MASS 2014

Toward Fast and Deterministic **Clone Detection** for Large **Anonymous RFID** Systems

Kai Bu, Mingjie Xu, Zhejiang University
Xuan Liu, HK PolyU; Jiaqing Luo, UESTC; Shigeng Zhang, CSU

Anonymous RFID

unknown tag identifiers (IDs)

Anonymous RFID Clone Tag Detection

unknown tag identifiers (IDs)

any clone tags?

Cloning Attack

Cloning Attack

Compromise tags & Produce Replicas/Clones;

Clone tags = Genuine tags.


Delphi 7
Delphi 7
Delphi 7


VISA


1회용
지하철·전철 전용
1회용 교통카드
Single journey ticket


PASSPORT


Any Clones?
Delphi 7
1회용
지하철·전철 전용
1회용 교통카드
Single journey ticket
PASSPORT

Solution Goals

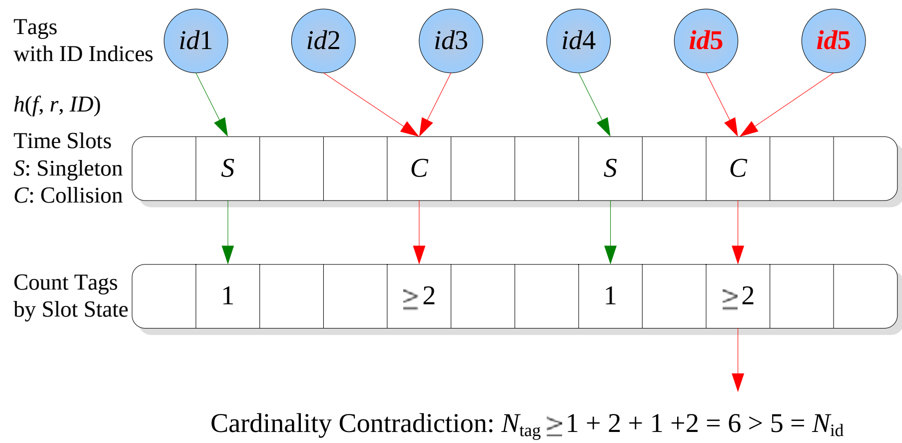
- Anonymity Preservation
- Deterministic Detection
- Fast Detection

Design Choices

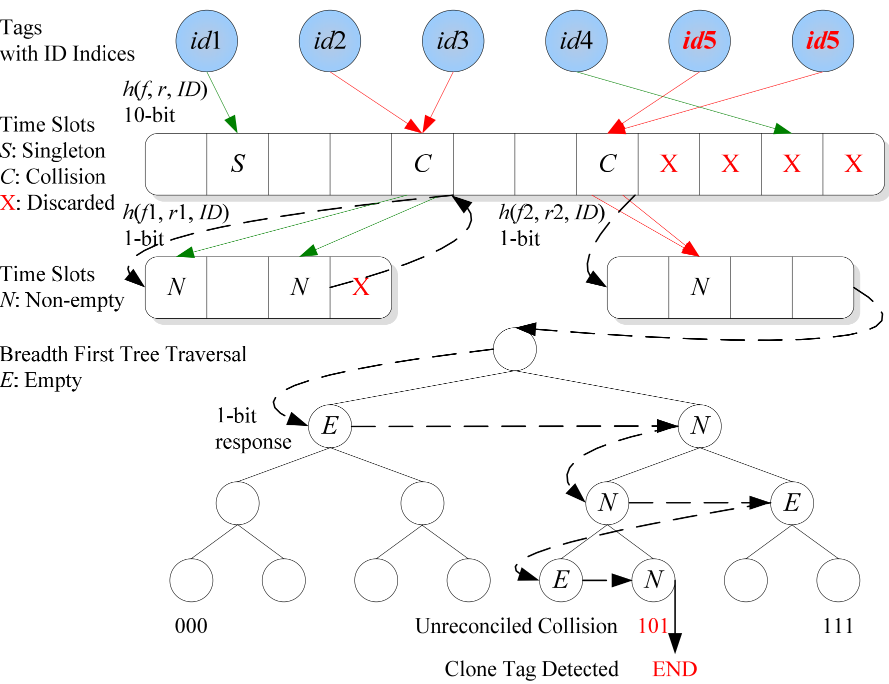
- Anonymity Preservation
  isolate ID from protocol design
- Deterministic Detection
  verify the existence of clones
- Fast Detection
  minimize time and comm. cost

Fast & Deterministic Protocols

BASE



DeClone

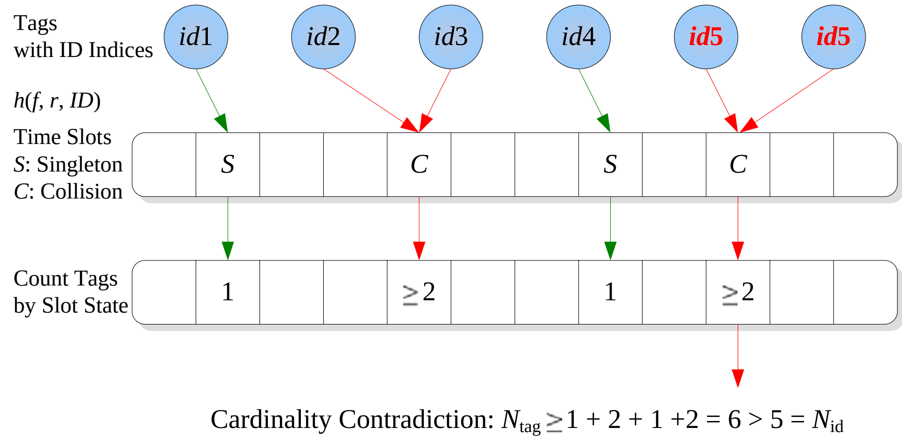


Anonymous RFID Clone Detection

Fast & Deterministic Protocols

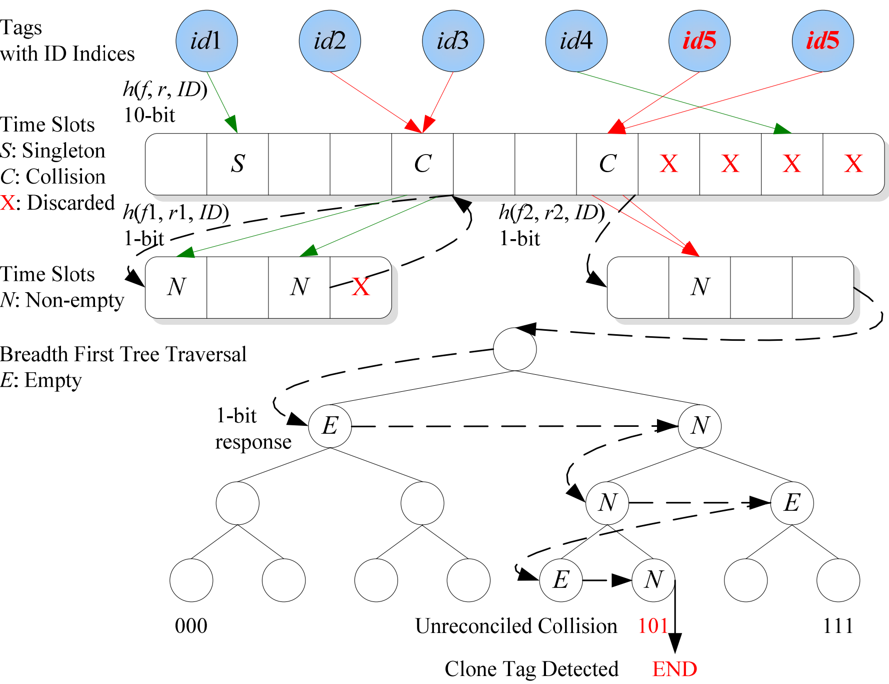
BASE

using cardinality contradiction



DeClone

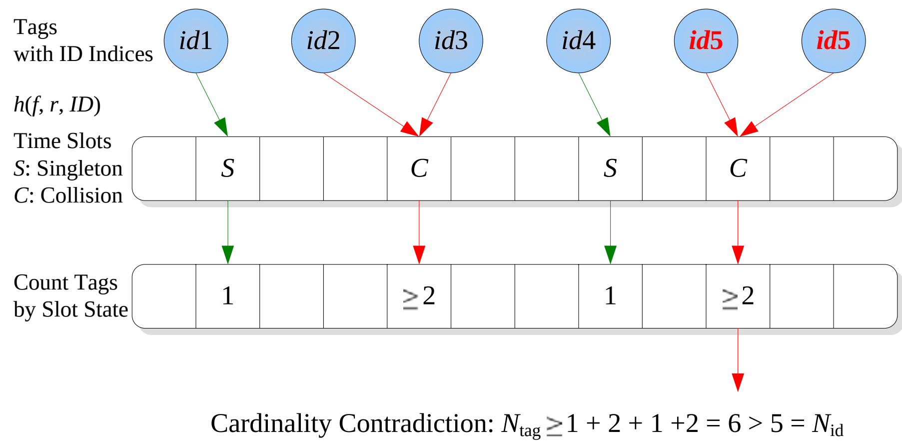
using unreconciled collision



Fast & Deterministic Protocols

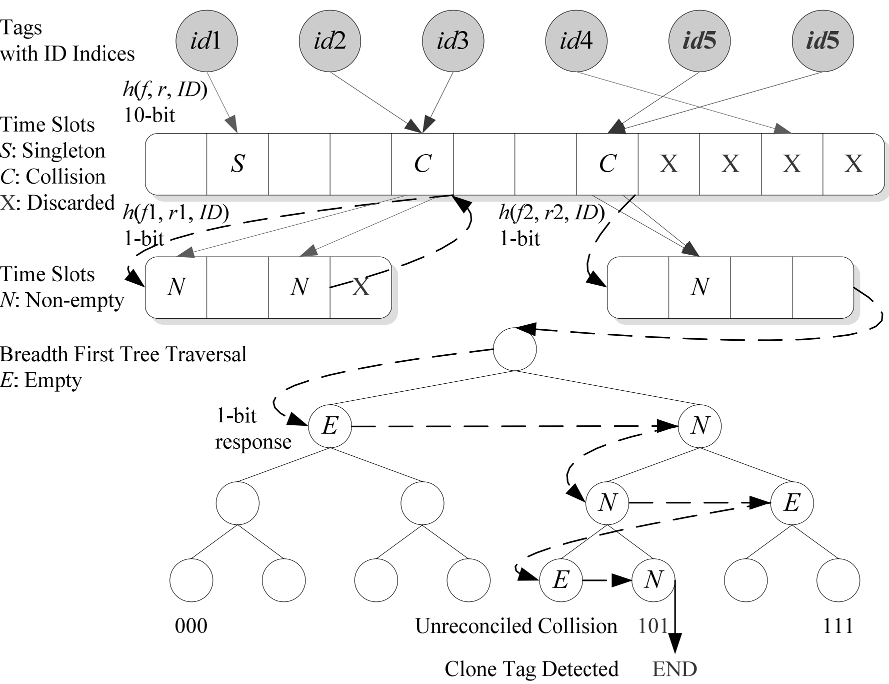
BASE

using cardinality contradiction



DeClone

using unreconciled collision



BASE

- Motivation

  clone tags make

  tag cardinality > ID cardinality

BASE

- Motivation

  clone tags make

  tag cardinality > ID cardinality

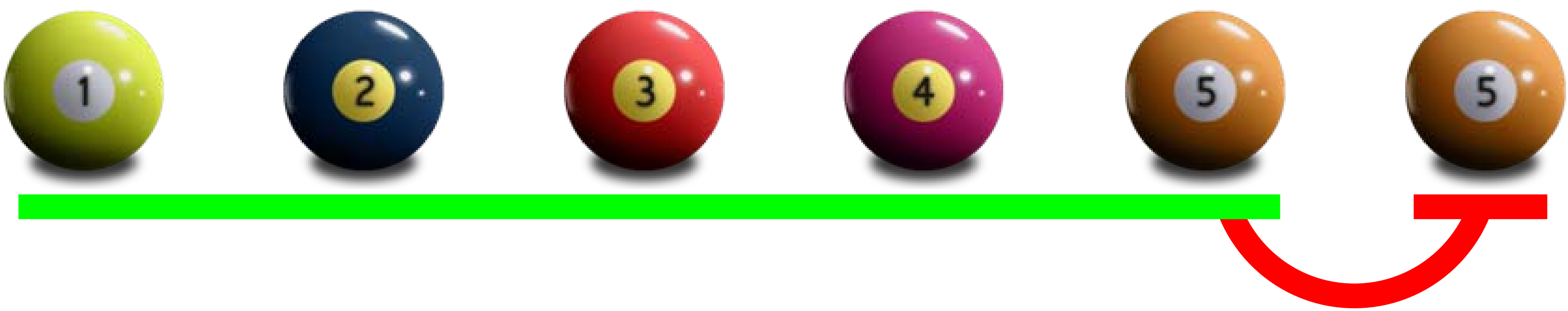
$$N_{\mathrm{id}} = 5$$

BASE

- Motivation

  clone tags make

  tag cardinality > ID cardinality

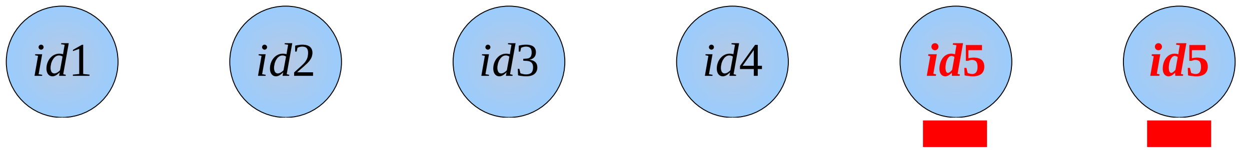


$$N_{\mathrm{id}} = 5 \longrightarrow {\color{red} N_{\mathrm{tag}} = 6}$$

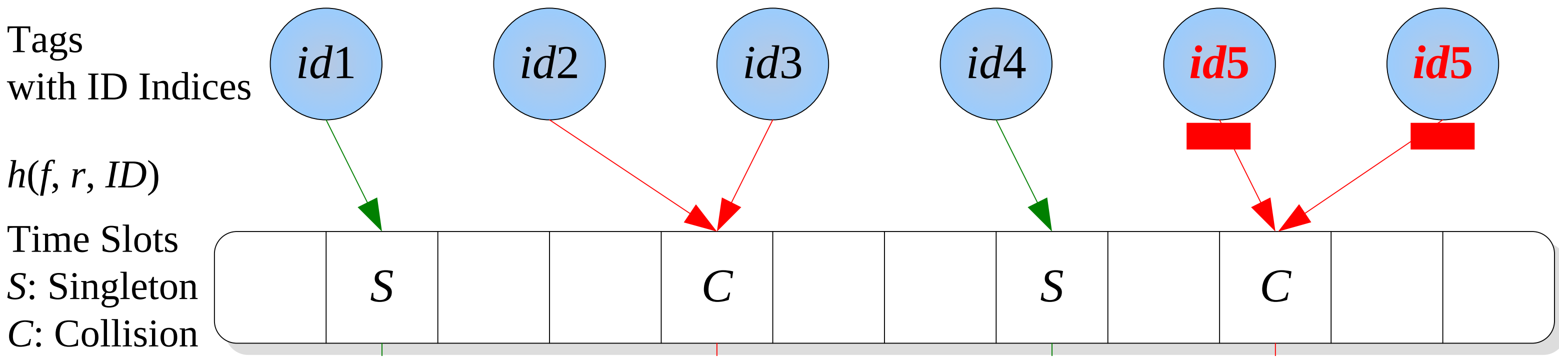
cardinality contradiction

BASE

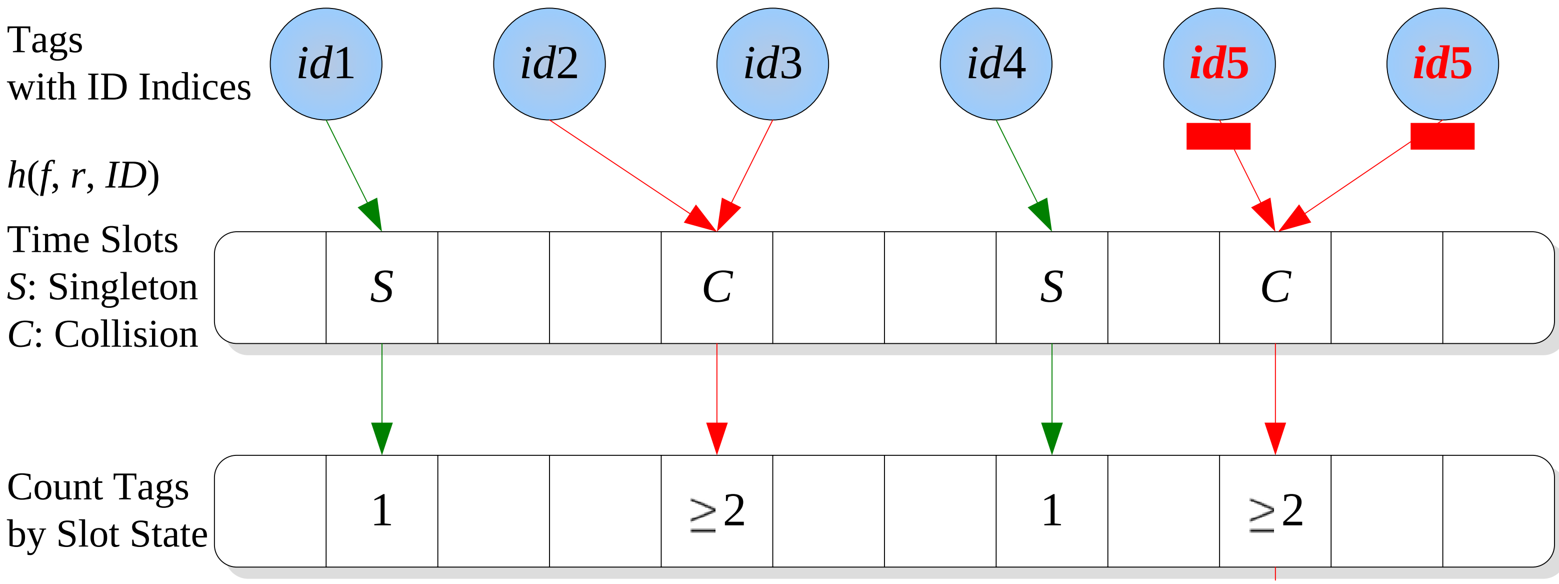
Tags
with ID Indices



BASE

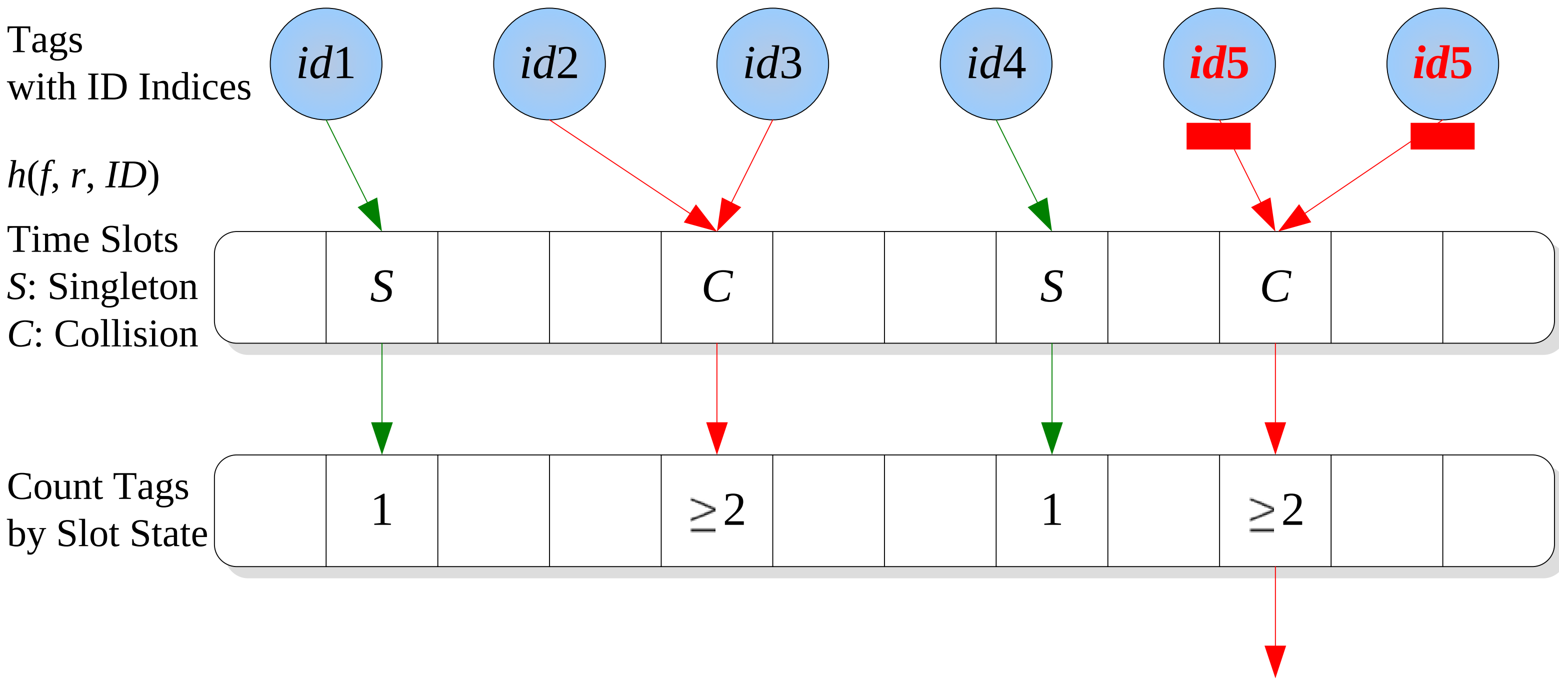

Tags
with ID Indices
*id*1
*id*2
*id*3
*id*4
*id*5
*id*5
h(*f*, *r*, *ID*)
Time Slots
S: Singleton
C: Collision
S
C
S
C

BASE



Tags
with ID Indices
id1
id2
id3
id4
id5
id5
h(f, r, ID)
Time Slots
S: Singleton
C: Collision
S
C
S
C
Count Tags
by Slot State
1
≥2
1
≥2

BASE

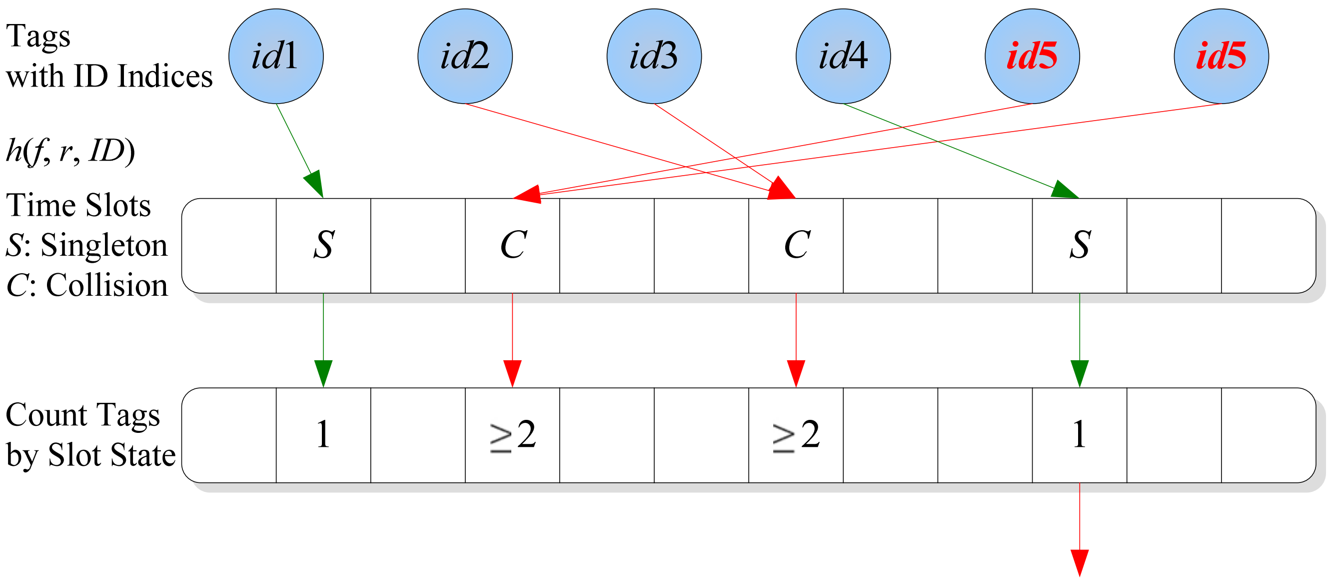


Cardinality Contradiction: $N_{\text{tag}} \geq 1 + 2 + 1 + 2 = 6 > 5 = N_{\text{id}}$

clone detected

BASE

- Limitation
  not that fast for large systems



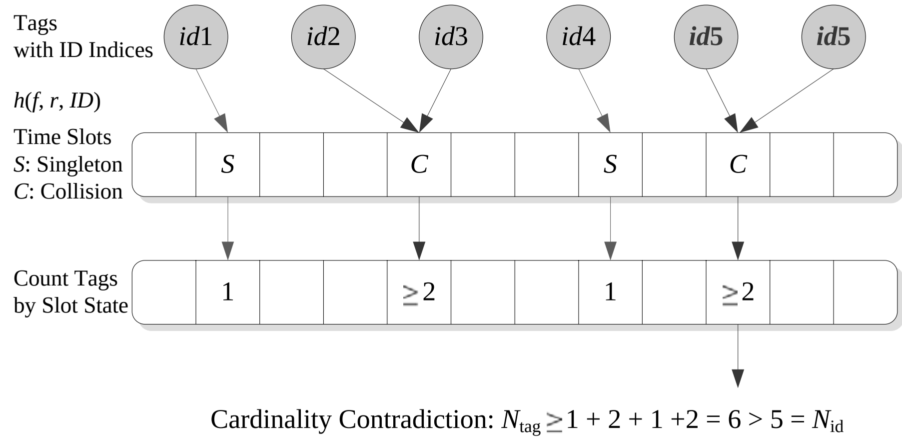
Cardinality Contradiction: $N_{\text{tag}} \geq 1 + 2 + 1 + 2 = 6 > 5 = N_{\text{id}}$

detect clones when almost all tags are counted;
but clone tags may respond earlier.

Fast & Deterministic Protocols

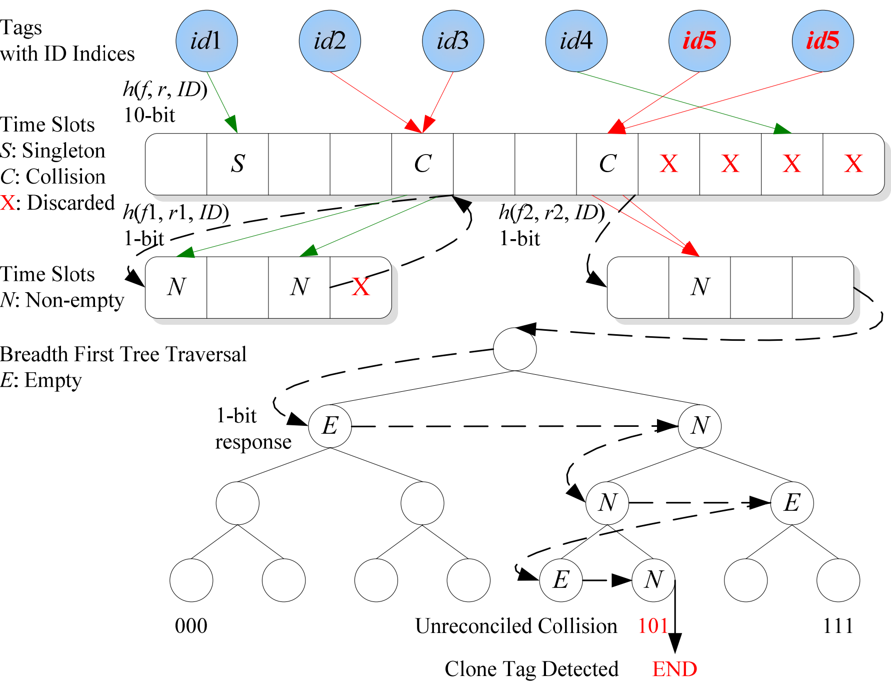
BASE

using cardinality contradiction



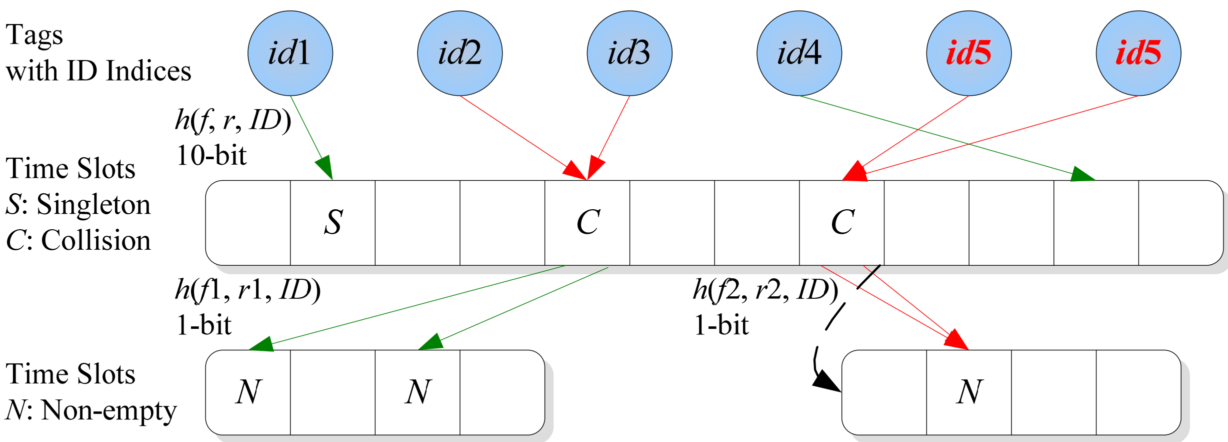
DeClone

using unreconciled collision



DeClone

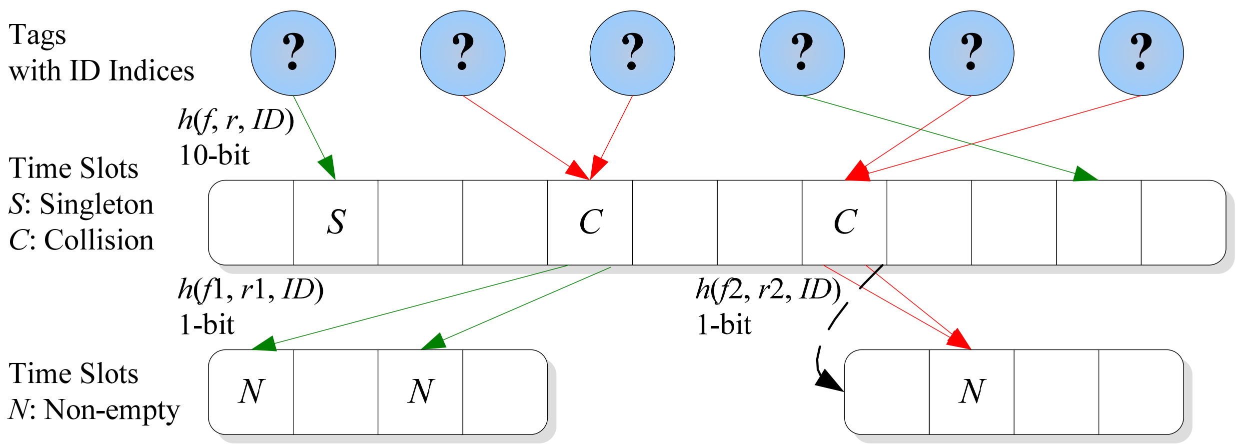
- Motivation
  clone tags induce collisions that cannot be reconciled via re-arbitration



unreconciled collision

DeClone

- Challenge
  verify unreconciled collision
  without tag IDs known a priori?

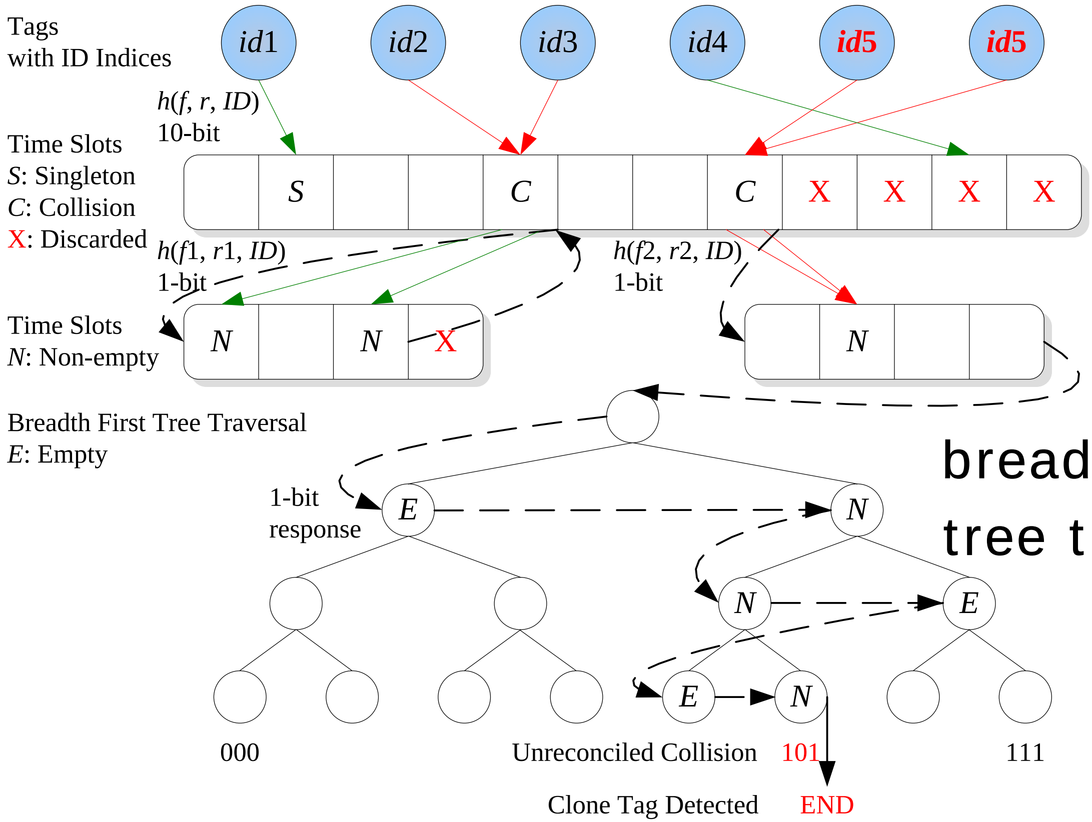


unreconciled collision
due to two same-ID tags?

DeClone

- Design

  marry up slotted Aloha and tree traversal



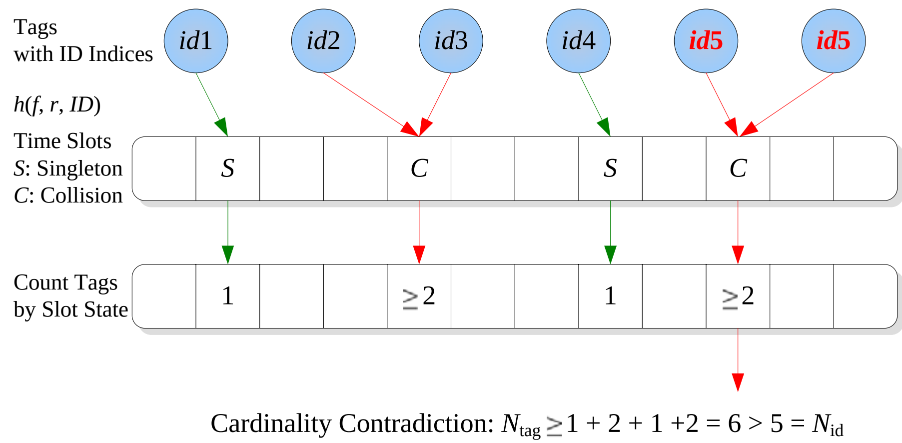
breadth first

tree traversal

Fast & Deterministic Protocols

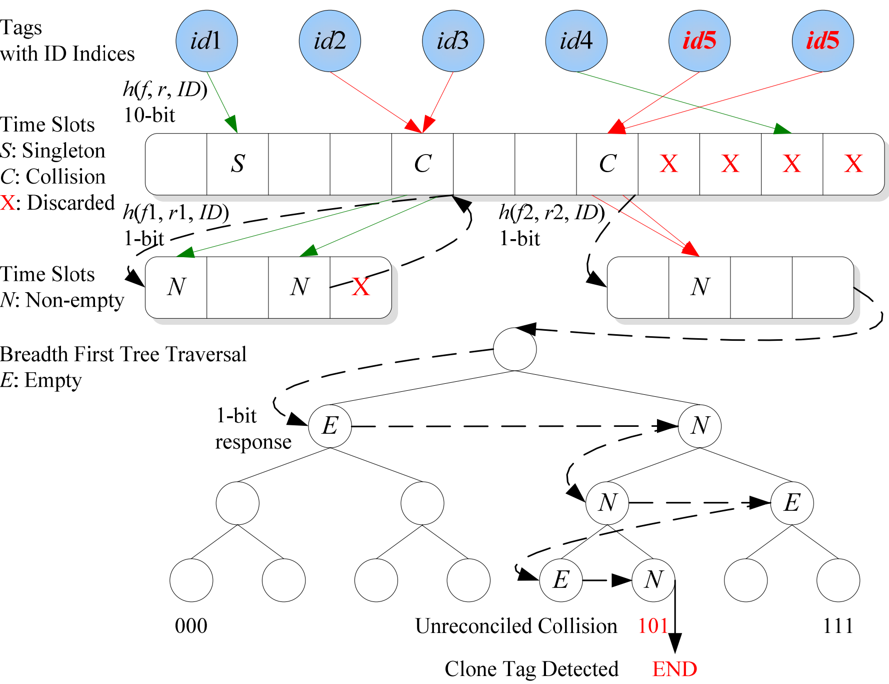
BASE

using cardinality contradiction



DeClone

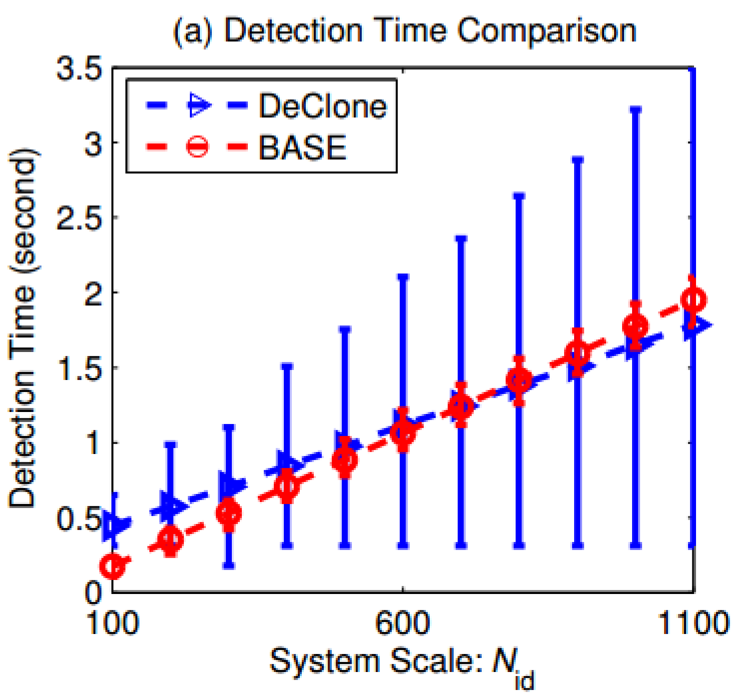
using unreconciled collision

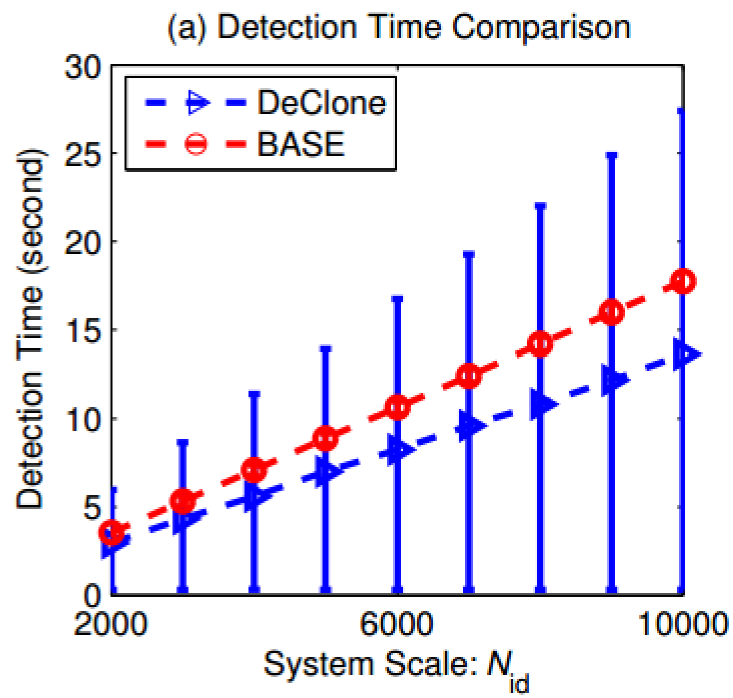


Evaluation

BASE is faster for small systems

DeClone is faster for large ones

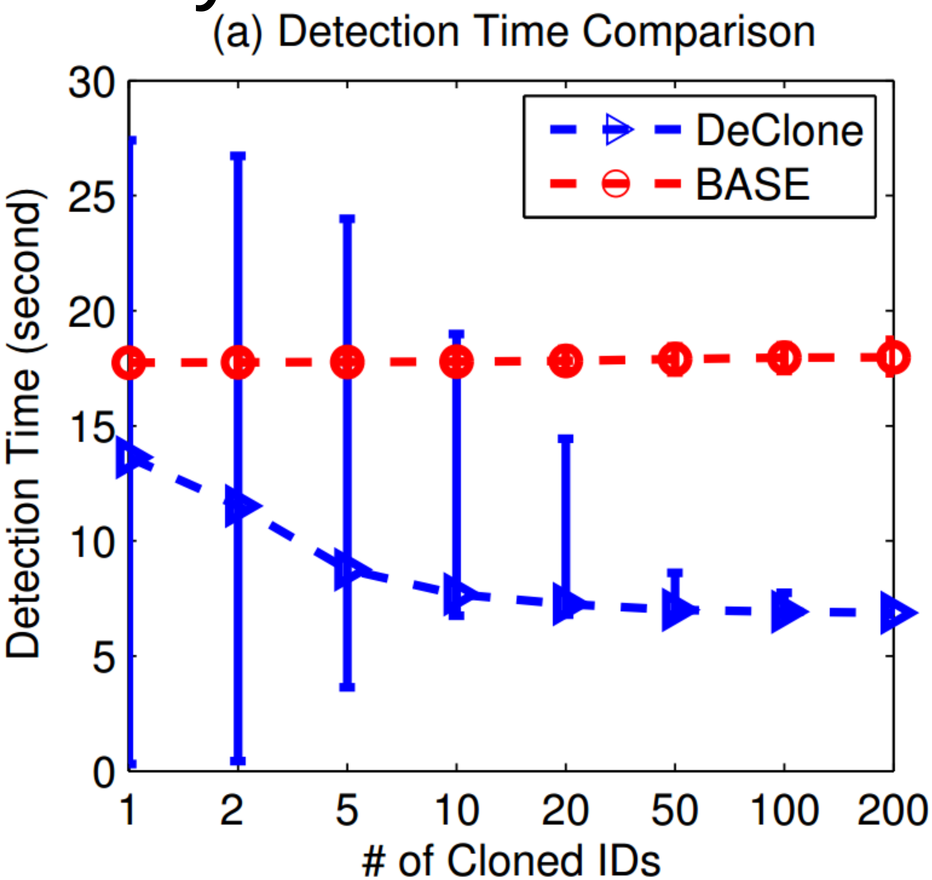




Evaluation

DeClone is faster as clone ratio increases

BASE is nearly constant

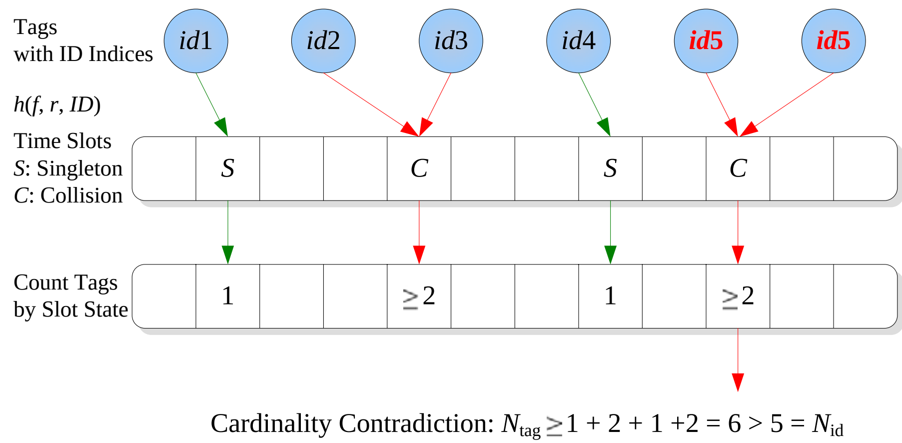


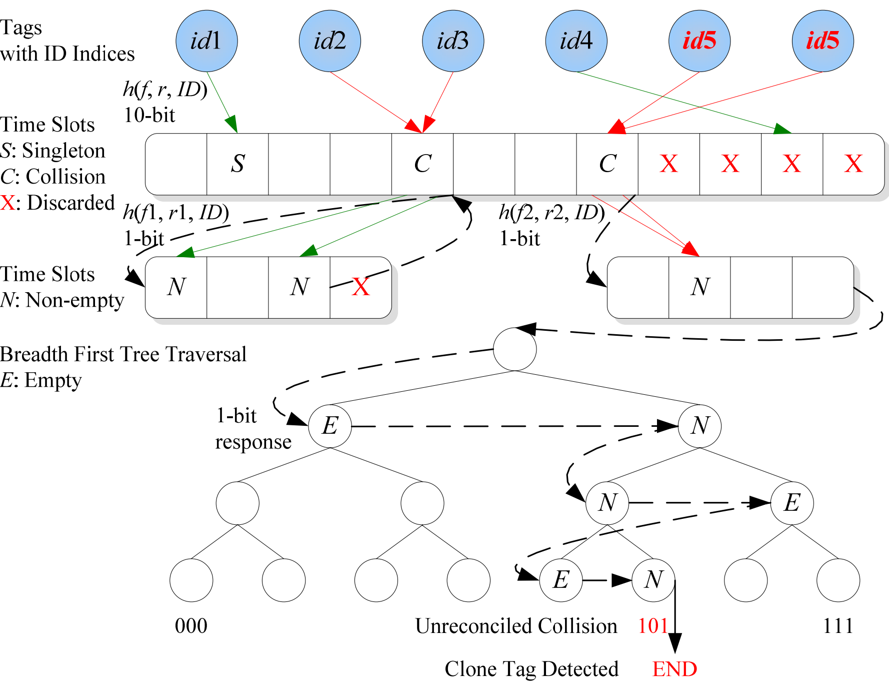
CONCLUSION

Two Fast & Deterministic Protocols

BASE

using cardinality contradiction
faster for small systems





DeClone

using unreconciled collision
faster for large systems
esp when clone ratio↑

Thank You

kaibu@zju.edu.cn
http://list.zju.edu.cn/kaibu

Thank You

kaibu@zju.edu.cn

http://list.zju.edu.cn/kaibu