AC3N: Anonymous Communication in Content-Centric Networking

Christopher A. Wood
University of California Irvine
woodc1@uci.edu

Gene Tsudik
University of California Irvine
gts@ics.uci.edu

Ersin Uzun
Palo Alto Research Center
ersin.uzun@parc.com

IEEE CCNC 2016
Las Vegas, NV, USA
1/11/2016

Agenda

1. Quick CCNx review
2. ANDaNA overview
3. Shortcomings
4. AC3N design
5. Performance
6. Q&A

Security in CCN

CCN is all about *transferring named data*

All data is named, **secured** (to some degree), and then transferred

We focus on the security of data and users with regards to:

Authenticity: trusting the legitimacy of content

Confidentiality: controlling who has access to the data

Anonymity: Hiding who is requesting, using, and producing data

…Solutions to all of these problems are still an area of active research in CCN (and ICNs in general)

Anonymity in CCN

CCN already benefits from a lack of source and destination addresses

…but, (global) adversaries capable of eavesdropping and monitoring network traffic can still match interest and content objects

A sampling of approaches

- Use cover traffic to “hide in plain view” [1]
- Use TOR-like onion encryption [2]
- Random interest propagation (e.g., CROWDS) [3]
- …

[1] S.Arianfar,T.Koponen,S.Shenker,andB.Ragha- van. On preserving privacy in content-oriented networks. In ACM SIGCOMM Workshop on Information-Centric Networking, 2011.
[2] S. DiBenedetto, P. Gasti, G. Tsudik and E. Uzun, ANDaNA: Anonymous Named Data Networking Application, 19th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, 2012.

[3] Zhang, P.; Li, Q.; Lee, P., "Achieving Content-Oriented Anonymity with CRISP," in *Dependable and Secure Computing, IEEE Transactions on* , vol.PP, no.99, pp.1-1.

Onion Routing in CCN (ANDaNA)

Use TOR-like **onion routing** to ***unlink*** producers (content) and consumers (interests)

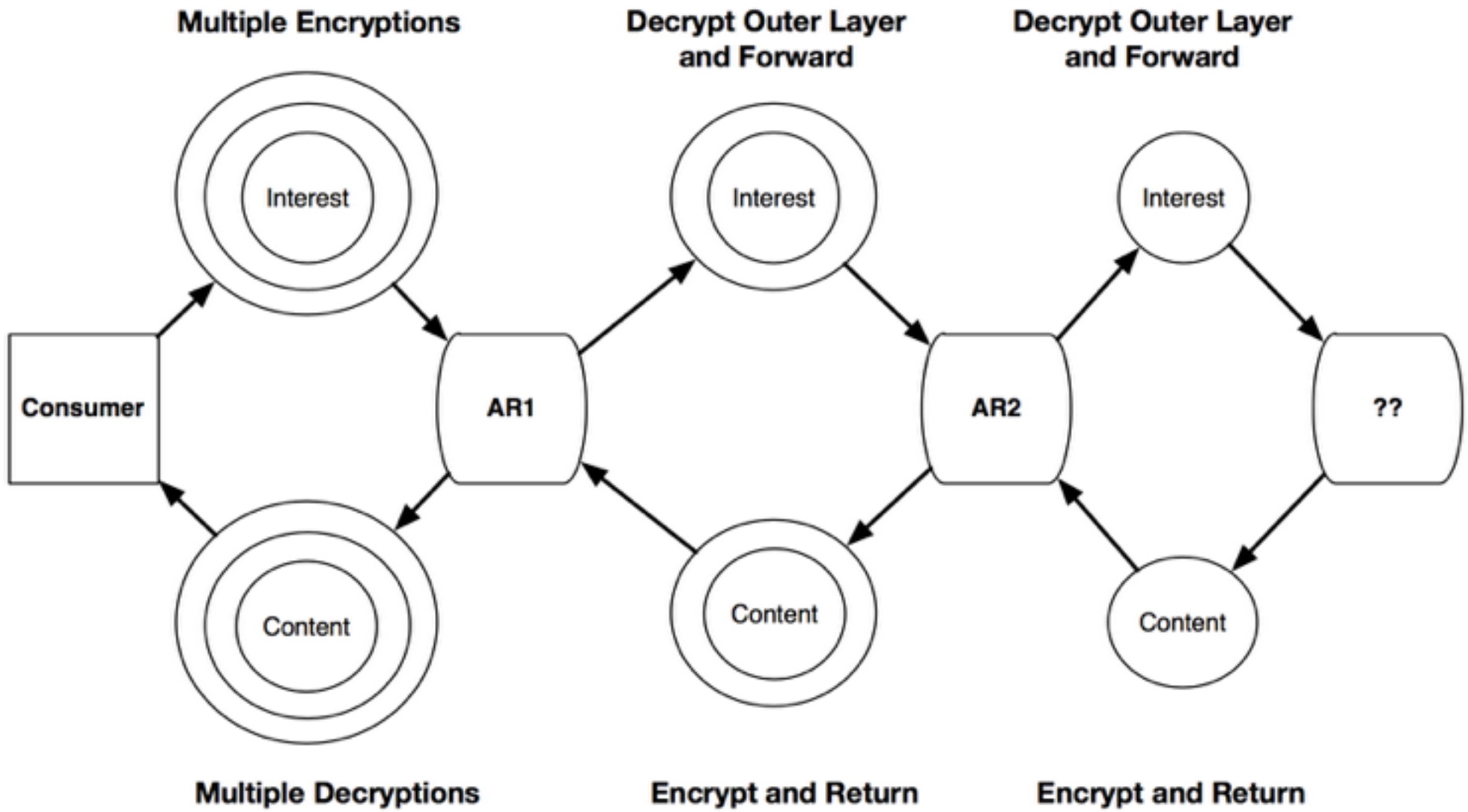
An application-layer circuit is established to:

- Decrypt ingress upstream interests

- Verify, encrypt, and re-sign ingress downstream content

Onion routing is based on public-key or symmetric-key encryption

Onion Routing in CCN (ANDaNA)



Quick Definitions

- **Producer (consumer) anonymity**: Unable to determine if a producer (consumer) produced (requested) a particular piece of content

- **Packet unlinkability**: Unable to link interests with their corresponding content objects.

- **Session unlinkability**: Unable to link interests that belong to the same circuit

Shortcomings

- ANDaNA provides consumer and producer anonymity and packet unlinkable with wrapping based on public-key encryption
- Session-based ANDaNA does not provide session unlinkability
    - Session IDs identify keys used to encrypt packets

AC3N Overview

AC3N: Anonymous Communication for CCN

It's (session-based) ANDaNA V2 with the following improvements:

1. Exclusive use of symmetric crypto online (for higher throughput):

- XOR-based encryption with asynchronous key stream generation

- (H)MACs for authenticity tag generation and verification

2. Dynamic session identifiers to prevent linkability between Interests and Content Object message pairs in a session

XOR-based encryption

- Each packet in a circuit is associated with a unique key stream that can be precomputed

- Consumers precompute this key stream to decrypt content objects using XOR-based encryption

- Anonymizing routers encrypt by XORing the content object with their key stream

MAC-based verification

- Anonymizing routers and consumers use HMAC to tag and verify wrapped content objects
- HMAC keys are derived during session establishment
- Anonymizing routers in a circuit share pair-wise HMAC keys to a complete chain from the producer to the consumer

Dynamic Session Identifiers

- The session identifier is mutated after every sequential interest that's received

- Consumers and anonymizing routers share a common secret (SessionIV) used to advance the identifier

$$\mathsf{SessionIndex}_i^{j+1} = H(\mathsf{SessionIV}_i^j + \mathsf{SessionIndex}_i^j)$$
$$\mathsf{SessionIV}_i^{j+1} = 1 + \mathsf{SessionIV}_i^j \mod (2^\kappa).$$

Anonymity Properties

AC3N achieves

- Complete producer and consumer unlinkability, and

- Complete Interest and Content Object unlinkability in packets and sessions,

subject to a *global, active adversary* capable of:

- Observing and replaying traffic,

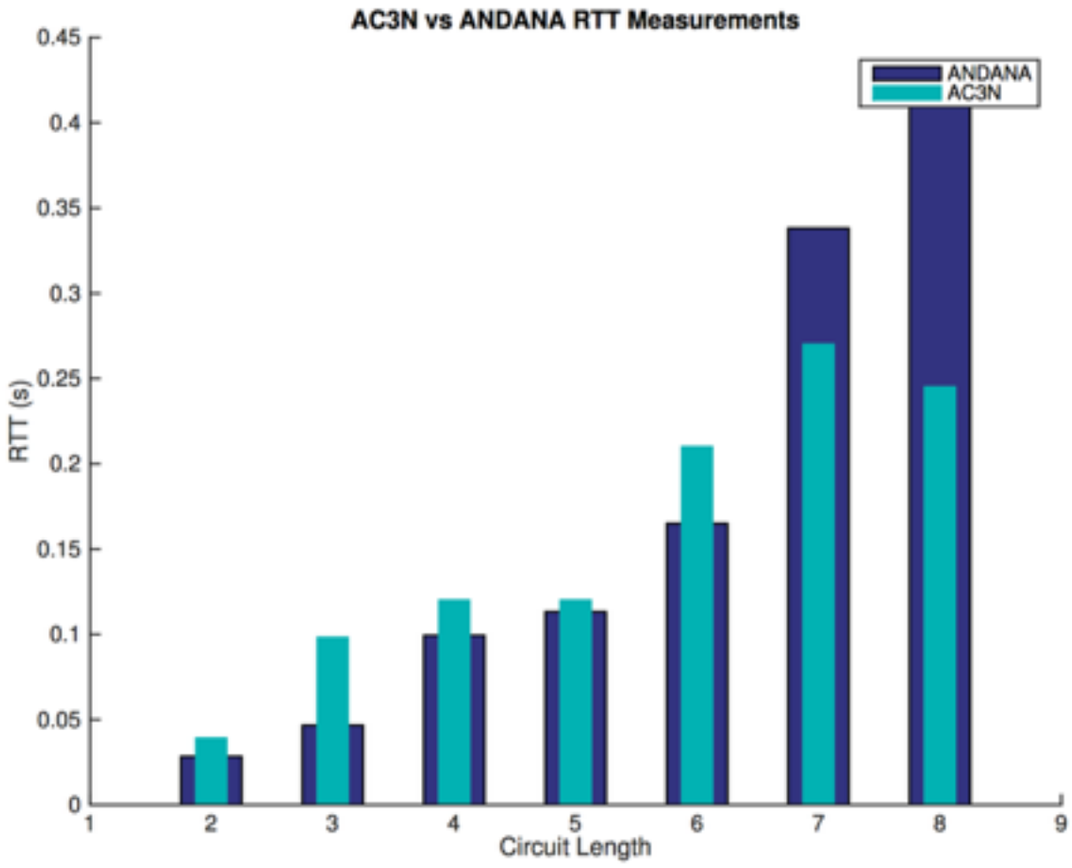
- Compromising and deploying non-border routers, and

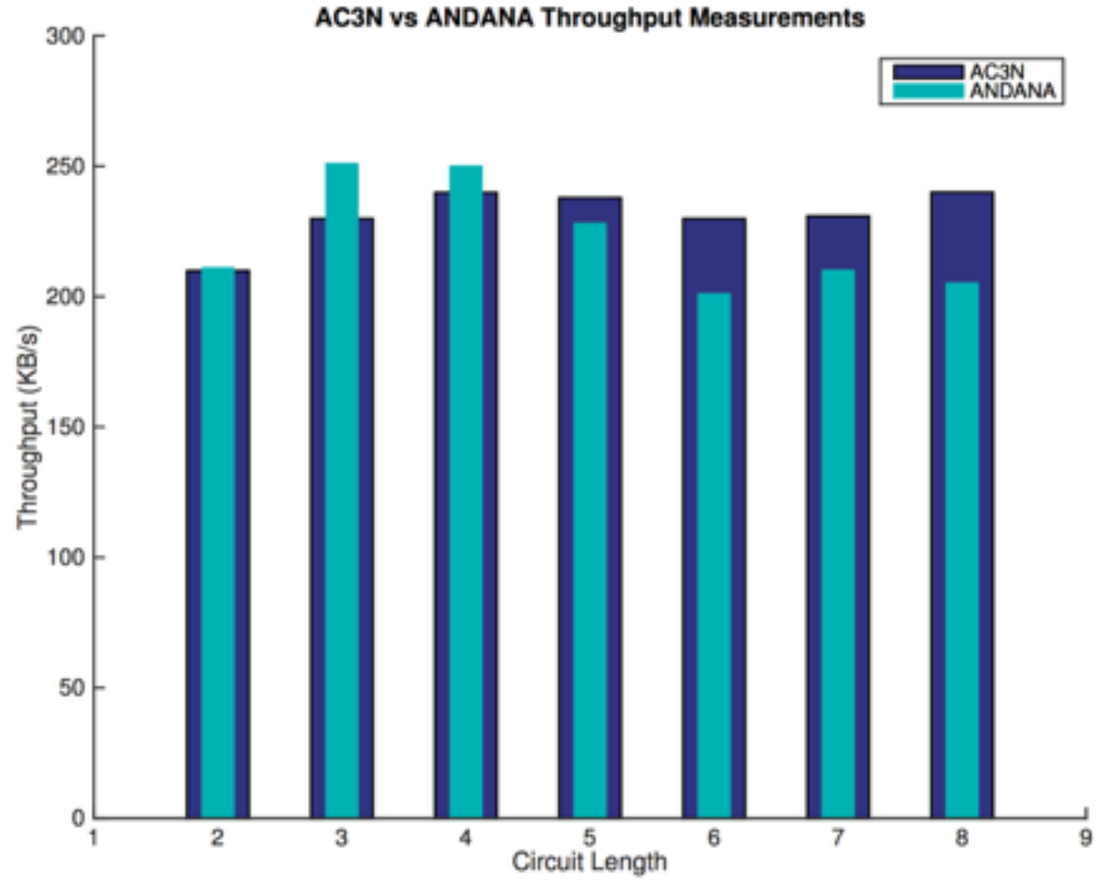
- Controlling content producers.

Future Work

- Replace session initialization protocol with one that builds on CCNx-KE or something similar
- Integrate the AC3N API into the CCNx stack as a service
- Adopt the HORNET onion routing design to AC3N

Quick Performance Peek





Future Work: Add an AC3N API to CCNx

A consumer API should be developed to enable:

- Participating node namespaces (DNS-like service)

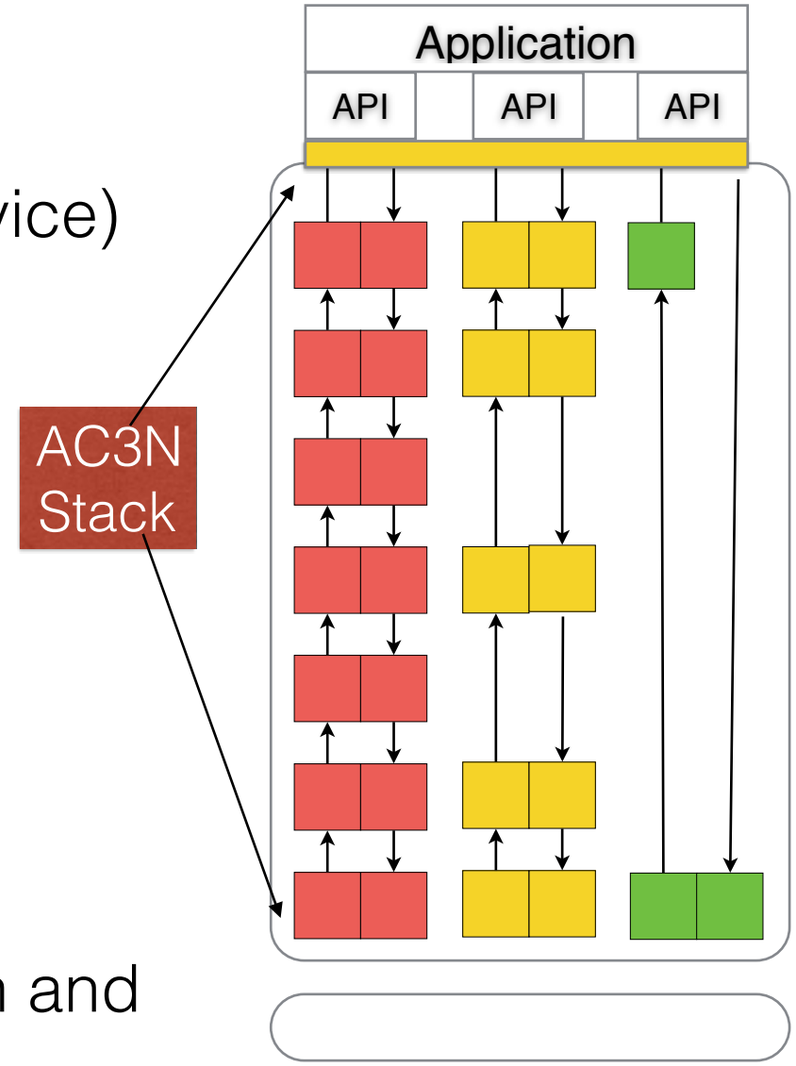
- Circuit setup

- “Anonymous” interest creation

A producer API should be developed to enable:

- Instantiate an “anonymous” (AC3N) stack

- Handle Interest and Content Object encryption and MAC generation



Questions?

Fire away!