Hybrid Event
Hosted by
NIST

NAMED DATA NETWORKING COMMUNITY MEETING

March 6
March 7
2024

Panel Abstracts

Panel 1: Building an Open-Source Ecosystem around NDN

After years of strong research activity and community building, the NDN team is ready to explore the creation of an Open-Source Ecosystem (OSE) to empower the user community and drive further innovation. There is a significant difference between running a research project (as the NDN team has done so far) and creating, nurturing, and managing an OSE. An OSE poses challenges that are not present in a research project, such as establishing a guiding vision, developing the appropriate governance structure, expanding and coordinating a productive community of developers, and establishing an effective management organization. This panel brings together experts from industry and academia to discuss the exciting opportunities and unique challenges associated with this transition.

Panel 2: From Local-First to Fully Decentralized Applications

There exist many ongoing efforts aiming to steer Internet applications towards decentralized realizations; one such work was presented at last IETF "Local-first software, resilient and secure collaboration". This panel will show case examples of decentralized designs, articulate their commonalities and differences, share experience from the different efforts, and identify remaining challenges in building secure, resilient, and easy to use and deploy codebase with well-defined API to facilitate new generations of decentralized apps.

Panel 3: Present and Future of Network Security Framework

Network security remains one of the biggest challenges on the Internet. Currently, we have several scattered solutions at different levels providing a level of security and privacy. This panel aims to identify the scope of today's solutions, current strengths, potentially missing functions, and discuss a potential for a comprehensive security framework for future security needs.

Presentation Abstracts

Low-Earth-Orbit Satellite Constellations and Named Data Networking

Sirapop Theeranantachai (UCLA)
Beichuan Zhang (The University of Arizona)
Lixia Zhang (UCLA)

Large low-earth-orbit (LEO) satellite constellations such as Starlink can provide Internet access to users around the globe and low-latency communication over long distance. To achieve their full potential would require scalable and efficient routing and forwarding using inter-satellite links (ISLs). This talk will discuss the basic characteristics of LEO constellations, the implications on network design, and the potential and challenges of applying NDN to such a network environment.

NDN for Data-Intensive Science Experiments: Progress and Future Directions

Edmund Yeh (Northeastern University)
Harvey Newman (Caltech)
Lixia Zhang (UCLA)
Jason Cong (UCLA)
Susmit Shannigrahi (Tennessee Tech)

The NDN for Data-Intensive Science Experiments (N-DISE) project focuses on designing and implementing a new, highly efficient and field-tested data distribution, caching, access and analysis system for the Large Hadron Collider (LHC) high energy physics (HEP) network and other major science programs. In this talk, we review the progress of the N-DISE project over the past three years, and discuss future directions.

NDN based CNI for Kubernetes: Unlocking Secure, Smart, and On-Demand Communication

Tushar Sood (Tata Communications)
Mohit P Tahiliani (National Institute of Technology Karnataka, Surathkal)

This work-in-progress introduces an innovative Named Data Networking (NDN) based Container Networking Interface (CNI) architecture to address the evolving challenges in containerized workload communication within cloud and edge computing environments. By leveraging NDN, we intend to offer enhanced security, improved efficiency, and dynamic intelligence, presenting a promising alternative to existing solutions. Through a comprehensive analysis, we aim to highlight the architectural advantages of NDN-CNI over conventional options, particularly emphasizing its benefits in pod-to-pod, pod-to-service, and external-to-service communications. Although NDN is still not widely adopted, its integration as an overlay on existing IP infrastructure demonstrates promising potential, especially in intra-cluster deployments. We intend to facilitate pure NDN-based communication within nodes and NDN overlay communication between nodes, ensuring compatibility and scalability. We believe that integrating NDN seamlessly into Kubernetes clusters promises heightened security, efficient routing, dynamic service discovery, and simplified ingress configuration, paving the way for a new paradigm in Kubernetes communication.

Data-oriented, Decentralized, Daring: Opportunities and Research Challenges for an Information-Centric Web

Dirk Kutscher (HKUST)

Research and development in ICN has led to different communication patterns such as Sync and API implementations such as CNL. It is now time to think about how to leverage Information-Centric principles for providing better foundations for hypermedia applications in the future web. This talk will talk about how ICN could possibly help, what could be fruitful future research directions, and why web3 and dweb are not the answer.

Naming in Named Data Networking

Lixia Zhang (UCLA)

Names play a fundamental role in the NDN design. This talk elaborates the three important roles of names in developing applications running over NDN, and discusses the role of DNS names in NDN data names.

Naming a Microverse of One's Own

Jeff Burke (UCLA)

This lightning talk uses the example of a "microverse" to introduce naming challenges and potential differentiating strategies in NDN. Specifically, it discusses the opportunity to support interoperability of secure web objects that is protocol- and application-independent in the conventional sense of those terms.

Analysing NDN and MQTT performance for Industrial IoT Scenarios

Parth Anand (fortiss)
Rute C. Sofia (fortiss)

In Industrial IoT, Publish-Subscribe approaches such as MQTT or OPC-UA are being heavily used to provide support to data exchange across environments such as shop-floors, warehouses, etc. Host-based IP PubSub approaches are not fully suitable to IIoT environments, as they are not data-oriented but host-oriented. IIoT environments would benefit from a decentraliised communication pattern, data-oriented, to support publishers and subscribers in a many-to-many asynchronous data exchange, which ICN/NDN provides. This talk debates on the advantages of NDN in comparison to MQTT as an example of a broker-based PubSub approach, for IIoT environments. We have evaluated NDN against MQTT on our open testbed lab involving embedded devices, and present a performance evaluation of NDN against MQTT in terms of latency (time to completion of tasks), and messaging overhead. We will also present the current steps we are developing in the testbed towards an analysis of NDN vs. MQTT involving mobile embedded robots.

Deadline-Aware Named Data Networking for Time-Sensitive IoT Applications

Afia Anjum (University of Texas at Arlington)
Sena Hounsinou (Metro State University)
Habeeb Olufowobi (University of Texas at Arlington)

Named Data Networking (NDN) has evolved as a networking model that can facilitate Internet of Things (IoT) applications by providing a name-based communication model, in-network caching, and inherent support for data-centric security. However, despite the benefits, the best-effort NDN cannot offer the deterministic data delivery required by safety-critical IoT applications. This paper proposes a novel deadline-aware NDN protocol that utilizes a critical deadline first scheduler to prioritize traffic based on the approaching deadline. Evaluation results show that the proposed deadline-aware NDN can meet the communication needs of time-sensitive IoT applications.

Developing a Mobile Application for IoT using Named Data Networking (IoT-NDN) with FIWARE

Ahmed M. Hail (University of Lübeck)

This work presents the development of a mobile application for IoT over Named Data Networking (IoT-NDN) using Flutter, NDN, and NFD, integrated with FIWARE. The system utilizes ESP32 DevKits as sensor nodes, running NDN, to facilitate seamless communication within the network. The primary objective is to build a testbed where sensor nodes can be controlled via the mobile app, enabling efficient data exchange and management. Key functionalities include sensor data transmission to FIWARE for storage and analysis. Through the integration of NDN principles and the utilization of Flutter for app development, the project aims to bridge the gap between IoT networks and user-friendly mobile interfaces. By leveraging FIWARE integration, the system enhances scalability and interoperability, paving the way for robust IoT solutions. This work provides insights into the design, implementation, and deployment of the IoT-NDN mobile application, offering valuable contributions to the field of IoT and NDN integration.

Updates on the NDN Testbed

Varun Patil (UCLA)
Tianyuan Yu (UCLA)
Lixia Zhang (UCLA)

The global NDN Testbed is a real NDN deployment spanning four continents. We discuss the current status of the testbed topology and plans for expansion, recent changes to the testbed and how you can utilize the testbed for your research, along with ongoing efforts for improving the testbed.

Workspace: A Data-Oriented, Decentralized Collaboration Web App

Tianyuan Yu (UCLA)
Xinyu Ma (UCLA)
Varun Patil (UCLA)
Yekta Kocaoğullar (UCLA)
Lixia Zhang (UCLA)

Remote collaborations are one of the popular applications on today's Internet. However, the existing collaborative apps are all hosted on the cloud servers, largely owned by a small number of providers. In these apps, although contents are generated by end users, they can only collaborate through

connections to clouds. This work explores an alternative path to building collaborative applications by making use of named, secured Web Objects (SWO). Inspired from the original data-orientation vision of web, we developed a decentralized collaborative application dubbed Workspace. Workspace users establish trust relations among each other, secure their data productions directly, exchange SWO through rendezvous points, and support users with intermittent connectivity.

Distributed User-Centric mHealth Data-Sharing Application Running on NDN Testbed

Adam Thieme (The University of Memphis)
Suravi Regmi (The University of Memphis)
Lan Wang (The University of Memphis)

Mobile health (mHealth) data collection and sharing have made significant strides, yet challenges persist in achieving fine-grained contextual access control and facilitating real-time data sharing. To address these challenges, we introduced an enhanced version of mGuard, a distributed NDN-based data sharing system. This iteration of mGuard focuses on a user-centric approach, enhancing the user interface (UI) and streamlining access control policies for improved usability.
The demonstration will showcase the distributed nature of mGuard, to ensure secure data sharing across networks. Additionally, we will present the upgraded UI, featuring more fine-grained policies and an intuitive graphical interface enabling consumers to subscribe/unsubscribe to distributed data streams and retrieve corresponding information. Leveraging the NDN testbed, live demonstrations will illustrate the integration of these enhancements within the mGuard framework.

A New API in Support of NDN Trust Schema

Tianyuan Yu (UCLA)
Xinyu Ma (UCLA)
Yekta Kocaoğullar (UCLA)
Lixia Zhang (UCLA)

The decade-long experiences from developing applications over Named Data Networking (NDN) have taught us the importance of well-designed libraries that offer support to application developers to support data security. NDN trust schema provides a critical component in the NDN security support, however its implementation and support only started receiving significant attention in recent years. This work provides a summary of the existing API support for trust schema, and takes a step forward by developing a new trust schema API, named Envelope. Envelope addresses the application requirements by offering comprehensive trust schema functionalities, an easy-to-write schema language, and an extensible design.

VerSec Schema Visualization

Varun Patil (UCLA)
Lixia Zhang (UCLA)

Writing Trust Schema can be a challenging task as they grow more complex. This demo showcases NDN-Play's abilities to help write and visualize VerSec schema in the browser.

CLedger: A Secure Distributed Certificate Ledger via Named Data

Tianyuan Yu (UCLA)
Xinyu Ma (UCLA)
Varun Patil (UCLA)

Lixia Zhang (UCLA)

Named-Data Networking (NDN) is a novel network that secures network communication by fetching semantically named and secured data. All data packets in NDN are signed by producers and verified by data consumers. Therefore, it is vital to have producers' certificates available all the time. In this paper, we describe the design of CLedger, a secure distributed certificate ledger, to ensure certificate availability in NDN. CLedger logs certificate records in an immutable Directed Acyclic Graph (DAG) structure and replicates the DAG among a set of distributed loggers. We implemented CLedger using NDN's pub/sub API, and evaluated our design through an emulated deployment setting. Our initial evaluation results show that CLedger is effective, efficient, and resilient to failures.

NDN for AI: Starting From A Data-Centric Collective Communication

Teng Liang (Peng Cheng Laboratory)
Beichuan Zhang (The University of Arizona)

Generative AI may depend on large models, which require a robust and scalable system to collaborate massive computing resources. Such systems can be complicated to achieve high performance built on top of the end-to-end architecture. NDN provides a data-centric architecture, which is potentially more suitable for such systems, given its architectural benefits demonstrated in other scenarios. In this presentation, I will explain the design of ndn-allreduce, a data-centric collective communication, which is the first step of NDN for AI. Additionally, potential benefits and research directions will be discussed.

Hydra: An NDN based federated storage system for multi-organizational science data

Susmit Shannigrahi (Tennessee Tech)
Lixia Zhang (UCLA)
Alex Afanasyev (FIU)

We provide updates on the Hydra project that aims to build a federated repository over NDN. We plan to show our deployment on FABRIC and also plan to do a demo of the prototype.

Traffic Measurement on the Global NDN Testbed

Davide Pesavento (NIST)
Junxiao Shi (NIST)
Sankalpa Timilsina (Tennessee Tech)
Susmit Shannigrahi (Tennessee Tech)
Lotfi Benmohamed (NIST)

High-quality network traffic measurements from realistic network deployments are crucial to analyze and better understand emerging network technologies for the purpose of maturing them. However, achieving this measurement goal for the NDN protocol remains a challenge mainly due to the lack of real-world deployments. At the ACM ICN 2023 conference, we announced the first non-synthetic dataset of NDN traffic traces, captured directly from the actual routers of the official NDN testbed, and made it openly available to the research community. In this talk, we will provide an update on our ongoing trace collection project, which recently grew to cover the entire global testbed, and discuss potential next steps.

NDN Service Framework (NDNSF)

Tianxing Ma (University of Memphis)
Lan Wang (University of Memphis)

NDNSF is a secure service framework that offers encrypted service communication and permission management between service providers and users. In NDNSF, a service controller will be responsible for automated key distribution and service permission management during bootstrap. However, secure communication and permission control can be achieved without the controller after bootstrap. The service request/response messages' names are published via a sync protocol. The message data is encrypted using NAC-ABE and then later served/stored using an NDN repository. When a service provider receives a Service Request from a new user, it will initiate a Permission Challenge by sending an encrypted token. If the service user is authorized to use the service, they can decrypt the token and respond with a Permission Challenge Response. Later, the service provider will start processing the request and publish a Service Response Message if the Permission Challenge Response is valid.
For the time being, we will bootstrap manually and demonstrate the entire Service Request/Response/Permission-Challenge/Permission-Challenge-Response process in the demo.

Edge Challenges with Data Management and Networking

Jeff White (Dell Technologies)

Edge is an accelerating new computational architecture deployment framework that is largely driven by the emergence of data intensive applications requiring time sensitive processing such as AI/ML, Environmental Simulation, XR/VR, Industry 4.0, etc. This presentation explores the technical challenges of data management in an Edge context.