Named Data Networking (NDN) a quick overview

milcom

Military Communications for the 21st Century

LAX Marriott, Los Angeles, CA

NDN: a new way to build networks

- Why we need a new way

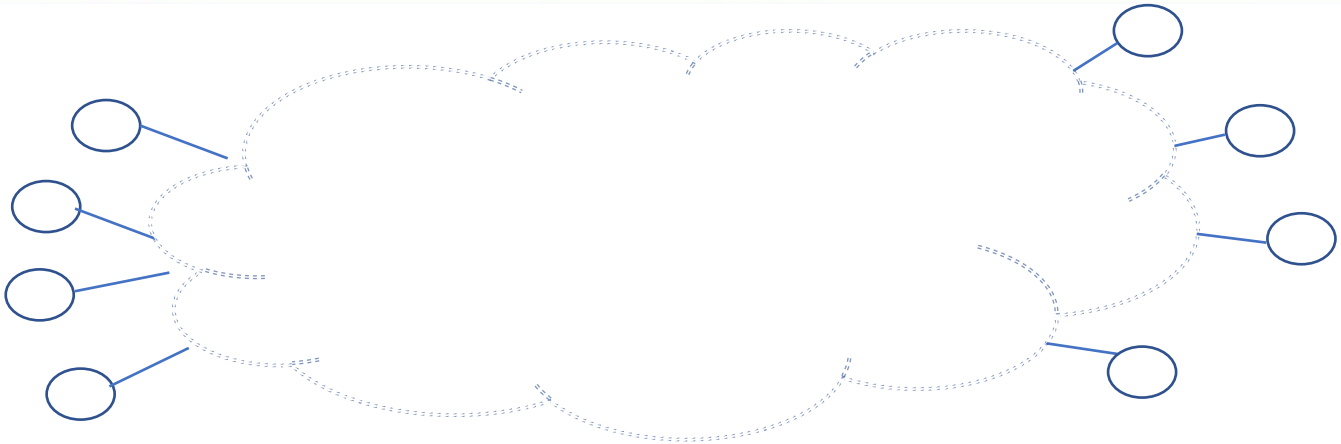
- What is the new way

- How this new way is inherently more secure & resilient than the existing TCP/IP network architecture

TCP/IP : a revolution to communication (40 years ago)

- Telecom: setting up a circuit first
- From circuit to packet switching
  - "It was this need for *survivability of communications* that required plodding through new ground not previously explored." – Paul Baran, 1977
- Packet switching: computers as switches
  - Enabling one to send data packets *without setting up a circuit first*
  - Enabled by technology advances

TCP/IP: building a resilient network infrastructure



- Point-to-point datagram delivery
  - The same communication model as telecom
  - IP addresses identify network attachment points
- Communication through the infrastructure is orders of magnitude more resilient due to *dynamic routing*

40 years passed, technology advanced again (by a lot)

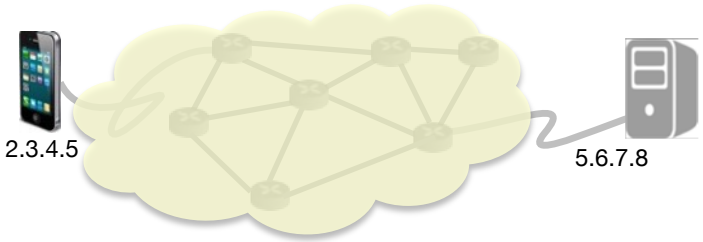
(IP-based Infrastructure communication succeeded beyond the wildest dreams)

- Today: (ad hoc) mobile wireless communications
  - Hand-held devices, drones, ships, aircrafts
  - Each may possess multiple interfaces
- Applications have changed too
- Mobiles and large number of IoT devices have made it increasingly difficult to achieve communication resiliency by shooting packets to specific IP addresses

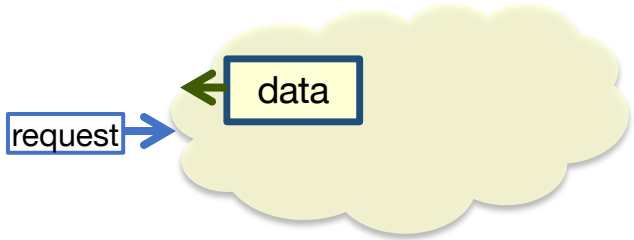
https://www.youtube.com/watch?v=oCZMoY3q2uM

What's the new way:

- IP delivers packets to hosts based on numeric IP addresses



- Named Data Networking fetches data by using application data object names



- Example data names
  - www.nist.gov/document/ndnagendav5docx
  - www.youtube.com/watch?v=oCZMoY3q2uM
    - Large objects fragmented to multiple packets, each fragment uniquely named

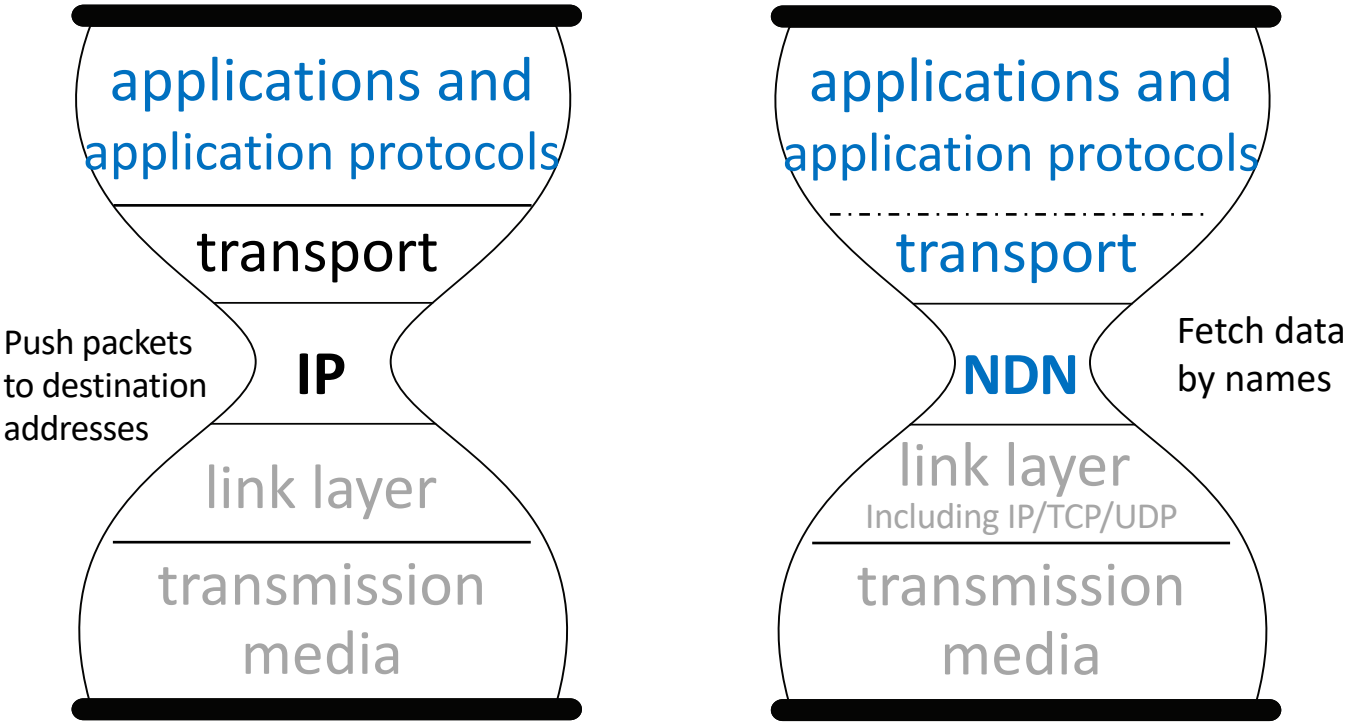
Networking by application named data

milcom

Military Communications for the 21st Century

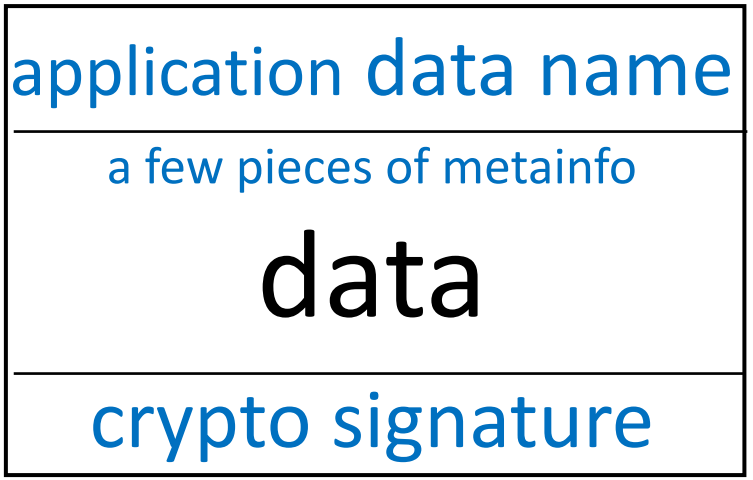
LAX Marriott, Los Angeles, CA

A conceptually simple change



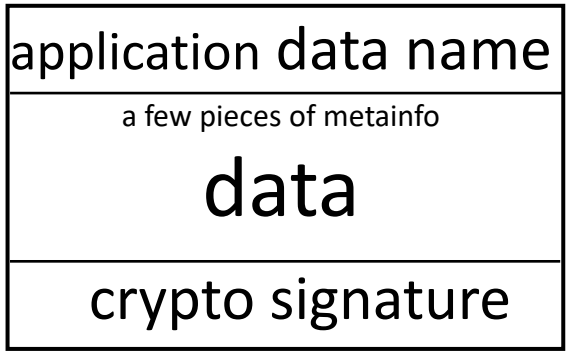
NDN: two types of network layer packets

Consumer requests data by sending **Interest packet**



Producer binds name to content to create **Data packet**

Named data enables securing data directly

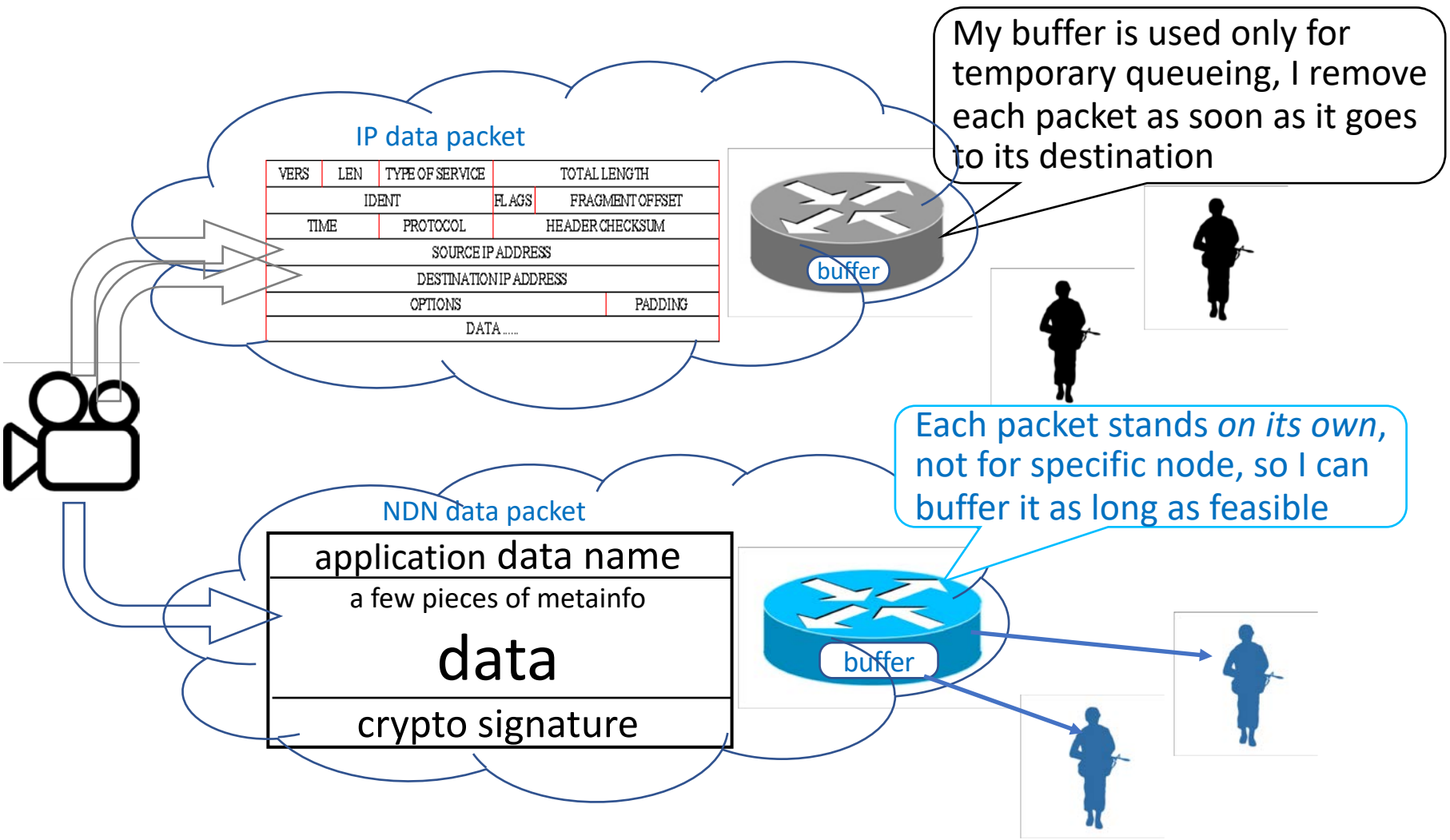


The signature binds the name and content at data production time

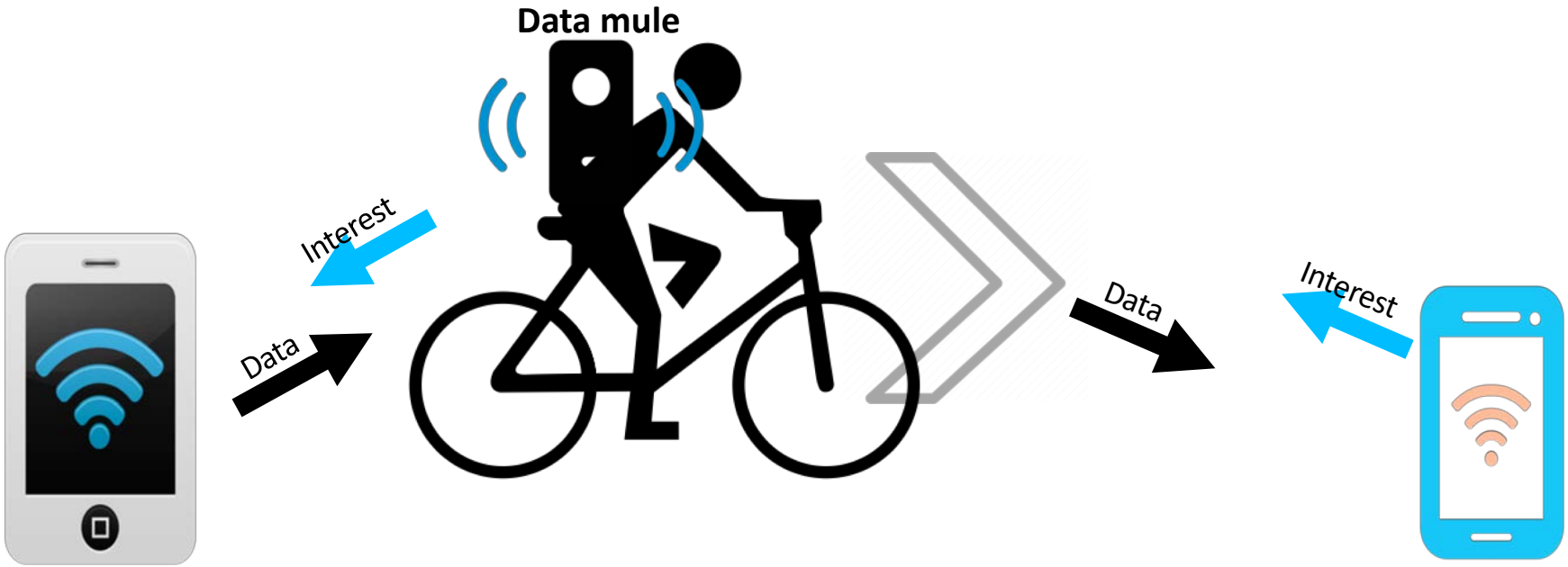
Named data enables host multihoming

- IP assigns address to each interface, switching between interfaces leads to address change
- Data name is independent from interface, can freely use any or all of the interfaces

Named, secured data enables in-network caching



Named data enables data muling at network-layer



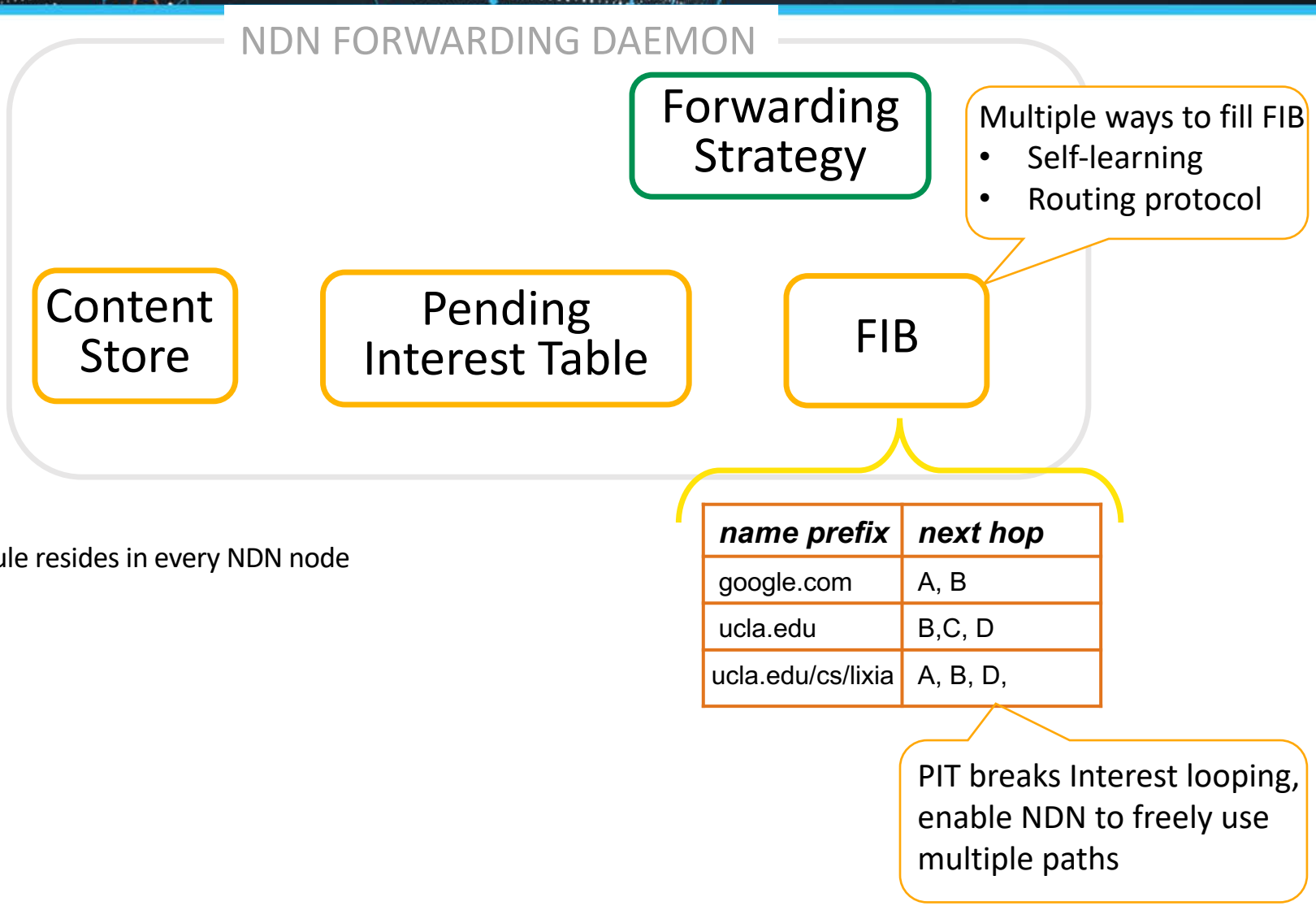
NDN's Stateful Forwarding Plane

milcom

Military Communications for the 21st Century

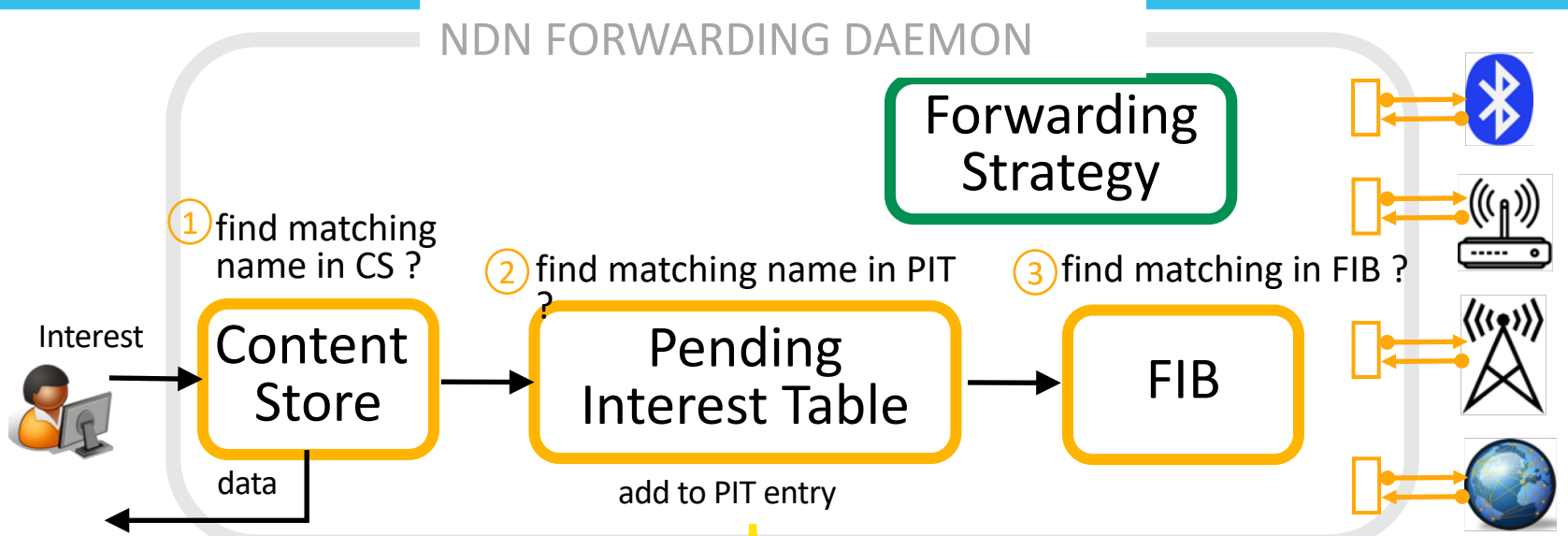
LAX Marriott, Los Angeles, CA

NDN's node model



NFD module resides in every NDN node

NDN Interest Forwarding

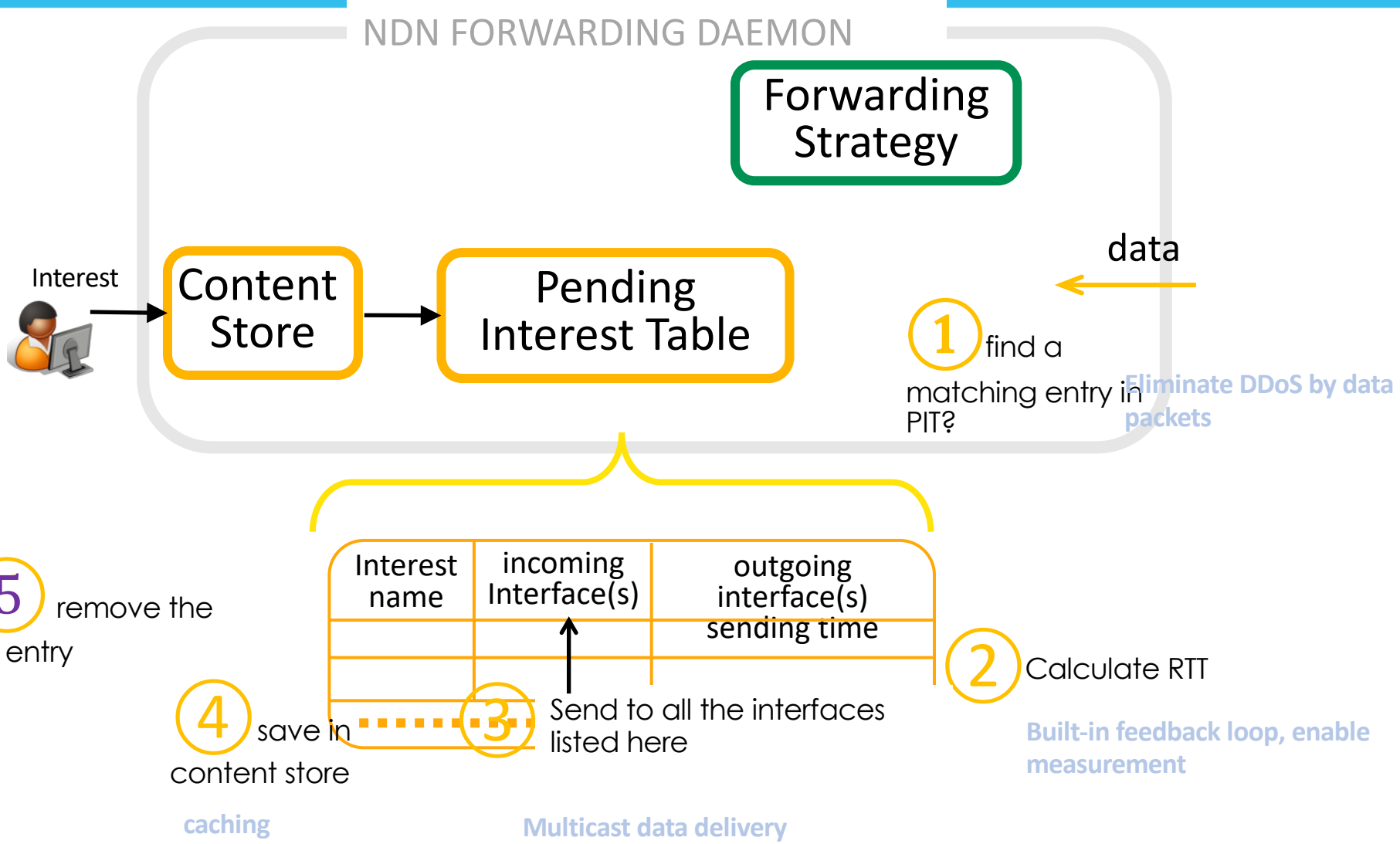


For each PIT entry:

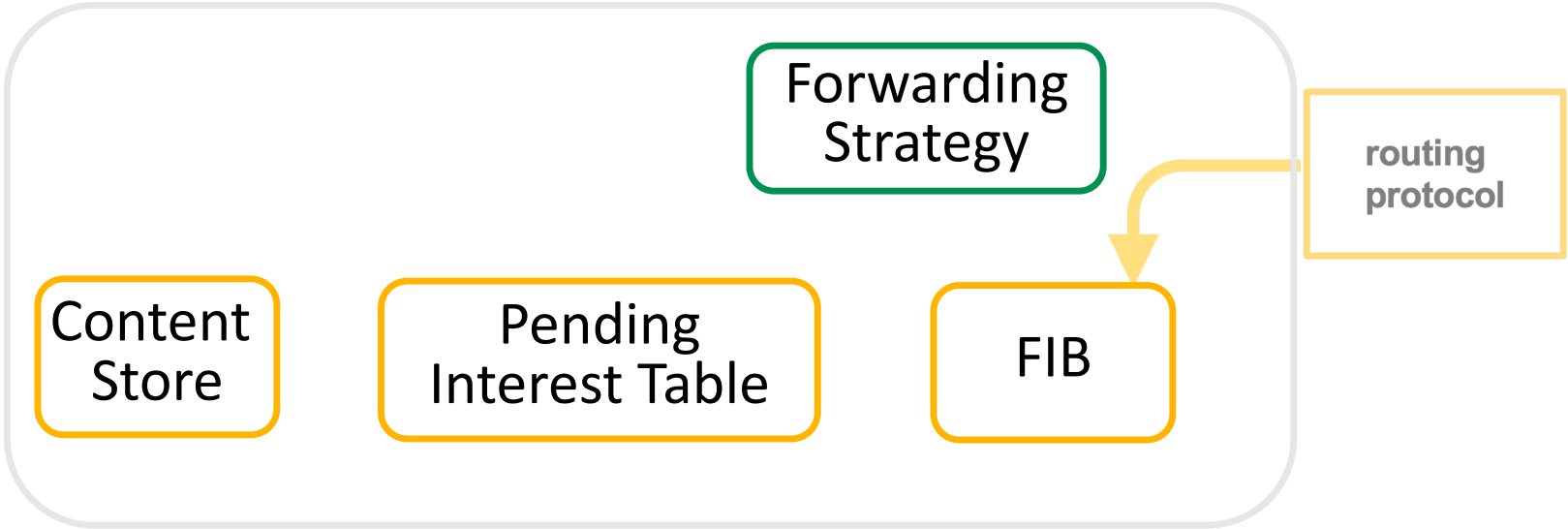
Interest name	incoming Interface(s)	outgoing interface(s) sending time

May forward an interest packet out through one or more interfaces

NDN Data Packet forwarding



Forwarding Strategy



- Forwarding Strategy makes interest forwarding decisions by taking input from
  - FIB
  - measurement from Interest-data exchange (and any other local resource information)
  - Per-namespace forwarding policies

Resilient data availability means

- Host multihoming
- Pervasive in-network storage
- Delay/disruption tolerance
- Multipath forwarding
- Multicast delivery

- All the above lead to *redundant* means to get data
- Enabled by making data itself identifiable independent from containers or channels

NDN's Security Support

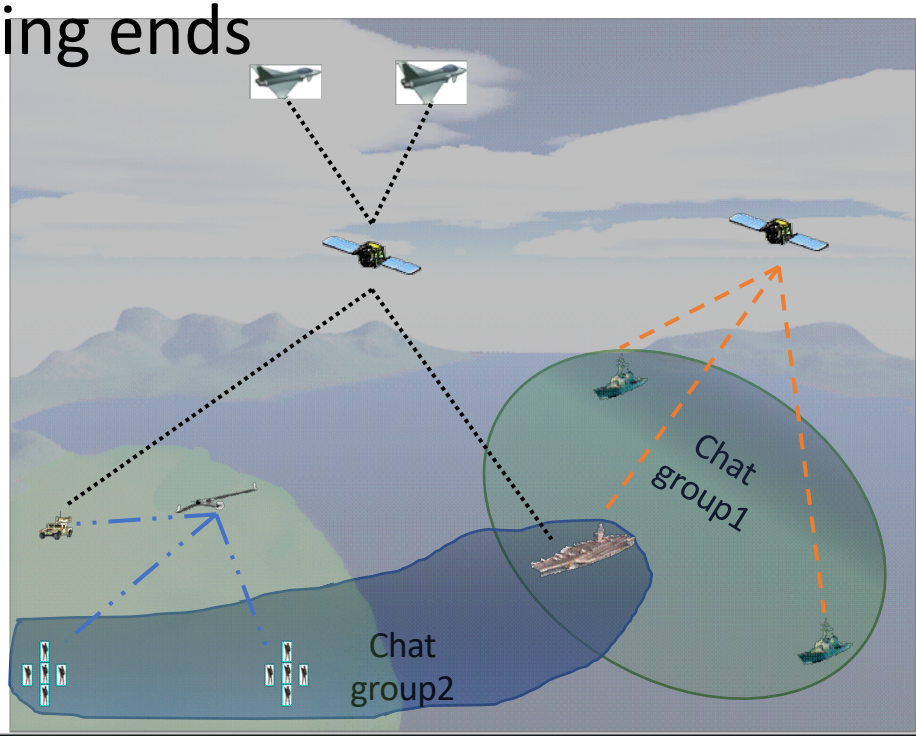
milcom

Military Communications for the 21st Century

LAX Marriott, Los Angeles, CA

Howe we secure communication today

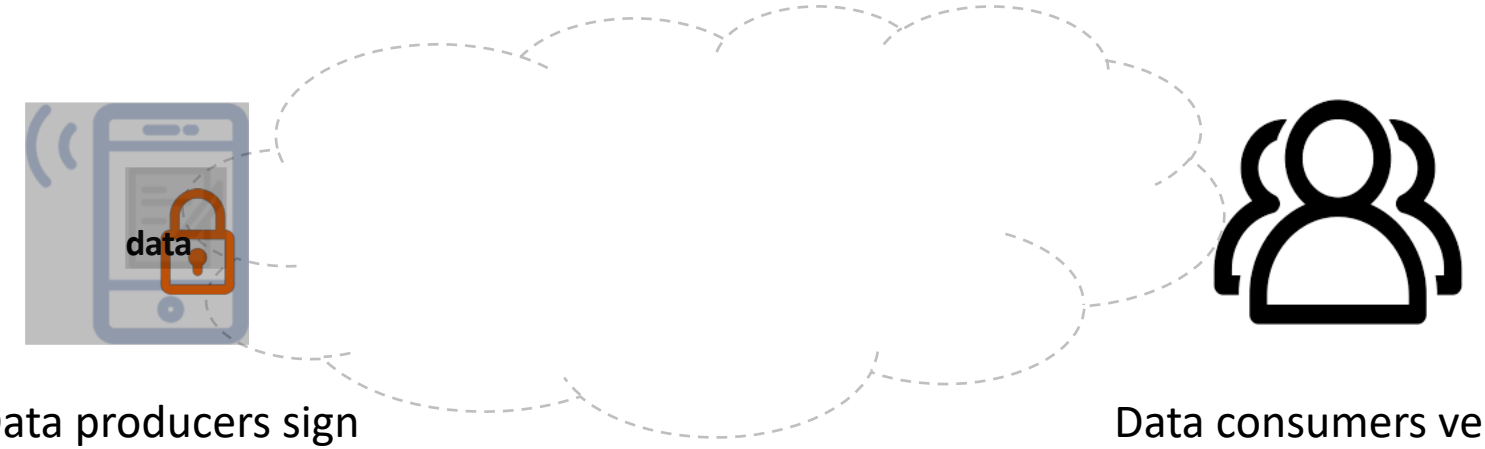
- Encrypting point-to-point channels
  - TLS
  - QUIC
- Running over IP, requiring synchronized connectivity between the two communicating ends
- Battlefields need support for delay/disruption tolerant communications



NDN builds security into (data) packets

- Independent from data containers or communication channels
- Data packets are sealed at production
- Interest packets can be authenticated as well

NDN enables end-to-end data security



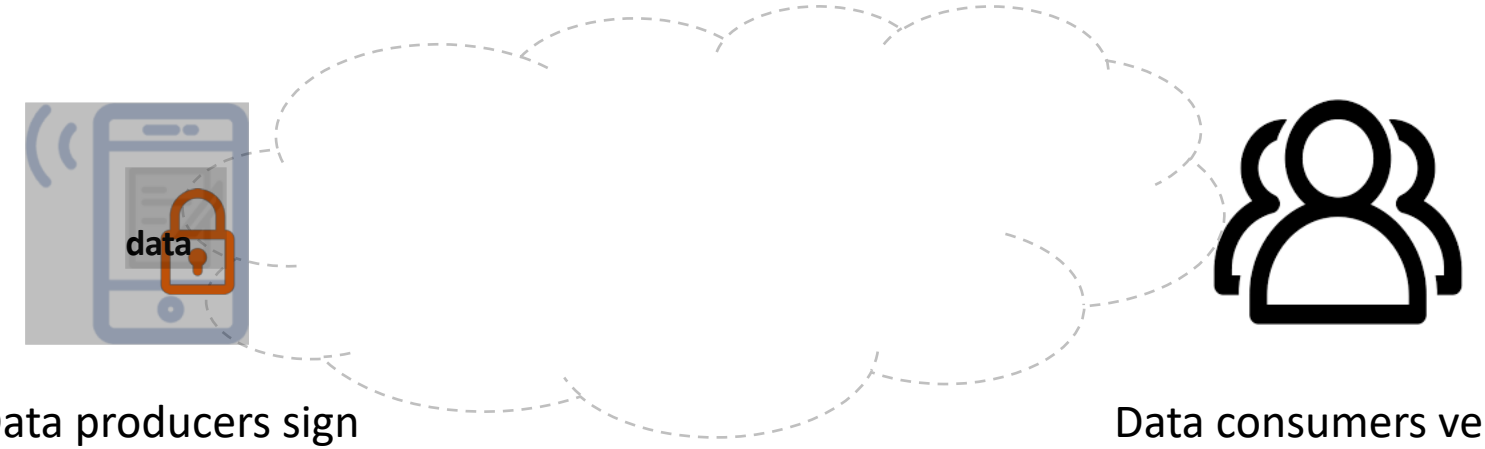
Data producers sign

Data consumers verify

End-to-end data authenticity

independent from intermediate communication channels, middle boxes, intermittent connectivity

End-to-end data security



Data producers sign

Data consumers verify

- Requiring security bootstrapping: installing trust anchor(s) into all entities in an NDN network
- Requiring every data producing entity possess cryptographic key(s)
- Requiring efficient signing and verification for resource constrained devices

Designing security building block into the narrow waist

Network security is conceptually simple:

- Data authenticity → Signing/verifying received data
  - NDN mandates data authentication
- Data confidentiality → Encrypting data
  - NDN supports name/attribute-based encryption
- Data availability → via redundancy
  - Making multiple copies
  - Trying multiple paths
  - Native properties of the forwarding plane

The real security challenges

- Trust management
  - Today: through commercial certificate authority services
  - NDN's approach to trust management
    - Start with local trust anchors
      - UCLA as the trust anchor for all UCLA controlled business
    - Establish relations among trust anchors

    Similar to "SDSI - A Simple Distributed Security Infrastructure https://people.csail.mit.edu/rivest/sdsi10.html
- Usability
  - Comprehensive trust policy configurations
  - Automated crypto key management

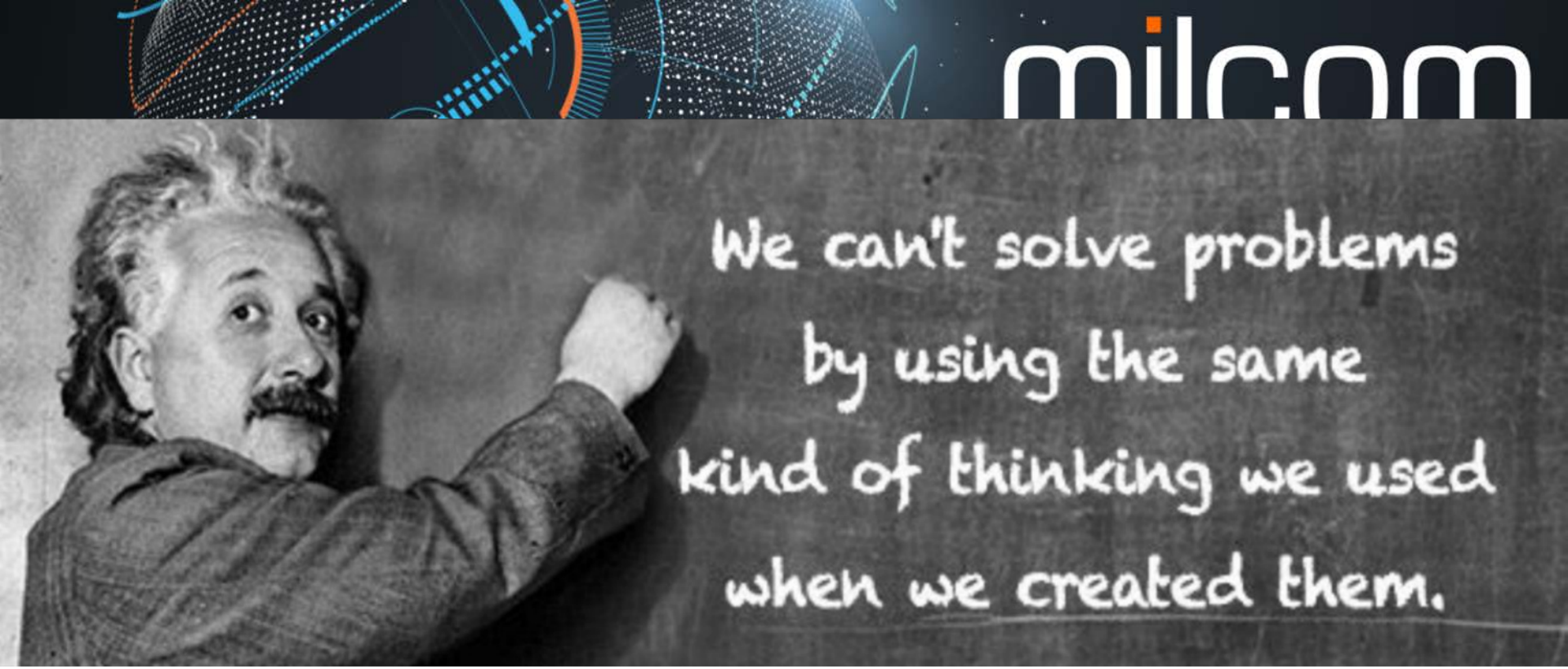
Addressing crypto usability challenges

- Crypto keys and trust policies are all named, secured data
  - They can be fetched by anyone as needed
- Establish well known naming conventions
  - Enable one to construct the names for desired keys and policies
  - Facilitate the definition of security policies through defining the relations between the names of keys and their permitted actions on data (trust schema, see reference 3)
- Automating crypto key management
  - Certificate issuance
  - Automated key generation and distribution for content encryption/decryption (name-based access control, reference 4)
    - Developed solutions for attribute-based encryption

The above concepts will be illustrated in the chat and PLI apps

Takeaway

- One can communicate by requesting named data, *without needing network addresses*
- Fetching named data at network layer is
  - Demanded by new apps and network scenarios
  - enabled by technology advances
- Networking by app defined data names enables NDN
  - Securing data directly →remove dependency on intermediaries
  - Using semantic names of both data & keys to reason security policies, automate crypto management and operations
  - Increasing data availability via
    - host multihoming
    - Multipath forwarding
    - Multicast delivery
    - Pervasive in-network storage
    - Delay/disruption tolerance



NDN as a new Internet protocol architecture to meet the military communication challenges

Further readings

1. An Overview of Security Support in Named Data Networking, IEEE Communications Magazine, November 2018.
2. Opportunities and Challenges for Named Data Networking to Increase the Agility of Military Coalitions *Proceedings of Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations (DAIS)*, 2017.
3. Schematizing Trust in Named Data Networking, ACM ICN 2015
4. NAC: Automating Access Control via Named Data, IEEE MILCOM 2018
5. The Story of ChronoShare, or How NDN Brought Distributed Secure File Sharing Back, IEEE MASS 2015 Workshop on Content Centric Networking

Backup slides

Name confidentiality, double layer encryption

"Realizing a Virtual Private Network using Named Data Networking", ACM ICN 2017

Conclusions and Future Directions

Raytheon BBN Technologies

- Considering the classic IP VPN security question, applied to NDN, we provide evidence that:
  - A relatively straightforward NDN-in-NDN analogy provides all of the standard NDN benefits while gaining much of the needed security for VPNs
  - Most VPN security holes within NDN-in-NDN, resulting from IP and NDN differences, can be solved
  - Some security concerns are difficult, and often require a tradeoff between privacy and scalability
- Future directions:
  - Name obfuscation, balancing privacy and scalability
  - Detailed traffic analysis of NDN-in-NDN
  - Implement an NDN-in-NDN prototype