Hybrid Event
Hosted by
NIST

NAMED DATA
NETWORKING
COMMUNITY
MEETING

March 2
March 3
2023

Presentation Abstracts

Resilient Edge Ecosystem for Collaborative and Trustworthy Disaster Response (REsCue): An Information-Centric Approach,

Abde Mtibaa (UMSL)

We address networking and security challenges in next generation public safety and disaster response networks, where mission-critical emergency operations (e.g., search and rescue) need to be performed with limited surviving infrastructure, potentially augmented with diverse devices deployed by first responders. These mission-critical operations are performed in a challenging environment and can only be effective if the fundamental security and architectural challenges specific to them are addressed: (i) effective integration of diverse autonomous networks (e.g., utilities and smart homes) into a resilient, cooperative, and secure network-of-networks; (ii) a system for supporting network operations during broad disruptions including the enforcement of access control to data and services, and (iii) efficient verification of untrusted users' communications. The project's broader significance and importance are two-fold: (i) providing new research outcomes in networking, near-user computing, low-latency wireless communications, and cybersecurity, leading to the creation of disruption-tolerant networks, whose use extends beyond effective disaster/emergency response to other applications, such as rural networking and distributed manufacturing; and (ii) contributions to a diverse workforce through recruitment and training of a diverse student population.

The project identifies the fundamental architectural and security challenges in fragmented networks, such as seamless multi-modal communications, resilient and verifiable computing, and trust management, and addresses them for viable deployment in disaster-response scenarios. We use the Named-Data Networking (NDN) architecture as the underlying communication substrate to promote semantics-based communication and achieve seamless compute/data sharing. We design a generic blueprint to design an edge-centric, trustworthy, and resilient named data networking architecture to investigate foundational resilience challenges including engendering trust without a centralized certificate authority in a network stitched-together from independent network fragments, providing flexible and revocable access control and authorization for data/services, and ultra-reliable low latency wireless communications in challenging environments.

In-vehicle networking with NDN

Zach Threet (Tennessee Tech)
Susmit Shannigrahi (Tennessee Tech)
Christos Papadopolos (University of Memphis)

In-vehicle networks are increasingly adapting multiple network technologies such as CAN, FlexRay, SOME/IP, and more. At the same time, the community is moving towards Automotive Ethernet for high-bandwidth, low latency communication. Integrating so many different networking technologies can quickly become cumbersome. We expect NDN to provide several benefits in such a scenario. NDN adds naming standardization, data provenance, security, and improve interoperability between different ECUs and networks.

To test such complex in-vehicle networks, we have built a working benchtop testbed with Raspberry PIs, CANHats, and Ethernet switches that emulates a real vehicle. The testbed allows us to send and receive traffic between ECUs, develop and test new protocols, and replay real-world vehicular datasets to evaluate protocol properties and security primitives. In this talk, we demonstrate the capabilities of this testbed by replaying a real-world vehicular traffic trace between ECUs. We also demonstrate the idea of NDN gateways that can act as bridges between various automotive segments. Finally, our work shows the feasibility and advantages of a data-centric architecture for in-vehicle networks.

Secure Truck-Tractor to Trailer Communications based on NDN

Ahmed Elhadeedy (Colorado State University)
Jeremy Daily (Colorado State University)

Autonomous truck-trailer communication requires high bandwidth and low latency when sensors are added to trailer to increase the capabilities of the self-driving software in the truck such as reverse driving. Legacy communications use powerline carrier communications at 9600 baud, so upfitting existing trailers for autonomous operations will require adopting technologies like Ethernet or a wireless harness between the truck and the trailer. This would require additional security measures and architecture, especially when pairing a tractor with a trailer.

In this paper, we discuss a secure NDN-based architecture for tractor-trailer and cloud communication links that covers the process of pairing a truck with a trailer and secure ECU communication during operation. We compared NDN over UDP with a well-established automotive networking protocol, Scalable service-Oriented MiddlewarE over IP (SOME/IP) over UDP in the case of multicast, where 1 multicast device is acting as a trailer ECU transmitted sensor data and 3 other unicast devices acting as receivers to get the sensor data. Preliminary results indicate that NDN has a similar performance with additional 4 milliseconds latency when compared to SOME/IP performance due to the additional steps NDN goes through.

NDN is capable of meeting security needs for tractor-trailer ECUs intra-communication, pairing and cloud-communication and reduces the number of additional security layers needed on top of the traditional automotive networking approaches. NDN has a lot of room for performance improvements, implementation changes and tuning to be tailored for automotive networking, which makes it a strong candidate for automotive communication standardization.

To know the road ahead: A Forward-Looking Analysis of Lessons to Learn from IP DDoS

Zhiyi Zhang (UCLA)
R. Can Aygun (UCLA)
Guorui Xiao (UCLA)
Sichen Song (UCLA)
Eric Osterweil (George Mason University)
Angelos Stavrou (Virginia Tech)
Lixia Zhang (UCLA)

Distributed Denial of Service (DDoS) attacks have plagued the Internet for decades. There have been ever-increasing investments into mitigation solution developments, yet DDoS attacks are growing with ever-increasing frequency and magnitude. To identify the root cause of the above-observed trend, we perform a systematic analysis of volumetric DDoS detection and mitigation efforts over the last four decades. Our analysis reveals common design patterns across seemingly disparate solutions, as well as the grand challenge of effectively mitigating DDoS while creating aligned economic incentives at the same time. More importantly, our analyses show that NDN's architecture, by design, provides the fundamental building blocks to enable effective DDoS mitigation solutions.

Schema-Based Automation of Name-Based Access Control

Proyash Podder (Florida International University)
Alex Afanasyev (Florida International University)

Name-based Access Control (NAC) facilitates data-centric access control by utilizing NDN's naming convention to encrypt data at desired granularities and publish decryption keys to authorized parties. In order to make NAC a usable security system, we propose SEANAC, a schema-based approach to automate the overall name-based access control and effectively define and enforce desired control properties. Similar to schemas for access control, SEANAC leverages a domain-specific language to define access policies that are then converted into actionable NAC components: sets of encryption and decryption keys. With SEANAC, a management entity can easily define different granularities of data control (i.e., datasets or subsets that are access-controlled as a single item)---key encryption key schema---and different granularities data access (i.e., who can access specific granularity of data)---key decryption key schema. After that, SENAC generates and publishes all necessary KEK and KDK. This work is still at the early stage of experimentation and we plan to fully explore its potential using Hydra data storage application project.

A Security Bootstrapping Package for Hydra

Tianyuan Yu (UCLA)
Xinyu Ma (UCLA)
Hongcheng Xie (City University of Hong Kong)
Lixia Zhang (UCLA)

NDN requires that all entities in an NDN network go through a security bootstrapping process to obtain the trust anchor, certificate, and initial trust schema. This work presents a security bootstrapping package we have developed for a federated storage application called Hydra. Enabled by our package, Hydra controller authorizes and authenticates Hydra servers and users through their X.509 certificates or email addresses, then assigns names based on these identifiers, and finally issues certificates based on legitimate name assignments.

A Review of Defined Trust Transport (DeftT)

Turan Vural (UCLA)

This presentation introduces Defined Trust Transport (DeftT), an NDN-inspired networking protocol for limited domains that brings the enforcement of application-level integrity, authentication, and access control into the networking stack while improving ease of deployment and scalability.

Identity Authentication Security Strategies using TPM private key storage in an NDN Publish/Subscribe Industrial Energy Control System

Roger Jungerman (Operant Networks)
Scott Gray (Operant Networks)
Kathleen Nichols (Pollere LLC)

Secure identity management is critical in industrial energy control systems where cybersecurity compromise and unauthorized permissions can lead to grid-scale outages. These control systems need to restrict access to designated users and to particular utility equipment assets. This access control depends on securely defining member identities of both users and devices and distributing trust rules defining the allowed zero trust permissions. Identity certificate chains contain roles and other capabilities that can be securely validated. Identity certificates and trust rules can be efficiently distributed using a publish/subscribe architecture. A foundation of the security system is robustly securing private keys associated with each entity. The use of a Trusted Platform Module (TPM) to maintain private key security in a gateway that is often located in a remote site with limited physical security controls is discussed in the context of a DeftT publish/subscribe transport built on an NDN interest data protocol.

A Secure mHealth Infrastructure for Real-Time Data transfer with Fine-grained Access Control

Saurab Dulal (The University of Memphis)
Lan Wang (The University of Memphis)

Wearable devices such as smartwatches, fitness trackers, and body sensors have increased in popularity and are expected to continue growing in the future. These devices are used in the field of health and wellness, and researchers have been studying and analyzing their usefulness in mobile health (mHealth). mHealth involves the use of mobile and wireless technologies to gather and analyze health data, with the goal of improving health outcomes, healthcare delivery, and advancing research in the field. However, the privacy and legal concerns surrounding mHealth data and its characteristics make building a secure mHealth infrastructure a challenging task, and achieving fine-grained access control based on context is even more challenging.

To address these challenges, we present “A Secure mHealth Infrastructure for Real-Time Data transfer with fine-grained Access Control”. Our system addresses data security and privacy, real-time data collection and dissemination, and access control using the NDN architecture. It provides a secure pub-sub API for real-time data transport and implements access control policies with key-policy attribute-based encryption for fine-grained access control based on contextual information. In this presentation, we will also share our preliminary evaluation and real-world experience with data collection through sensors and sharing via the NDN testbed

A Dataset of NDN Traffic Traces for the Research Community

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

Networking researchers heavily rely on traffic traces to drive their experiments and simulations, and to ensure the comparability and reproducibility of their results. Yet, publicly available traces of NDN traffic are almost non-existent, thus forcing the NDN research community to resort to custom one-time solutions, which can undermine the confidence in the results and ultimately cause lots of duplicated work. In this talk, we briefly introduce a recent collaborative effort to publish a set of high-quality traces of a few representative NDN applications running on a global-scale test network. We wish to solicit feedback and suggestions from the community on our methodology and priorities, in order to make this project as useful as possible to other researchers. In addition to the dataset itself, we also plan to release an open-source toolkit to capture, analyze, and replay NDN traffic traces in a variety of environments.

NDN Sync API Overview

Varun Patil (UCLA)
Lixia Zhang (UCLA)

Good and easy-to-use APIs are crucial for enabling application development over NDN. We discuss a summarization of developments in higher level APIs related to Distributed Dataset Synchronization (NDN Sync) protocols. We discuss how different characteristics of such APIs enable their usage under varying conditions and satisfy diverse requirements.

Steering New Applications Away from Centralized Realization

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

There is a general consensus among the networking community that the Internet consolidation and centralization trend has progressed rapidly over recent years, as measured by the structural changes to the data delivery infrastructure, the control power over system platforms, and application development and deployment. In this talk we articulate the driving forces of this centralization trend, then use examples to illustrate how NDN may help new application developments that can operate without reliance on centralized cloud services.

iStack: An in-Kernel Networking Stack for Named Data Networking

Tian Song (Beijing Institute of Technology)
Tianlong Li (Beijing Institute of Technology)
Yating Yang (Beijing Institute of Technology)

In the last decade, NFD, as the most important NDN forwarder, has been designed and implemented for architectural research purpose. Besides, several dedicated forwarders, like NDN-DPDK, NDN-RIOT, are proposed to pursue high performance or meet the demands of special deployment scenarios. However, these forwarders are not general enough for application compared to TCP/IP, because they are not integrated into the framework of networking stack in current operating systems. Actually, NDN may be designed as a bypass forwarder, but an integrated version can gain more benefit for practical deployment with the support of operating systems.

In this talk, we will give a review on current implementation of forwarders and indicate that a general protocol stack developed within operating systems is crucial for practical uses and continuous evolution of a network protocol. Then, we present iStack, an NDN forwarder in the general networking stack, and discus our overall design philosophy and design choices. From 2019, iStack has been implemented as part of Linux kernel, and it has been tested on various hardware devices like wifi routers, Raspberry Pi, Android cellphones. Finally, we will present the roadmap of iStack to support NDN for broader applications.

Bringing Named Data Networking to Internet Livestreaming

Teng Liang (Peng Cheng Laboratory)
Yu Zhang (Peng Cheng Laboratory)
Wei Huang (Peng Cheng Laboratory)
Yang Zhang (Alibaba Group)
Weizhe Zhang (Peng Cheng Laboratory)
Beichuan Zhang (The University of Arizona)

The lack of application support is probably the biggest obstacle to ICN/NDN deployment. One approach to tackle this problem is to NDNizing existing applications by translating between application-level protocols and NDN, which can benefit from NDN’s architectural advantages while minimizing the development efforts needed. In this talk, I will introduce our work on bringing NDN into Internet Livestreaming by translating between HLS/NDN. Furthermore, we studied how to NDNize Low-latency HLS (LL-HLS), and the lessons can be applied to designing low-latency real-time data retrieval protocols in NDN. In addition, we built livestreaming prototypes which not only prove the effectiveness of the NDNizing approach but also generate real-world traffic for ICN/NDN-related studies.

Towards First Data Centric Medium Access Control Multicast Rate Control

Mohammed Elbadry (Stony Brook University)
Fan Ye (Stony Brook University)
Peter Milder (Stony Brook University)

Effective rate control algorithms are crucial for achieving high goodput and consistent performance in Medium Access Control (MAC) for 802.11 networks. Existing algorithms primarily focus on adjusting parameters such as modulation, coding, and spatial stream to find the best rate for data transmission. However, these algorithms often do not consider all available parameters and are address-based, only supporting unicast transmissions. Our work aims to improve the rate control algorithm by considering additional parameters such as guard interval and bandwidth that can enhance data rate without incurring data loss. We also take into account the unique challenges posed by data-centric paradigms and multicast transmissions, designing an algorithm that can optimize data rate performance while ensuring reliable and consistent data delivery. Importantly, our approach addresses the limitations of existing rate control algorithms, which primarily focus on unicast transmissions and may not take into account all available parameters. By considering a broader range of factors and designing an algorithm that supports multicast transmissions, our work offers significant improvements to the design of rate control algorithms for 802.11 data-centric networks.

mGuard: a Secure mHealth Data Sharing Infrastructure over NDN

Suravi Regmi (The University of Memphis)
Saurab Dulal (The University of Memphis)
Lan Wang (The University of Memphis)

Exploratory efforts in mobile health (mHealth) data collection and sharing have achieved promising results. However, fine-grained contextual access control and real-time data sharing are two of the remaining challenges in enabling temporally-precise mHealth intervention. We have developed an NDN-based system called mGuard (ICN'22) to address these challenges.
mGuard enables fine-grained contextual data access control and real-time data sharing through several core components, including a pub-subscriber API and access control policies that utilize NAC-ABE. The demo aims to showcase the high-level access control policies that can be employed to ensure precise control over mHealth data, both in real-time and archived. We also aim to demonstrate additional components of mGuard such as policy specifications, a simple GUI for consumers to subscribe/unsubscribe to data streams and fetch the corresponding data, and so on. Additionally, we will use the NDN testbed to carry out this demonstration.

NDN Opportunities in 5G/6G Core Networks

Junxiao Shi (NIST)
Davide Pesavento (NIST)
Lotfi Benmohamed (NIST)

This presentation describes two opportunities of adding NDN to 5G/6G core networks. Using a realistic use case, we present the potential benefits of having NDN forwarding in the 5G user plane. Then, we introduce the Service Based Architecture in the 5G control plane, and discuss the possibility of simplifying this architecture with NDN self-learning and NDN pub/sub.

N-DISE: NDN-based Data Distribution for Large-Scale Data-Intensive Science Experiments

Edmund Yeh (Northeastern University)

To meet unprecedented challenges faced by the world's largest data- and network-intensive science programs, the N-DISE project designs and implements 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.   The project develops a hierarchical Named Data Networking
(NDN) naming scheme for HEP data, implements new consumer and producer applications to interface with the high-performance NDN-DPDK forwarder, builds on recently developed high-throughput NDN caching and forwarding methods, and leverages FPGA acceleration subsystems. The project integrates NDN systems concepts and algorithms with the mainstream data distribution, processing, and management system of the Compact Muon Solenoid (CMS) experiment. N-DISE designs and prototypes stable, high-performance virtual LANs (VLANs) over a continental-scale wide area network testbed. At a recent demo at SC22, the N-DISE integrated system is shown to deliver LHC data over the wide area network (WAN) testbed at throughputs exceeding 63 Gbps between Caltech and StarLight, with dramatically reduced download time.

Edge Information Management - Demand is Only Growing

Jeff White (Dell Technologies)

Edge is an emerging computation paradigm built on the original ideas of ubiquitous computation and refined through Telecommunications, IoT and Cloud. Edge is driven by AIML, data intensity and reduced network latency, however, Edge is a super-scale distributed system that will require an enhanced approach to systems management, orchestration and data. This discussion focuses on the challenges of the modern Edge and how information awareness can be addressed.

SPAN-AI federated UCDN PoC - the first commercial ICN network at scale

Rhett Sampson (GT Systems)
Jaime Llorca (GT Systems and NYU)

GT Systems has been conducting privately funded research in content-based networking for a decade. We have collaborated with CSIRO, Bell Labs, Protocol Labs, the NDN community, IRTF ICNRG, and the IRTF. The result is SPAN-AI, the world's first intelligent, fully distributed, elastic, content based, autonomous, and self-optimising network protocol and operating system. We are building a Proof of Concept (PoC) of our federated Universal Content Distribution Network architecture based on SPAN-AI for Laser Light Communications. It will be the PoC of the first commercial ICN network at scale in the world. We are in discussions to include a major north American telco and several global datacentre SDN cross-connect service providers in that PoC.

As part of the PoC, we are considering forming a global Cooperative Research Centre (CRC) with the Australian government to provide funding for medium to long-term, industry-led research collaborations in Information Centric Networking and the "Metaverse" (Fediverse). The working title is "The Interverse CRC". We will also be applying for a Cooperative Research Centre Project Grant for the SPAN-AI PoC. The PoC will also become the first project funded by The Interverse CRC. Potential members of the Interverse CRC include GT Systems, University of Technology Sydney, Osaka University, UCLA, Hong Kong University at Guangzhou, Nokia, Intel, and Nvidia. We will welcome discussion of how that may proceed and the potential areas of R&D.

This submission is for a presentation outlining the SPAN-AI PoC, the possible Interverse Cooperative Research Centre and the Cooperative Research Centre Project grant for the SPAN-AI PoC. It is a discussion of technologies derived from or taking advantage of the NDN heritage and global application scenarios that benefit from NDN and how they solve some of the most critical problems in networking today.