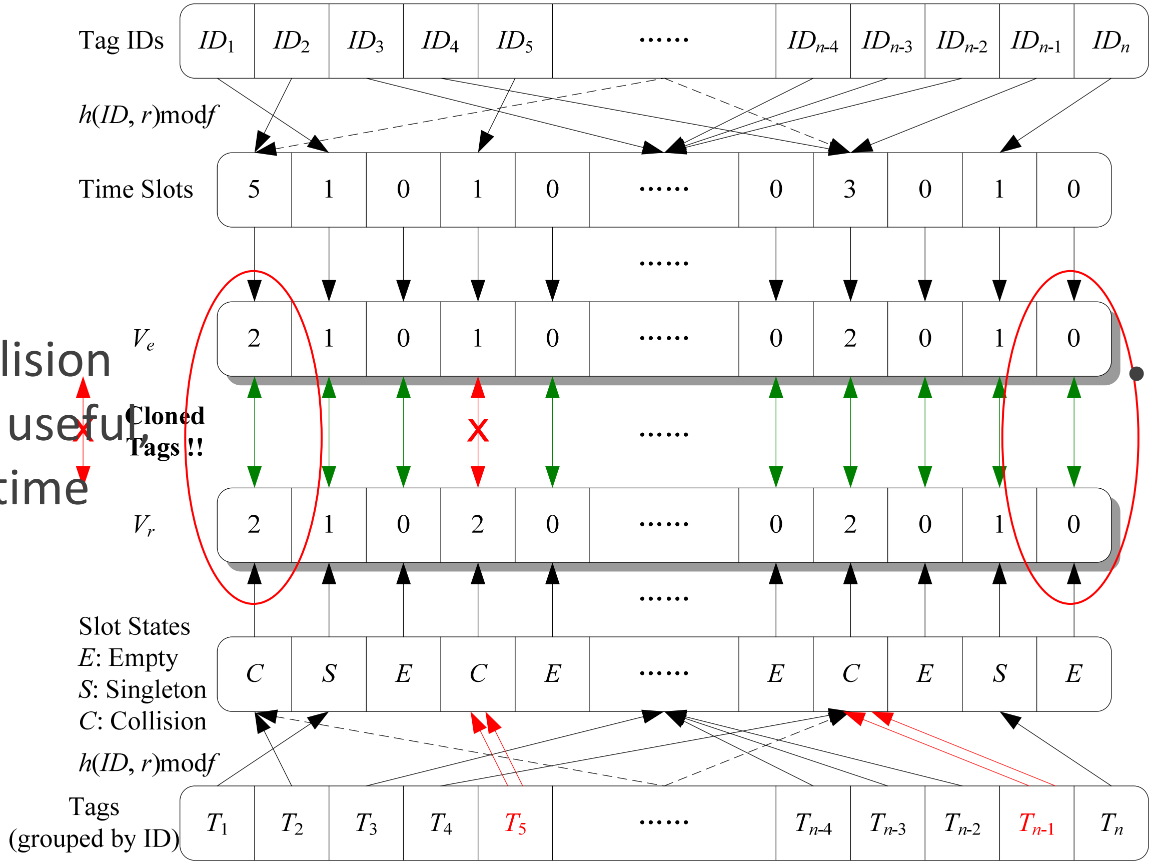
  ID transmission is time-consuming: *time inefficiency*

  ID transmission leaks sensitive information for some applications: *privacy leakage*

Without the transmission of tag IDs?

S-BID

Adopt slotted Aloha



- Expected collision slots are not useful, but wasting time

- Empty slots are not useful, but wasting time

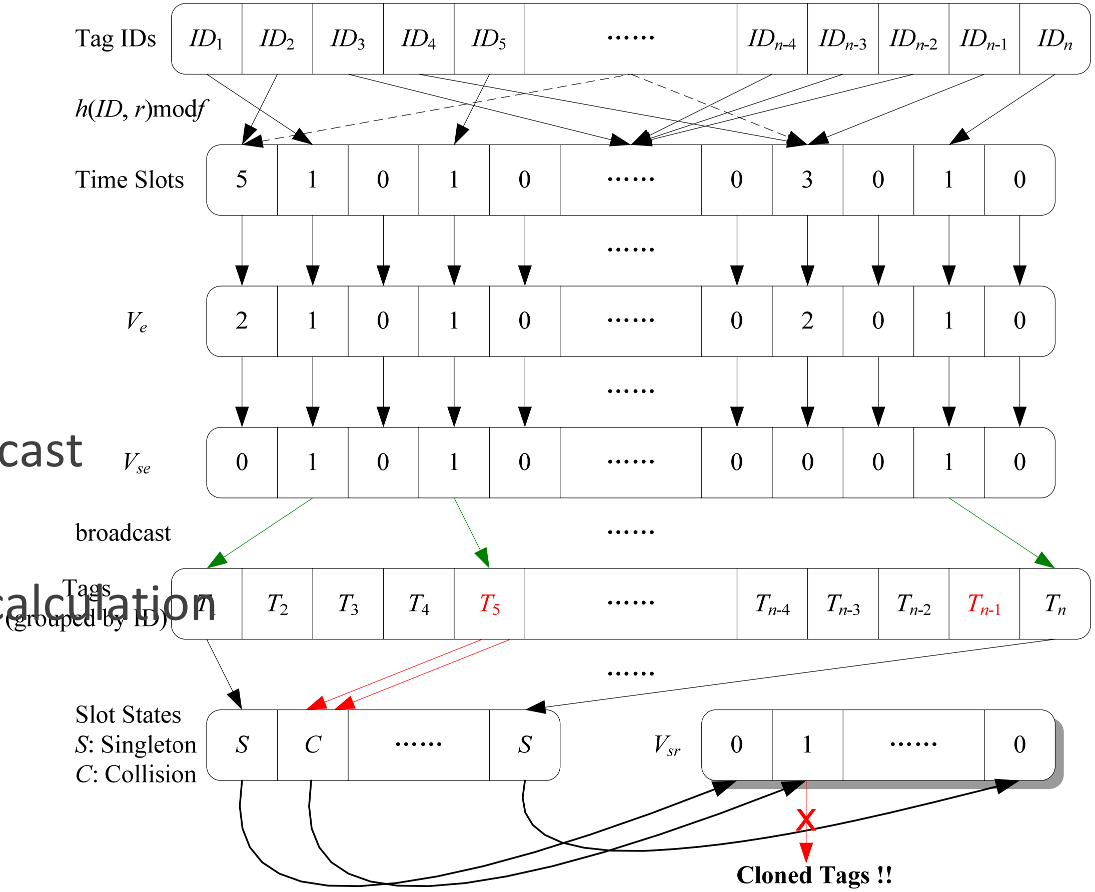
- Cloned-tag identification by S-BID. T_i denotes a set of tags (a genuine tag and cloned peers if any) with ID_i. Dashed arrow-shaped lines indicate that one or more IDs or tags are hashed to a time slot.

- Up to 70% time reduction over BID.

To bypass time slots that are
not expected to be singleton?

ES-BID

- Vector broadcast
- Slot index recalculation



Tag IDs | ID_1 | ID_2 | ID_3 | ID_4 | ID_5 | …… | ID_{n-4} | ID_{n-3} | ID_{n-2} | ID_{n-1} | ID_n

$h(ID, r)\bmod f$

Time Slots | 5 | 1 | 0 | 1 | 0 | …… | 0 | 3 | 0 | 1 | 0

V_e | 2 | 1 | 0 | 1 | 0 | …… | 0 | 2 | 0 | 1 | 0

V_{se} | 0 | 1 | 0 | 1 | 0 | …… | 0 | 0 | 0 | 1 | 0

broadcast

Tags (grouped by ID) | T_1 | T_2 | T_3 | T_4 | T_5 | …… | T_{n-4} | T_{n-3} | T_{n-2} | T_{n-1} | T_n

Slot States | *S* | *C* | …… | *S*

S: Singleton

C: Collision

V_{sr} | 0 | 1 | …… | 0

X

Cloned Tags !!

- Cloned-tag identification by ES-BID. ES-BID identifies a cloned tag/ID once any $V_{sr}[i]$=1 (e.g., $V_{sr}[1]$ as illustrated).
- Up to 60% time reduction over S-BID.

Preliminary Results

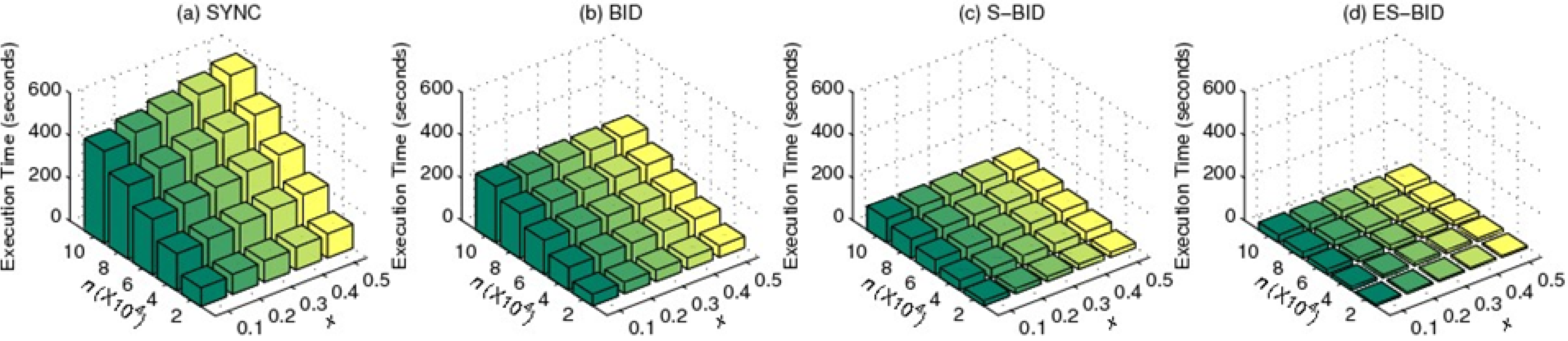


Fig. 1. Execution time comparison of SYNC, BID, S-BID, and ES-BID with varying number of tag IDs n and varying compromised tag ratio x.

- **ES-BID averagely yields up to 91% time reduction over SYNC.**

Conclusion and Future Work

- Identify cloned tags, for example, before injecting tagged objects into supply chains
- Leverage the broadcast and collision
- Propose time-efficient and privacy-preserving protocols
- Future work:

  Adapt the proposed protocols to applications with tagged objects distributed across multiple places

Q&A

Thanks