Privacy of Cached Data in Information-Centric Networks

Aziz Mohaisen

NDNComm – September 4-5, 2014

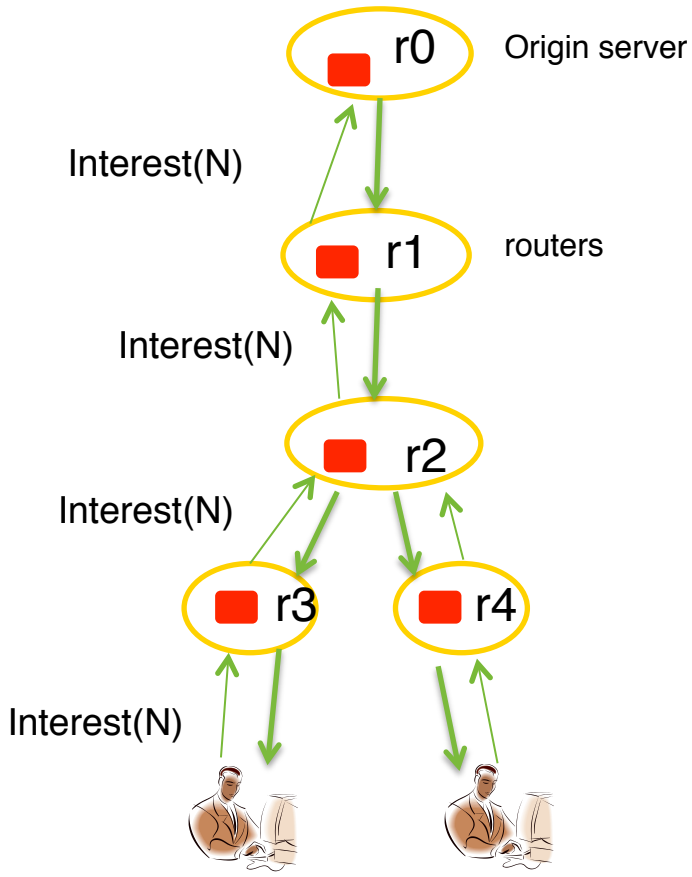
Verisign Labs

Joint work with Xinwen Zhang and Haiyong Xie

Information-centric Network (ICN)

- Several initiatives to realize a future Internet
  - DONA, CCN/NDN, XIA, …
  - NetInf, PSIRP, PURSUIT, …
- Some key features:
  - Named content as first citizen of network, not named host
  - End user files interests with names, not connection request to host
  - Content-oriented network routing, mobility, …
  - Secure content vs. secure channel
  - In-network universal cache
  - …

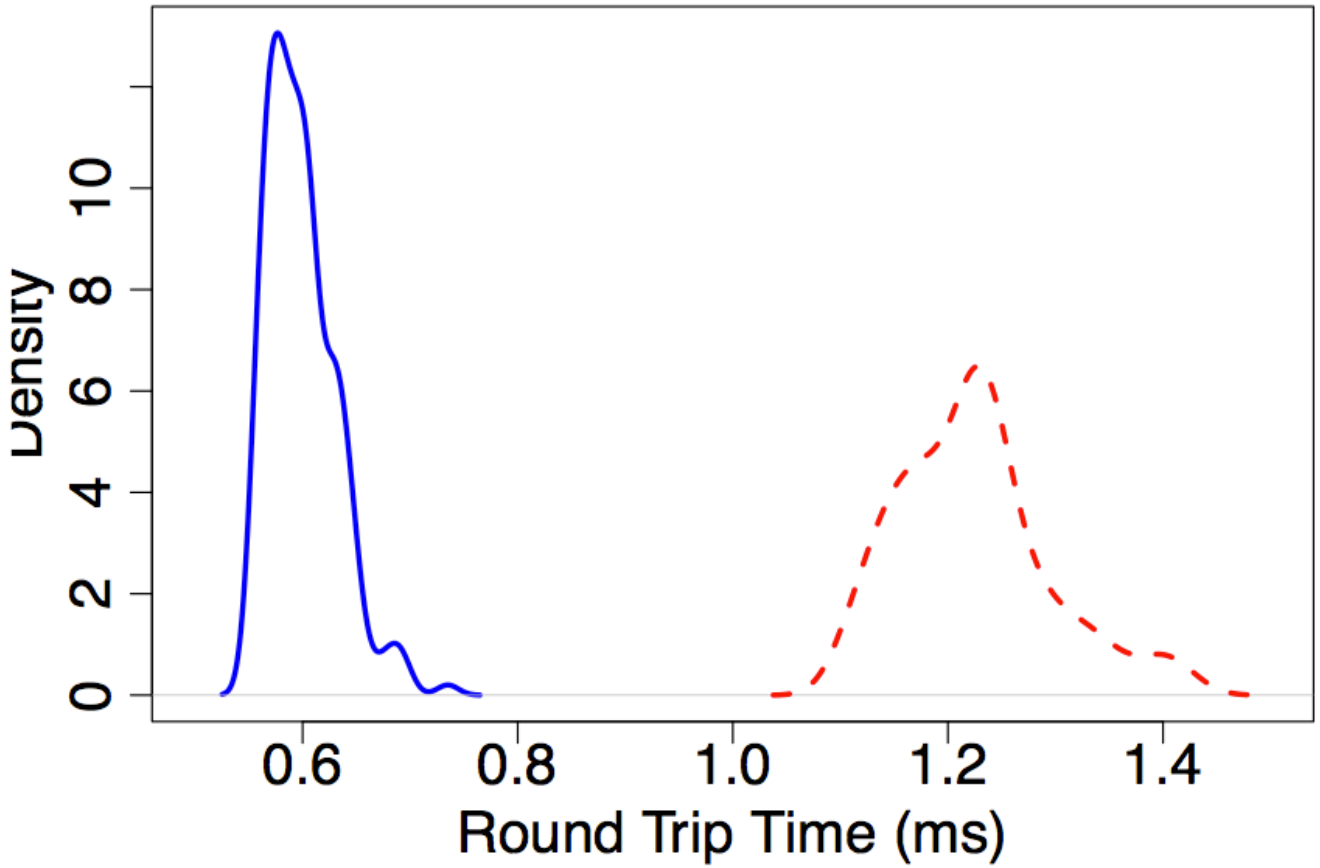
Example of Privacy Risk in ICN



- Fact:
  - If no access before U1 (the first access), then t1 > t2
  - If there is, then t1 ≈ t2
- Suppose U2 wants to know if U1 has accessed before:
  - U2 runs twice of the request and gets t1 and t2
  - If time difference is small, then U1 has accessed
  - If t1 > t2 obviously, then U1 hasn't accessed.
- Why U2 cares this:
  - Privacy of U1
  - Conflict of interest/benefits between U1 and U2

This example only shows that there is some leakage of information, but in general someone will not be able to learn much about individual users.

Example of Privacy Risk in ICN, cont.

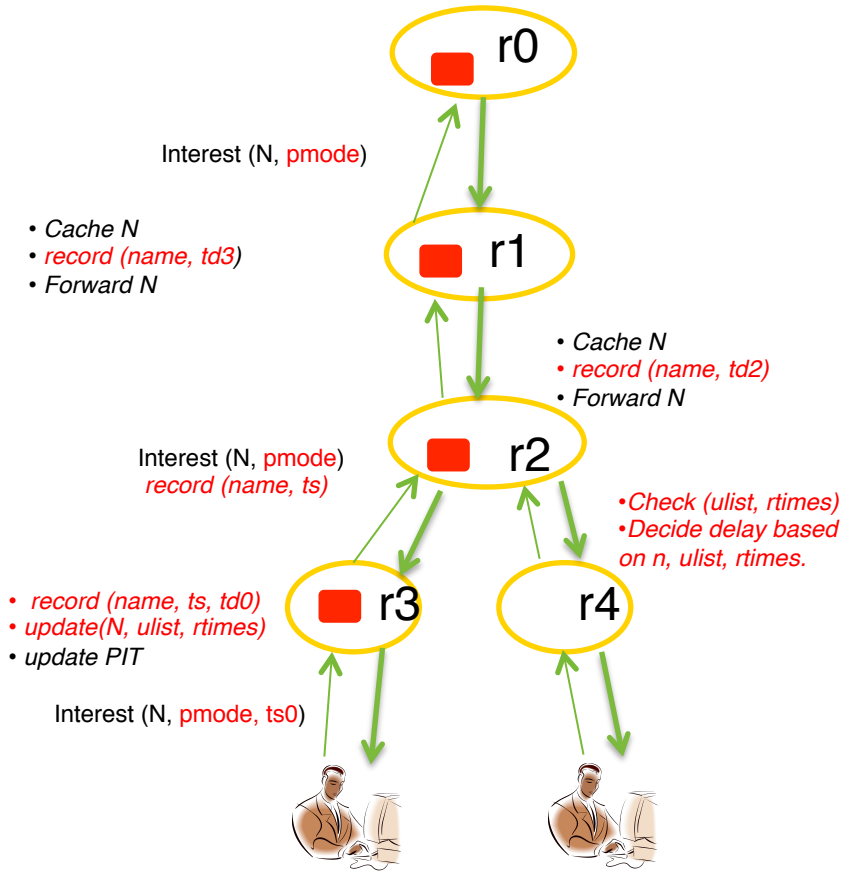


Then…

- Not caching is not an option:
  - It goes against the idea of ICN
  - Selective: two probes reveal if contents are NOT cached for privacy reason.

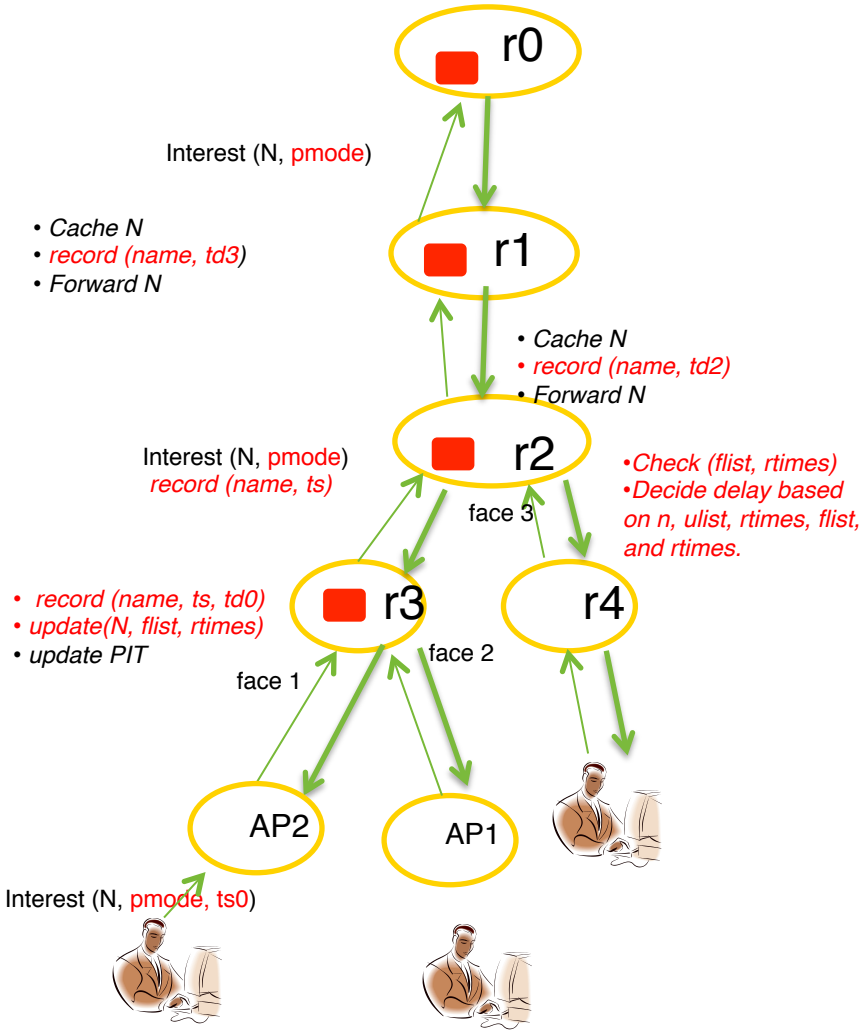
- Intelligent service/caching is required:
  - Relies on access patterns of users
  - Basic solution stores states of user access at routers
    - But comes at high cost (states in routers)
  - Advanced solution aggregates state per face
    - But does not allow low-granularity privacy preservation
  - Advanced solution to maintain state in access points
    - Achieves low granularity and nice performance features

Protocol 1: low-granularity solution



- Pros:
  - Make the time difference like noise of transport time
- Cons:
  - Benign access of N will lose some of the time efficiency – cost of privacy.
  - What if U1 is malicious?
    - Mark everything with pmode
    - May have large user states in router

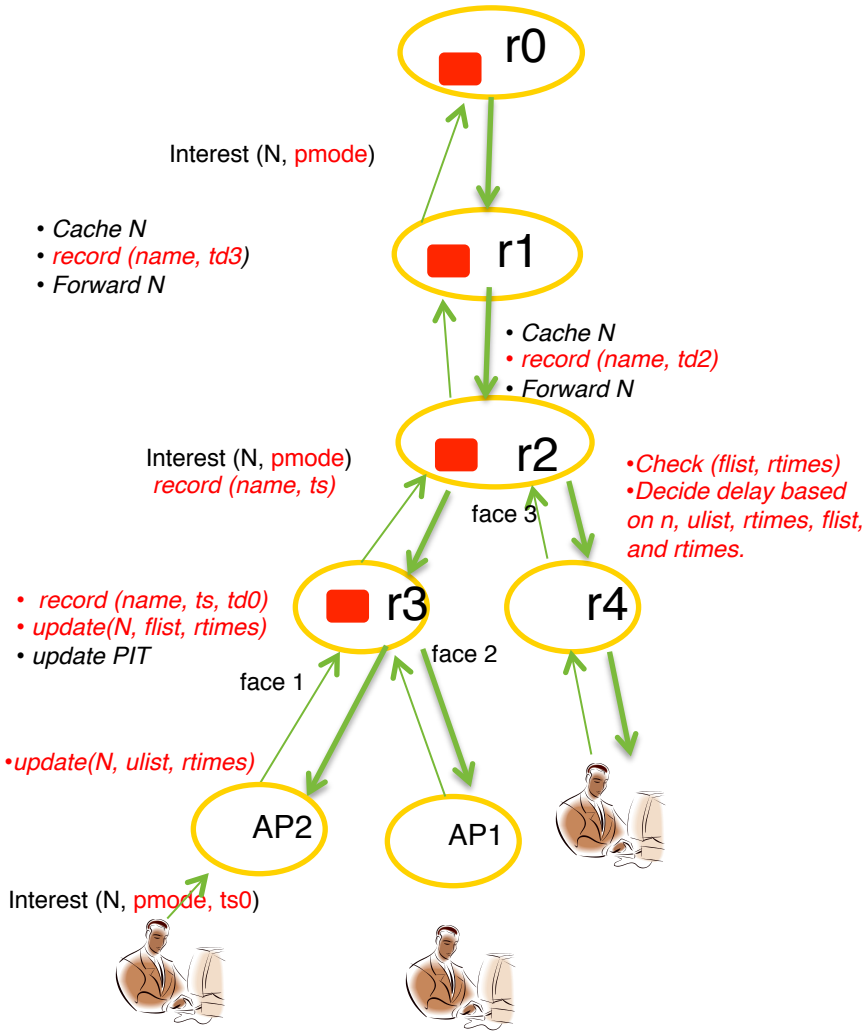
Protocol 2 (alternative)



- Routers only records if a pmode access has been filed from a face
- Interests coming from different domains (or sub-domains) traverse different faces (interface) at the router.

- Pros:
  - Reduces the number of states stored on the router X
- Cons:
  - Does not handle intra-domain privacy risks when the adversary and honest user are both behind the same AP.

Protocol 3 (alternative)



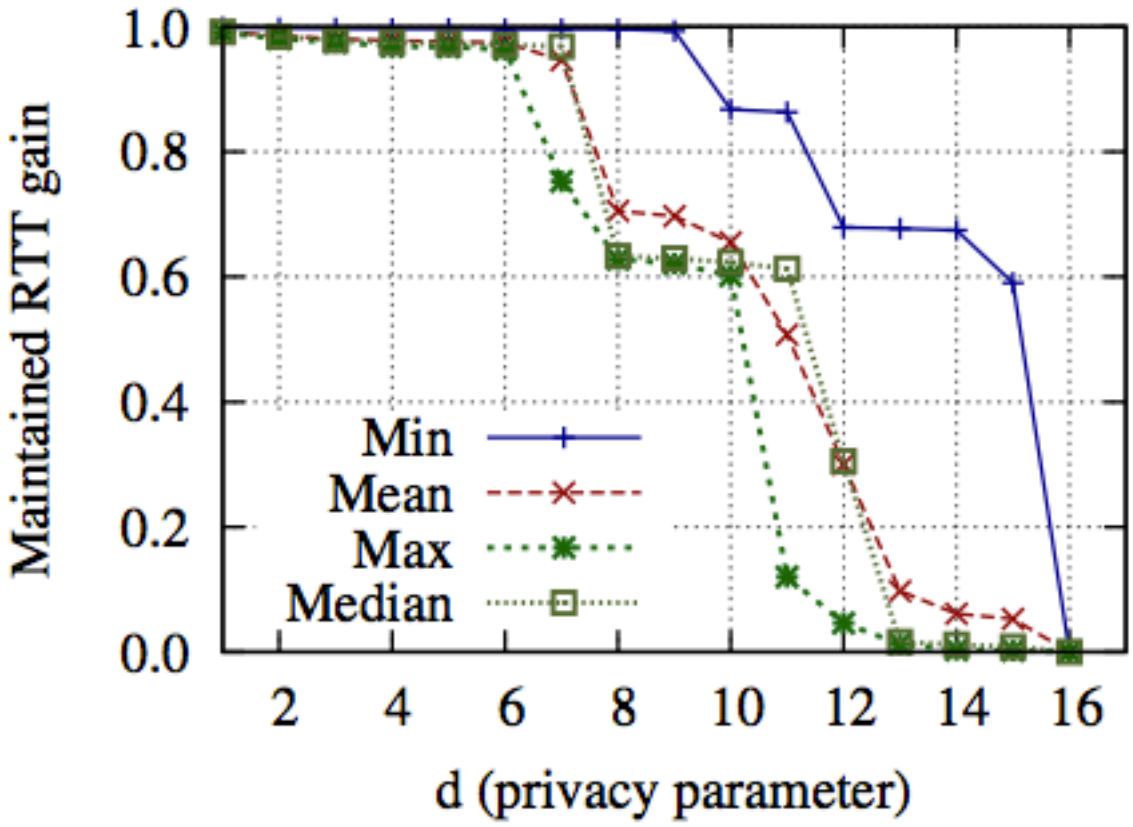
AP is hit before router (not collaboration with AP and attackers)

Distribute states of users sending interests, and the number of access times to AP.

Time stamping and delay is done as before at the side of the content caching router X. AP is used to distribute load of states

Evaluation

- The evaluation measure:
  - Maintained RTT gain under a given number of noise hops



Conclusion

- ICNs improve user experience by reducing RTT of serving contents
  - Enabled by *universal caching* of contents
- We show that this feature has a privacy risk
  - The timing channel can be used to profile access patterns for privacy
  - Simple solutions fall short for one reason or another
- We propose three protocols for the problem that strike a balance between privacy granularity and overhead
  - Evaluated using real-world timing measurements
  - Overhead to legitimate users is reasonable
  - Maintain the features of universal caching for ordinary users

References

- Aziz Mohaisen, Xinwen Zhang, Max Schuchard, Haiyong Xie, Yongdae Kim: Protecting access privacy of cached contents in information centric networks. ASIACCS 2013: 173-178
- Aziz Mohaisen, Hesham Mekky, Xinwen Zhang, Haiyong Xie, and Yongdae Kim: Timing Attacks on Access Privacy in ICN and Countermeasures, IEEE TDSC, 2014

VERISIGN®