Future Networking via Named Secured Data

Lixia Zhang, UCLA

Semiconductor Research Corporation
Workshop on New Trajectories for Communication

February 11, 2020

Future Networking

- New application drivers
  - Mobile
  - P2P, V2V, M2M
  - Embedded

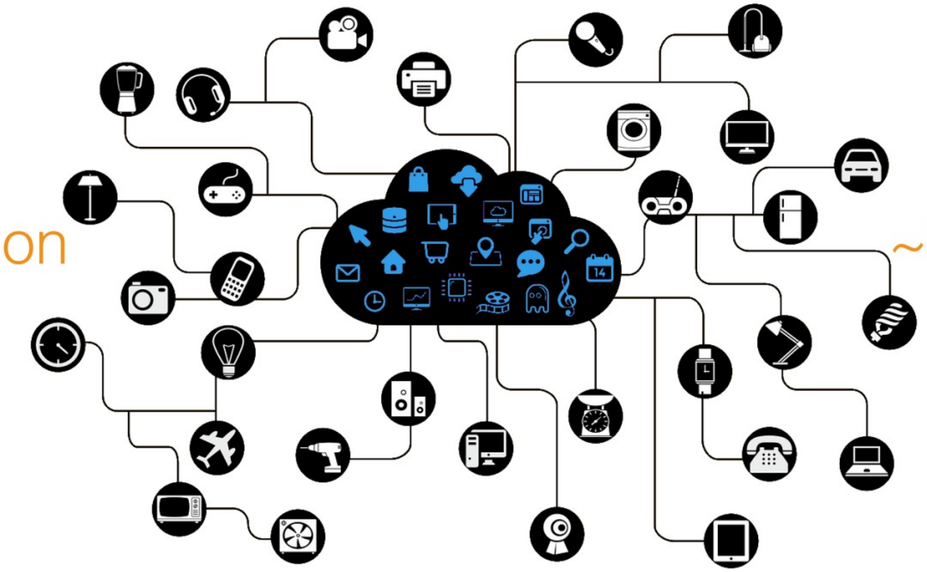
Information-Centric/Named Data Networking:

- Naming data instead of data containers
  - Using app names, removing address management
- Securing data directly
- Fully utilizing wireless broadcast media

- New communication needs
  - Wireless, *infrastructure-free* communication
  - Scalable communication
  - Secure communication
    - *Particularly important for communications with random encounters*

New challenges

- Networking *unlimited* number of (potentially mobile) computing devices
- Auto-X (autoconfiguration, auto-updates)
- **Security**



2016

6 - 9 Billion

2020

~30 Billion

https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

“Understanding the Mirai Botnet” USENIX Security 2017 paper

- “In contrast to desktop and mobile systems... IoT devices are much more heterogeneous and, from a security perspective, mostly neglected.
- **“Automatic updates** — already canonical in the desktop and mobile operating system space— .... require cryptographic primitives for resource-constrained devices and building PKI infrastructure to support trusted updates.
- ..... Over time, the risk that these devices pose to the Internet commons will only grow unless taken offline.”

The Bottomline

“We find that while IoT devices present many unique security challenges, Mirai’s emergence was primarily based on the absence of security best practices in the IoT space, which resulted in a fragile environment ripe for abuse.”

- Are you talking device problem, or communication problems?

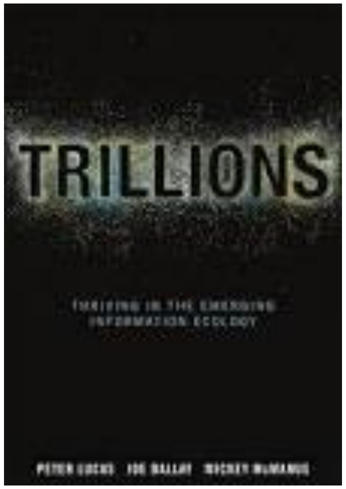
→ These two problems no longer separable in cyberspace made of trillions of interconnected devices

Challenges today *which have no established solutions*

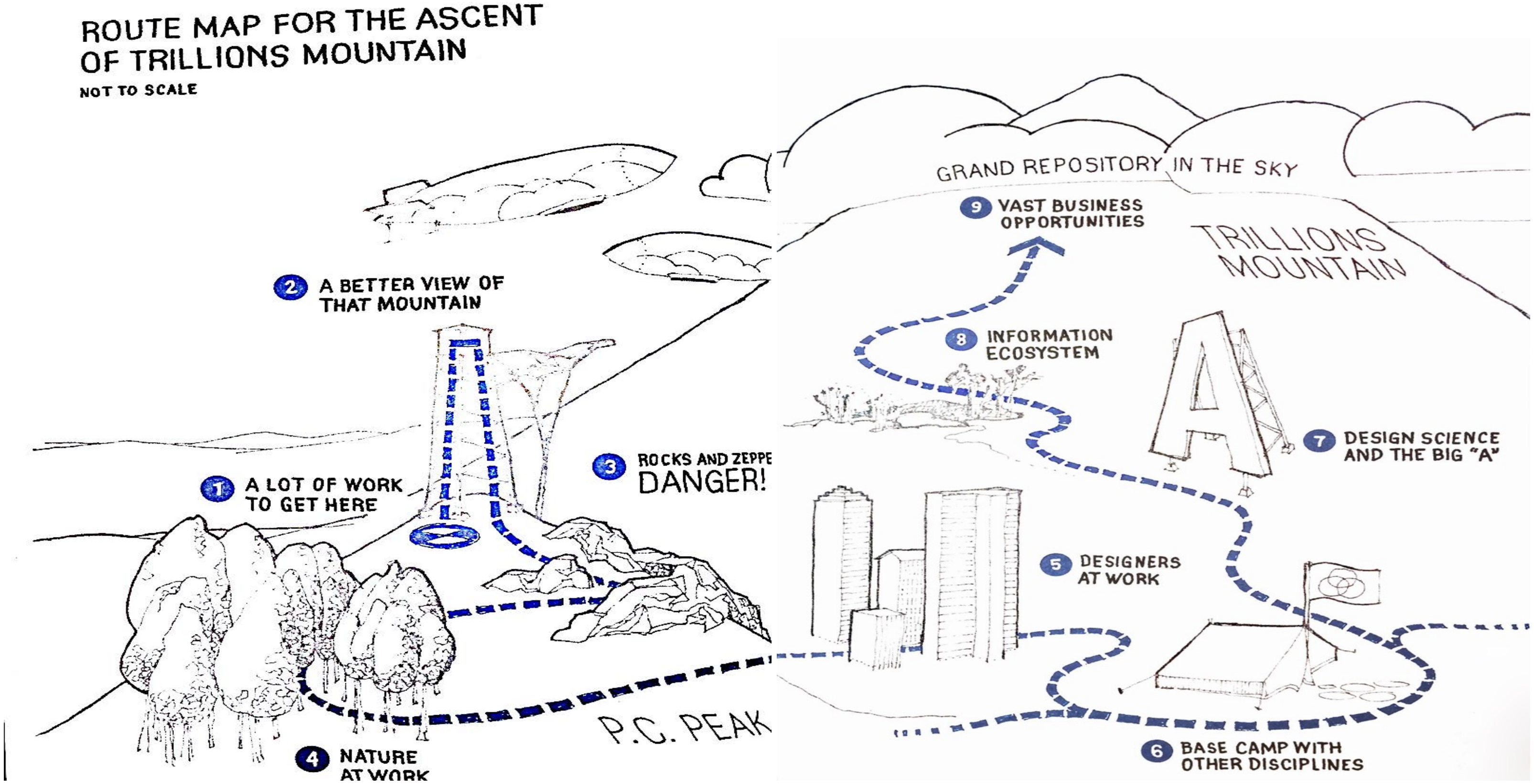
"What challenges do we have today which have no known solutions and need research focus?"

- **Security**
- **Security**
- **Security**
  - to enable networking unlimited number of (potentially mobile) computing devices

Trillions: Thriving in the Emerging Information Ecology

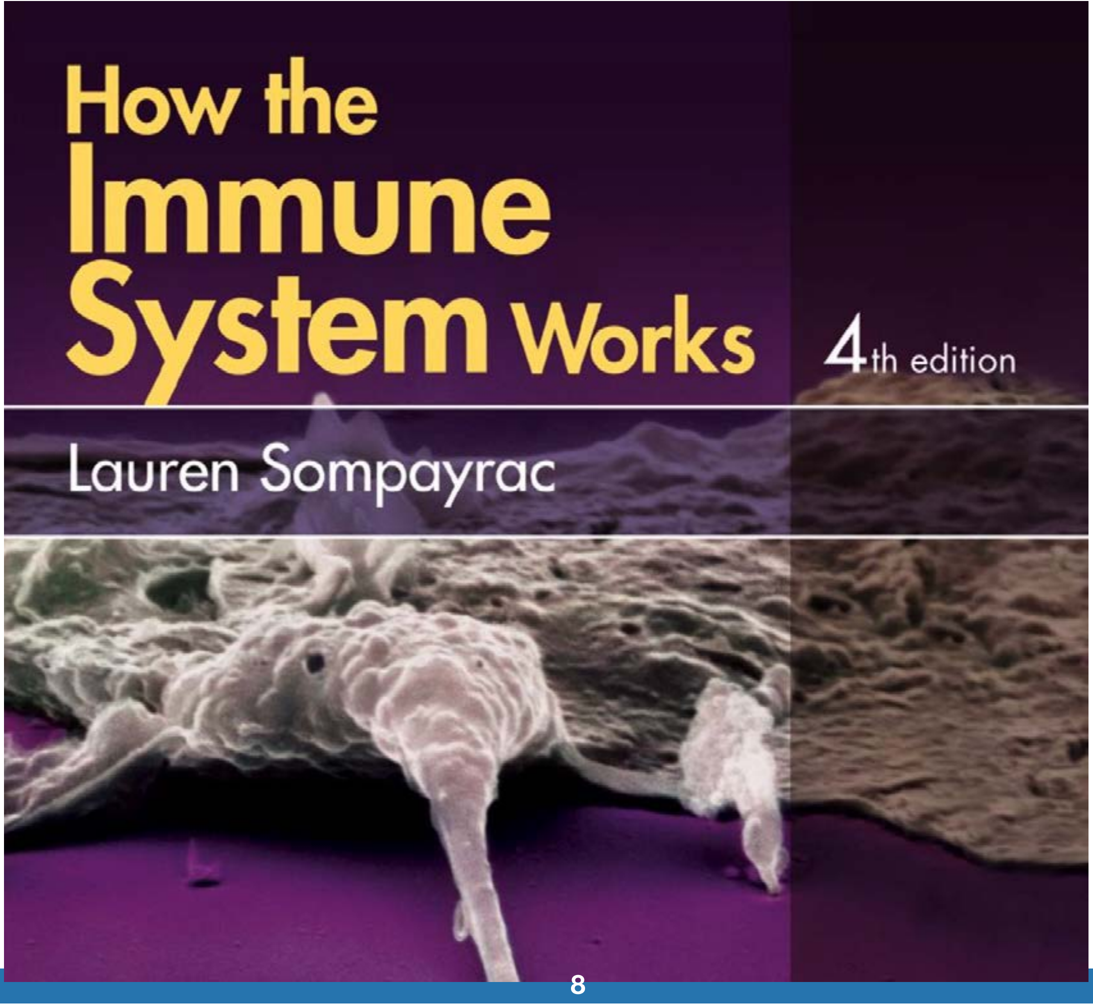

TRILLIONS
THRIVING IN THE EMERGING INFORMATION ECOLOGY
PETER LUCAS JOE BALLAY MICKEY McMANUS

By Peter Lucas,
Joe Ballay, and
Mickey McManus
2012


ROUTE MAP FOR THE ASCENT
OF TRILLIONS MOUNTAIN
NOT TO SCALE
GRAND REPOSITORY IN THE SKY
TRILLIONS MOUNTAIN
1 A LOT OF WORK TO GET HERE
2 A BETTER VIEW OF THAT MOUNTAIN
3 ROCKS AND ZEPPE DANGER!
4 NATURE AT WORK
5 DESIGNERS AT WORK
6 BASE CAMP WITH OTHER DISCIPLINES
7 DESIGN SCIENCE AND THE BIG "A"
8 INFORMATION ECOSYSTEM
9 VAST BUSINESS OPPORTUNITIES
P.C. PEAK
A

Climbing the trillion mountain requires descending down from where we are today (requiring a fundamental change of today’s way of networking

Security: Learn from bio systems

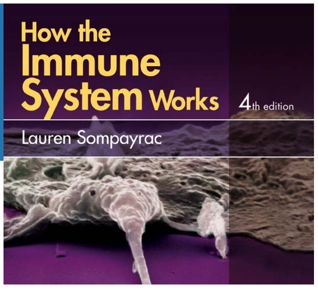


How the Immune System Works

4th edition

Lauren Sompayrac

Learning from bio systems



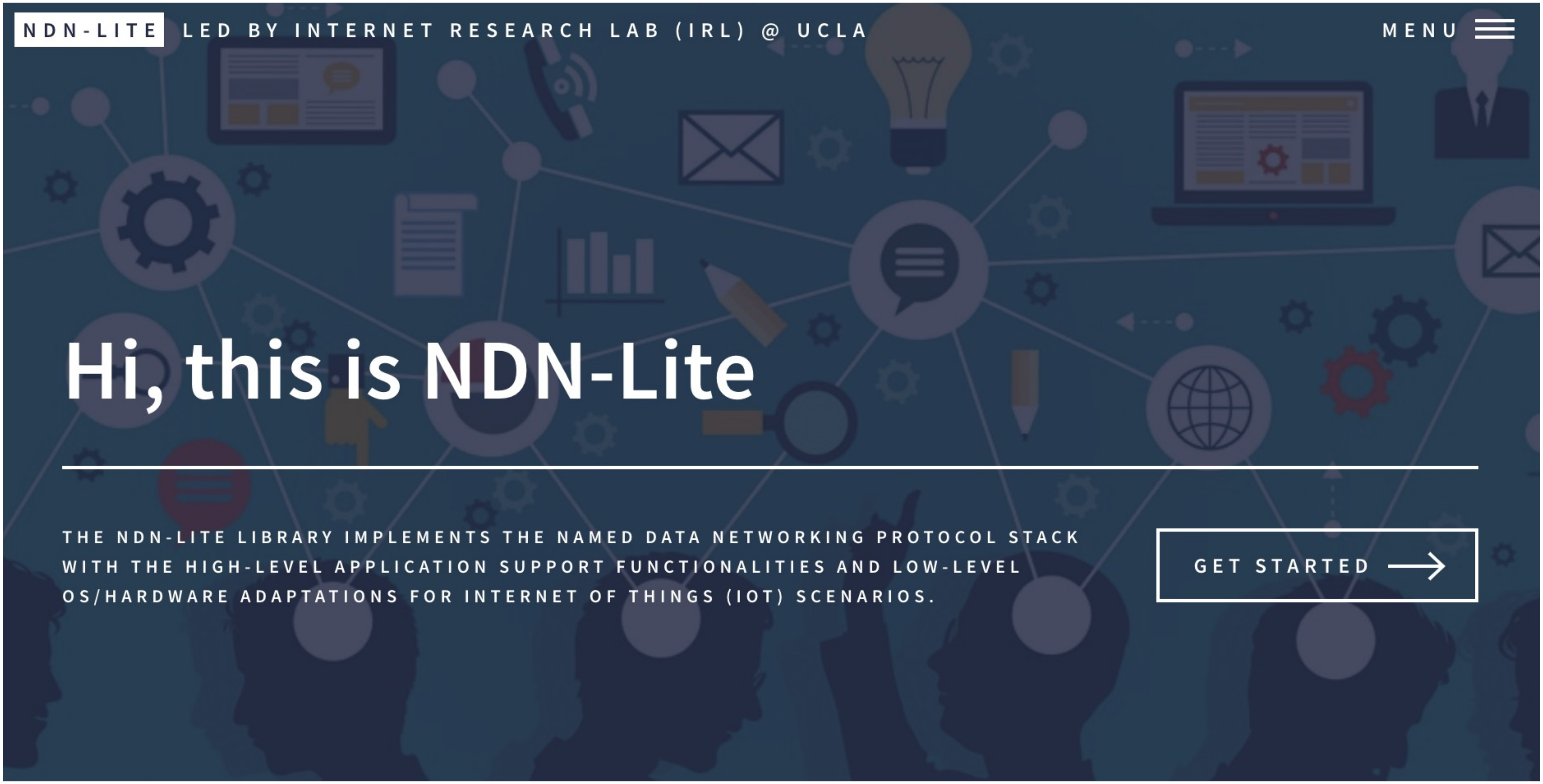
- ***The innate immune system***
  - Any invader that breaches the physical barrier of skin or mucosa is greeted by *the innate immune system* – our second line of defense. Immunologists call this system “innate” because it is a defense that all animals just naturally seem to have.
- ***The adaptive immune system***
  - About 99% of all animals get along just fine with only natural barriers and the innate immune system to defend them. However, for vertebrates like us, Mother Nature laid on a third level of defense: the adaptive immune system. This is a defense system that actually can *adapt* to protect us against almost any invader...

Taking 1st step toward innate immunity in cyberspace

The basic idea in Information-Centric/Named Data Networking (NDN):

- Each of all entities in a system should obtain
  - a semantically meaningful name
    - The name can reflect the context
    - Produce Key(s)
  - Trust anchor
    - which then issues certificate(s) and install security policies
- Securing data at production: sign, encrypt if needed
  - So that all data exchanges are authenticatable
- Communication by requesting named, secured data
  - data = data / apps / keys / policies / profiles

A demoware prototype: https://ndn-lite.named-data.net/



NDN-LITE LED BY INTERNET RESEARCH LAB (IRL) @ UCLA

Hi, this is NDN-Lite

THE NDN-LITE LIBRARY IMPLEMENTS THE NAMED DATA NETWORKING PROTOCOL STACK WITH THE HIGH-LEVEL APPLICATION SUPPORT FUNCTIONALITIES AND LOW-LEVEL OS/HARDWARE ADAPTATIONS FOR INTERNET OF THINGS (IOT) SCENARIOS.

A Wish List for Supporting Future Communications

- Hardware pseudo random number generator
- TPM to safely keep private keys
- Hardware crypto accelerator
  - like what this chip does:

    https://www.microchip.com/wwwproducts/en/ATECC608A
- Time & clock support

For resource constrained devices

Designing Security *into* Cyberspace

Lixia Zhang

Semiconductor Research Corporation
Workshop on New Trajectories for Communication

February 11, 2020