Towards Data-Centric Battlefields: Named Data Networking Services for Tactical Networks

milcom
Military Communications for the 21st Century
November 12–14, 2019 • Norfolk, VA, USA
Defining Multi-Domain Command and Control

Tutorial Objectives

milcom
Military Communications for the 21st Century
November 12-14, 2019 • Norfolk, VA, USA
Defining Multi-Domain Command and Control

- Identify communication challenges in tactical networks
- Introduce Named Data Networking (NDN)
- Apply NDN to example applications in a notional tactical environment
    - Namespace design
    - Resilient forwarding
    - Data-centric security design
    - Dataset synchronization and support for pub-sub paradigm
    - Integration challenges

Plan for this afternoon

2:00pm Lixia: NDN overview

2:40pm Alex: naming, security in tactical networks

3:30pm: 15min break

3:45pm Lixia: pub-sub, sync

4:00pm Tamer: In-network processing/edge computing

- prioritize caches, forwarding strategies

4:30pm wrapping up

- Alex: Code base and NDN resources available
- Q & A

Named Data Networking (NDN) a new way to communicate

milcom

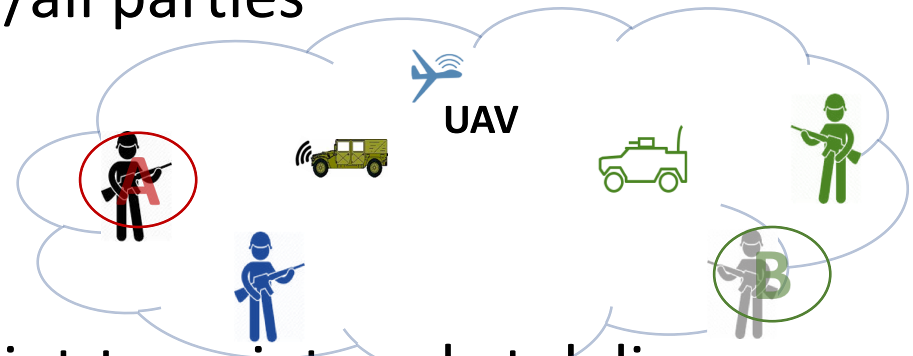
Military Communications for the 21st Century

November 12–14, 2019 • Norfolk, VA, USA

Defining Multi-Domain Command and Control

A fresh look at networking

- What a network does: deliver bits → enabling communication between any/all parties



- How IP accomplishes this: point-to-point packet delivery, A—to—B
  - network = collection of links between adjacent nodes
  - find a path by chaining together a set of nodes and links between A—B
  - Packets flow through the pipe while all the nodes between A—B connected and operational
- Issues: nodes move, links fail, connectivity changes

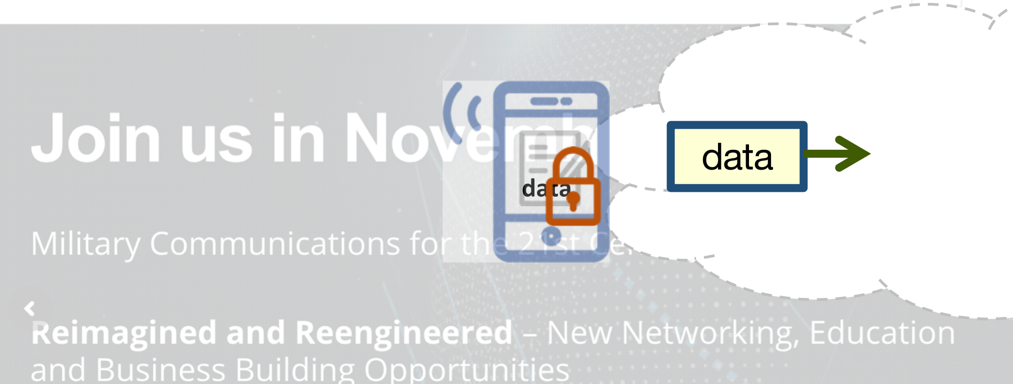
Why a new way

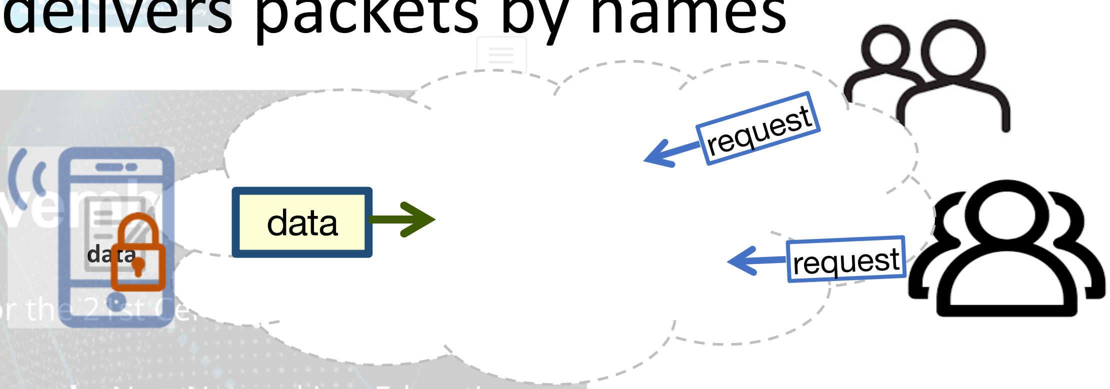

We can't solve problems
by using the same
kind of thinking we used
when we created them.

What’s the new way

milcom
Military Communications for the 21st Century
November 12-14, 2019 • Norfolk, VA, USA
Defining Multi-Domain Command and Control

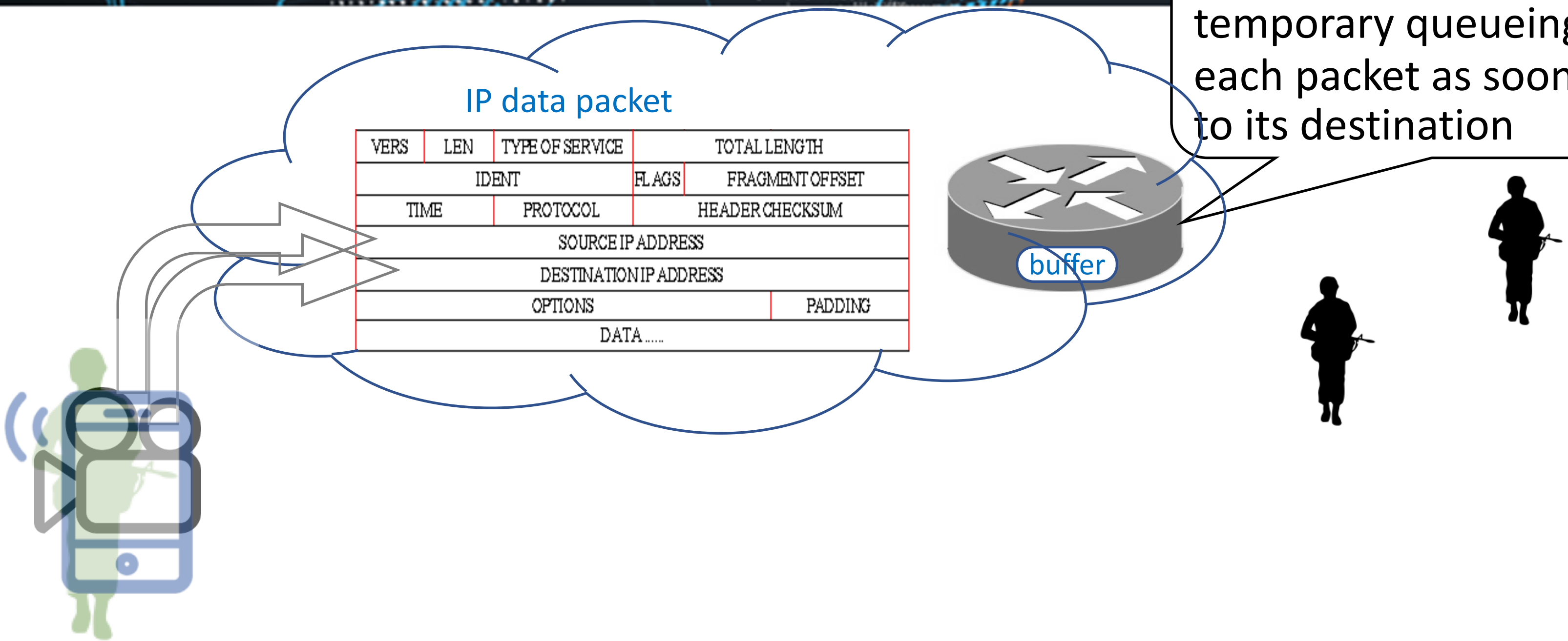
- Delivering desired bags of bits to all the parties who need them – *Named Data Networking*
- Data producers generate named, secured data packets
  - Name data objects by application layer names
    e.g. https://events.afcea.org/MILCOM19/Public/enter.aspx
- Consumers request desired data by names
- Network delivers packets by names





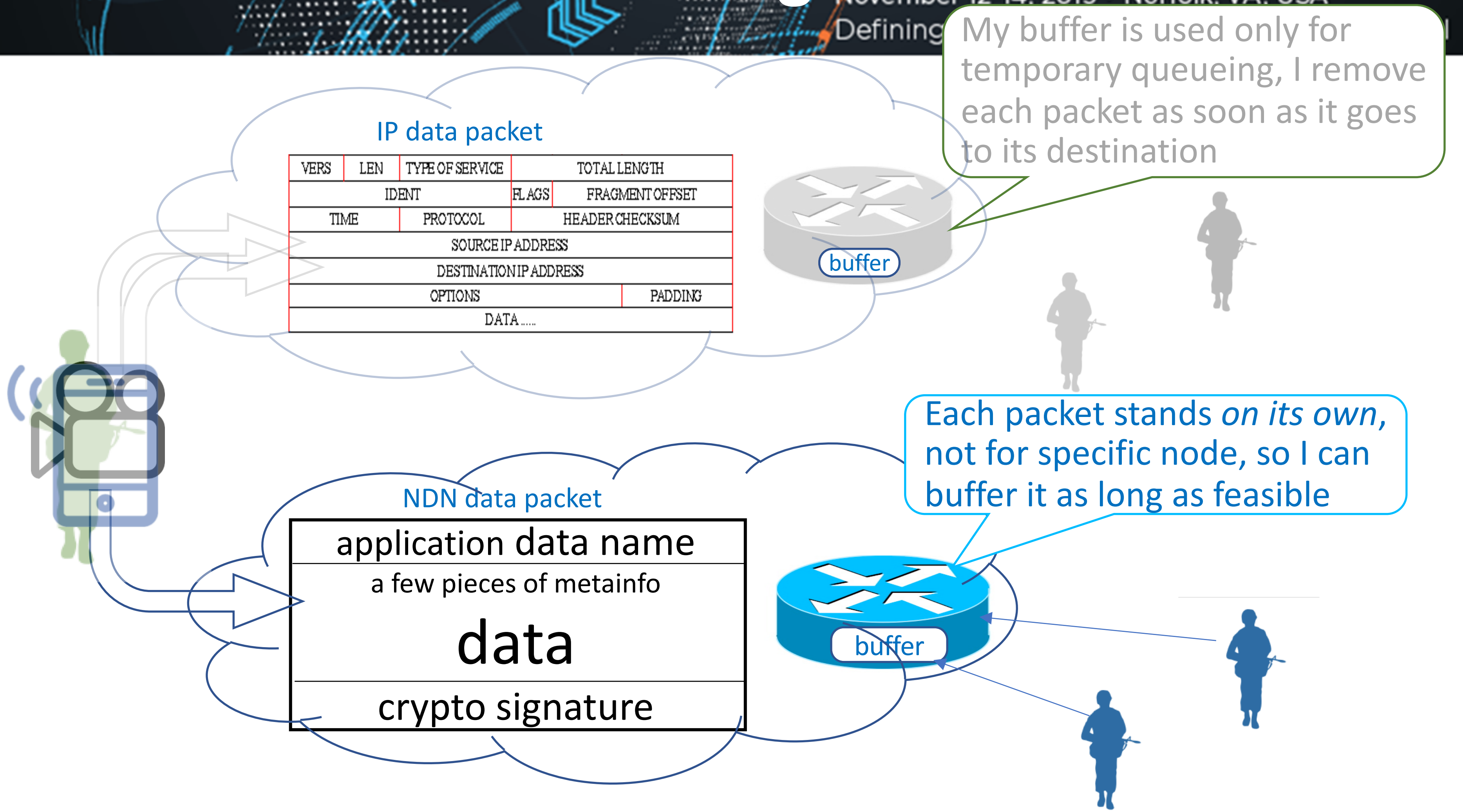
Data consumers verify

IP data delivery by addresses



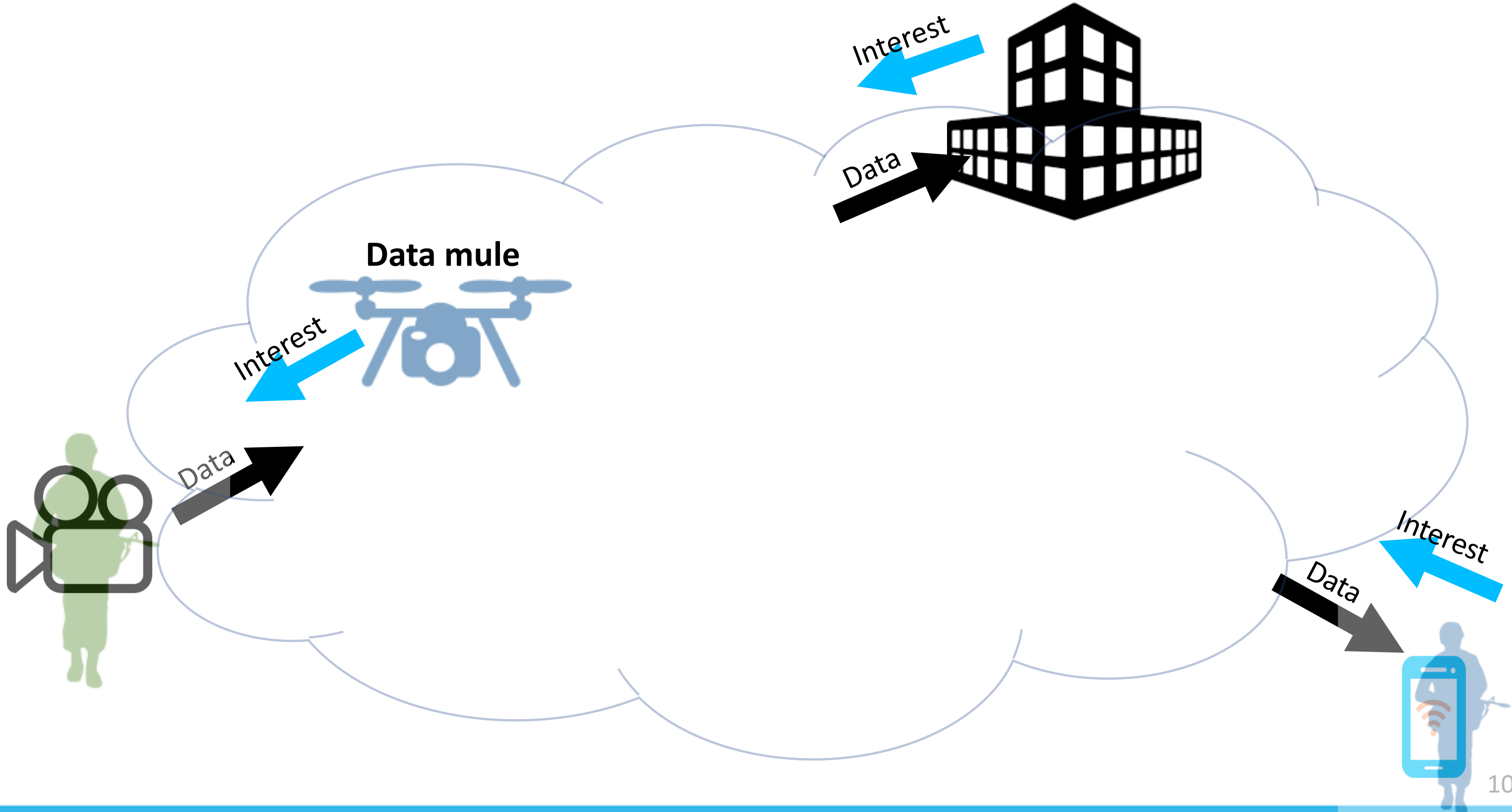
Named, secured data → in-network caching

milcom
Military Communications for the 21st Century
November 12-14, 2019 • Norfolk, VA, USA



Named, secured data enables data muling

Effective communication in face of intermittent connectivity



NDN’s Stateful Forwarding Plane

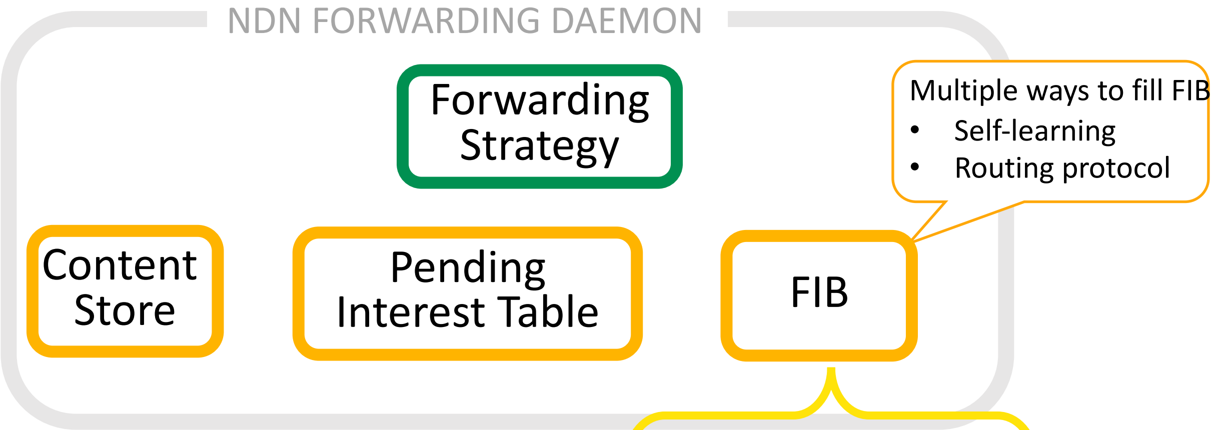
milcom

Military Communications for the 21st Century

November 12–14, 2019 • Norfolk, VA, USA

Defining Multi-Domain Command and Control

NDN’s node model

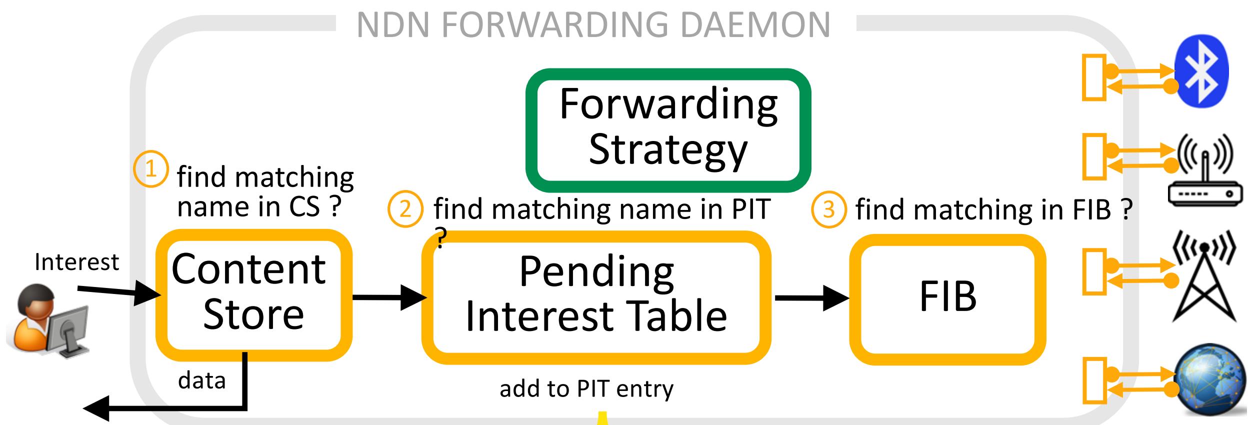


A NFD module resides in every NDN node

name prefix	***next hop***
google.com	A, B
ucla.edu	B,C, D
ucla.edu/cs/lixia	A, B, D,

Breaks Interest looping, can freely use any/all paths

NDN Interest Forwarding

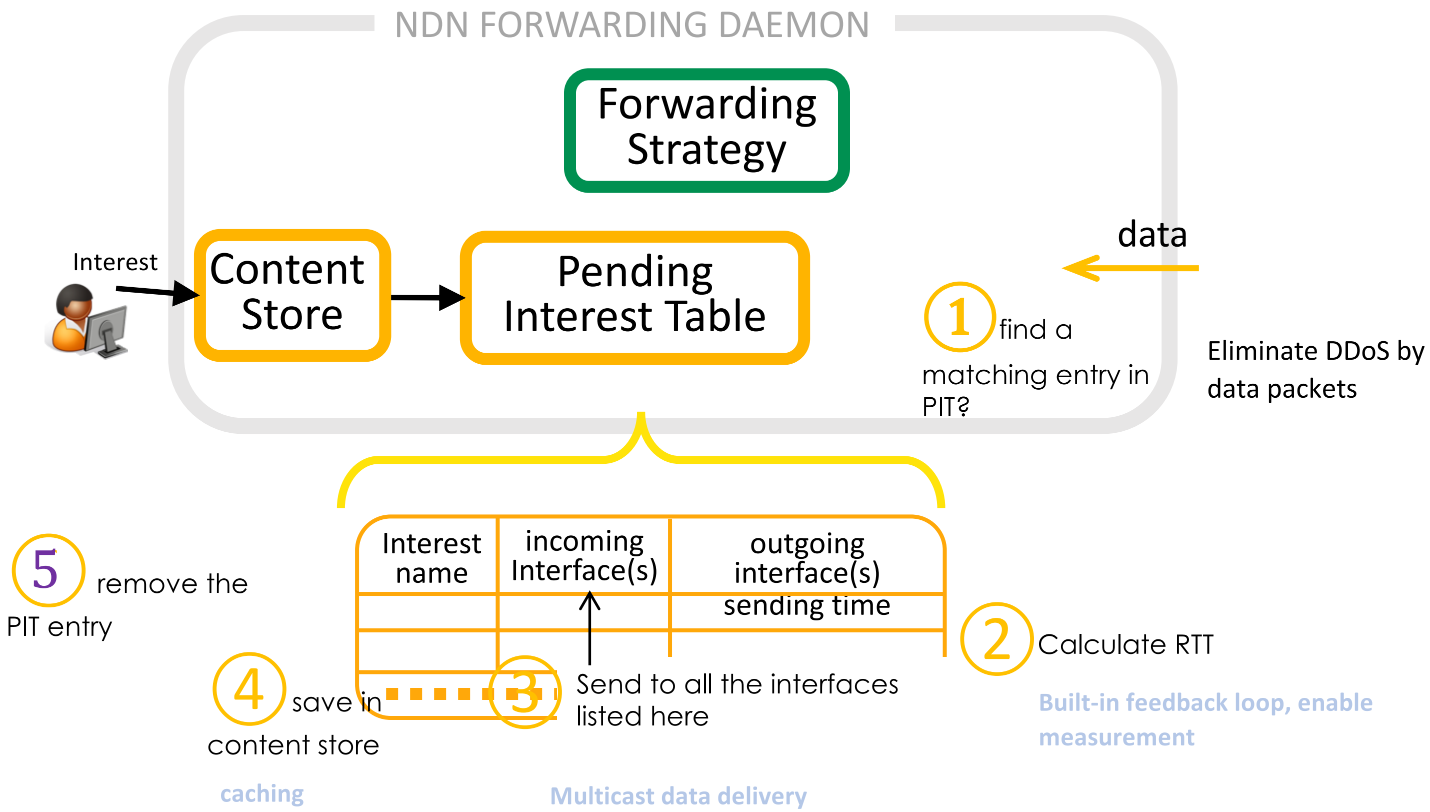


For each PIT entry:

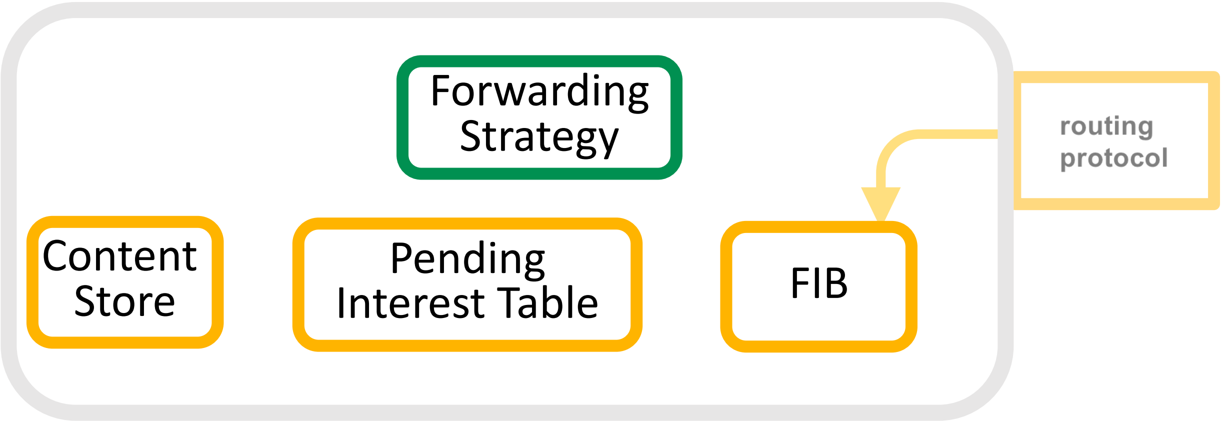
Interest name	incoming Interface(s)	outgoing interface(s) sending time
...		

May forward an interest packet out through one or multiple 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
- Multicast delivery
- Pervasive in-network storage
- Delay/disruption tolerance
- Multipath forwarding

- Can be addressed by IP-based solutions
- Solving each in isolation by amending TCP/IP with special tweaks

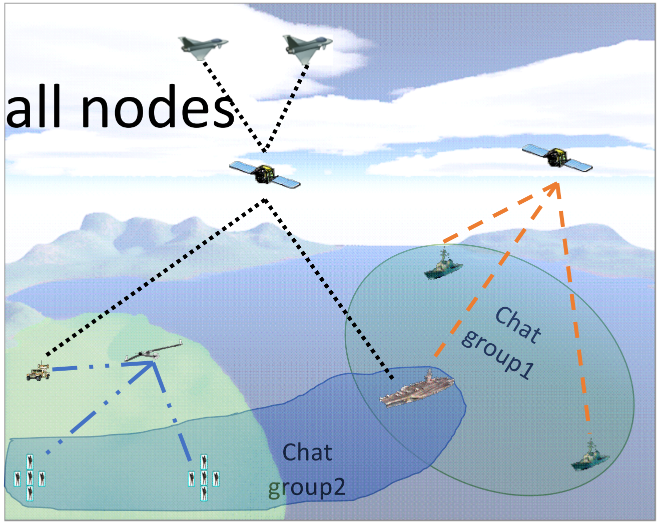
All the above lead to *redundant* means to get data

NDN: making data itself identifiable, independent from its containers or channels

- this requires that data be secured directly

How we secure communication today

- Encrypting point-to-point channels
  - TLS
  - QUIC
- Assumptions
  - synchronized connectivity between two communicating ends
  - All CAs' crypto keys configured into all nodes
- Battlefields need support for delay *and* disruption tolerant (asynchronous) communications
  - No centralized CAs



How NDN secures communications

- The NDN design mandates that all Data packets are secured at the time of production
  - Signed
  - Encrypted as needed
  - Interest packets can be secured as needed
- Enabling secure communication *independent* from data containers or underlying communication channels

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

NDN enables end-to-end data security

End-to-end data authenticity

independent from intermediate communication channels, middle boxes, intermittent connectivity

Security bootstrapping:

- installing trust anchor(s) into all entities
- All data producing entities receive crypto certificates

Network security is conceptually simple

- Data authenticity → Signing (verifying) produced (received) data
  - NDN mandates data authentication
- Data confidentiality → Encrypting data
  - NDN supports name & attribute-based encryption
- Data availability → via redundancy
  - Maintaining multiple copies
  - Trying multiple paths

} native properties built into the NDN forwarding plane

The real security challenges

milcom
Military Communications for the 21st Century
November 12-14, 2019 • Norfolk, VA, USA
Defining Multi-Domain Command and Control

- **Trust management**
  - Today: through centralized commercial ce
    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

    (adopted from "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

- **Easy access to crypto keys and trust policies**: they are all *named, secured data packets*
  - Can be fetched by anyone as needed
- **Establishing naming conventions for keys and policies**
- **Naming keys in a way to simplify the definition of security policies** via the relations between names of keys and their permitted actions
  - *trust schema*, see reference 3
  - Automated key generation and distribution for content encryption/decryption
    - *name-based access control*, with attribute-based encryption, reference 4

Takeaway

- **A new way to communicate**: 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 data & keys to reason security policies**, automate crypto management and operations
  - **Increasing data availability** via
    - host multihoming, multipath forwarding, multicast delivery, in-network storage to support delay/disruption tolerance

Further readings

milcom
Military Communications for the 21st Century
November 12-14, 2019 • Norfolk, VA, USA
Defining Multi-Domain Command and Control

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 Information Centric Networking Conference 2015

4. NAC: Automating Access Control via Named Data, IEEE MILCOM 2018