Opening Session

A New Way to Support Security

Lixia Zhang (University of California, Los Angeles)
Alex Afanasyev (Florida International University)

Abstract: It is a commonly accepted notion that today's Internet security protections, mainly IPsec, (D)TLS, certificate authorities, and DNSSEC, are patch-on's to an already deployed Internet, and any future internet architecture should have the security designed-in. This talk aims to share with the community NDN's approach to achieve this goal, by providing an overview of the NDN security model, explaining the major components in this model and how they function together. The talk will also illustrate the basic difference between NDN security and the existing TCP/IP security, and identify new research challenges.

Panel 1

Security and Privacy in NDN: An Edge Computing Perspective

Chair: **Jay Misra** (New Mexico State University)
Alex Afanasyev (Florida International University)
Ken Calvert (National Science Foundation)
Tamer Refaei (MITRE Corporation)
Murugiah Souppaya (NIST)

Edge computing can support new applications, such as augmented reality and autonomous driving. It will also allow the interactions between multiple application and data stakeholders and tenants. This creates new security and privacy challenges at the edge. Several questions arise: How does an end-user trust the edge devices? Who owns the context generated by the edge device from user data? How can data sharing happen between the stakeholders and tenants? How are the data and user privacy issues handled? NDN may provide unique opportunities to address these challenges. In this panel, NDN experts and experts from outside the NDN community will present their thoughts on these and other challenges and discuss how NDN positions itself as a solution in the edge computing perspective.

Panel 2

Edge Computing: Shaping the Named Data Edge

Chair: **Christian Tschudin** (University of Basel)
Jeff Burke (University of California, Los Angeles)
Asit Chakraborti (Huawei Technologies)
Martial Michel (Data Machines Corp.)
Lan Wang (University of Memphis)

The edge highlights locality and diversity while the cloud wants to hide them. How can NDN support this difference? Where do computing resources play a role? Is NDN "edge-ready", has it the potential and is it already actively shaping the edge? In this panel, experts from inside as well as outside the NDN core community will reflect on these questions. The goal is to review the edge's use cases (IoT, reverse CDN) and requirements (security, low-latency) and to identify NDN's opportunities and challenges for building a post-IP named data edge.

Session 1: NDN support for computing

Towards an Augmented Reality Browser using NDN

Jeff Burke (UCLA REMAP) <jburke@remap.ucla.edu>
Peter Gusev (UCLA REMAP) <peter@remap.ucla.edu>
Jeff Thompson (UCLA REMAP) <jefft0@remap.ucla.edu>

Augmented reality is typically discussed as being achieved by individual "apps" that follow existing mobile application models. We propose that NDN enables a different and potentially more appropriate way of looking this application domain that is less oriented around the current model of vertically integrated, silo'd apps. AR overlays digital content on the physical world, and it is reasonable to assume that more than one such overlay might be active at any given time. Inspired by this requirement and the success of the world wide web, we propose a model of an ecosystem of named, signed, linkable NDN content that is retrieved and displayed by sandboxed code running in one of many layers within an AR "browser". NDN provides the necessary capabilities for low-latency, granular content access and efficient multicast distribution of user context to enable this approach. In this presentation, we present the application model, an initial NDN design and prototype focusing on edge support for mobile AR, and plans for future development.

Edge Computing Over Named Data Networking

Abderrahmen Mtibaa (New Mexico State University) <amtibaa@cs.nmsu.edu>
Satyajayant Misra (New Mexico State University) <misra@cs.nmsu.edu>
Reza Tourani (New Mexico State University) <rtourani@cs.nmsu.edu>
Jeff Burke (UCLA) <jburke@remap.ucla.edu>
Lixia Zhang (UCLA) <lixia@cs.nmsu.edu>

While edge computing research is rapidly growing, most of the proposed IP-based edge computing systems are centered around optimizing applications and services and are agnostic of the underlying networking problems. Such problems include complex mapping between application names and IP addresses without leveraging the available network conditions. Named Data Networking (NDN), however, solves the above problem by marrying app names to network forwarding. We discuss leveraging the NDN in-network features that can be used for seamless and efficient edge computing. We discuss how NDN can enable seamless computing resource discovery, task forwarding, and compute re-use in a distributed fashion without relying on a centralized entity while incurring a minimum overhead. Our approach can aid the optimization envisaged today with proxies and SDN controllers and may also be strong enough to be leveraged alone. We discuss the feasibility of a generic NDN edge computing paradigm that leverages NDN networking and forwarding features to seamlessly offload computation efficiently. We focus on in-network compute execution in NDN and we highlight the open issues for enabling secure, efficient and seamless edge computing functionalities over NDN.

Compute-First-Network for NDN

Asit Chakraborti (Huawei Technologies) <asit.chakraborti@huawei.com>
Dirk Kutscher (Huawei Technologies) <dirk.kutscher@huawei.com>
He Jianfei (Huawei Technologies) <jeffrey.he@huawei.com>
Cedric Westphal (Huawei Technologies) <cedric.westphal@huawei.com>

Syed Obaid Amin (Huawei Technologies) <obaid.amin@huawei.com>

Modern applications often expect the network to deliver it processed data. As a result, in-network compute capability has often been considered as a complementary feature for network architectures like Named Data Network (NDN). The desire for the computation to be performed in the network instead of at the data source, destination or a remote server might stem from reasons related to computing resource availability, access latency, network bandwidth optimization, geographical or other application context, etc. Compute-First-Network (CFN) is a generalized framework that will allow application vendors to provide functions that can be discovered and invoked by applications in a location agnostic way, with the network selecting the most optimal location for the function execution. CFN expands on the abstractions provided by NDN: it allows named access to functions and receiver driven data flow, the function body being treated essentially as data. A Request For Execution is a primary protocol entity of CFN. Functions can be short lived or long lived, stateless or stateful; and on-demand function instantiation is a key feature. It is expected that initially functions will be loaded at service points at the cloud and edge locations, but mechanisms will be available for a CFN node to download a function and offer execution of the same. A CFN capable network node will feature a Function Store to cache function bodies, and a Function Controller capable of managing the execution environment that uses Unikernels and Linux containers. The Function Controller maintains a state for every active function, and is capable of responding to new function instantiation requests from the NDN forwarder. CFN will accommodate protocols that facilitate parameter and result passing between the client and the function, as well as their mutual authentication. The discovery of function execution points can be aided by centralized entities, for example, a cloud based service; or it could be performed in a distributed way that takes care of resource congestion locally. One of the use-cases for CFN is performing resource heavy computation for AR/VR applications at a dynamically determined edge location. At the same time, the platform is intended to be equally applicable for ephemeral computations for IoT data. Other approaches to in-network computing like NFN and NFaaS lack the generality needed to be suitable for a large set of applications. NFN lacks a standard virtualization environment, and incorporating stateful functions and high-volume parameter passing using the lambda expressions could be difficult. While NFaaS offers Unikernel based execution, it does not focus on aspects like function discovery, parameter passing and congestion control.

Session 2: IoT and security

NDNoT: A Framework for Named Data of Things

Zhiyi Zhang (UCLA) <zhiyi@cs.ucla.edu>
Yanbiao Li (UCLA) <lybmath@cs.ucla.edu>
Tianyuan Yu (Sichuan University) <royu9710@outlook.com>
Alex Afanasyev (Florida International University) <aa@cs.fiu.edu>
Lixia Zhang (UCLA) <lixia@cs.ucla.edu>

The Named Data Networking (NDN) architecture provides simple solutions to the communication needs of Internet of Things (IoT) in terms of ease-of-use, security, and content delivery. To utilize the desirable properties of NDN architecture in IoT scenarios, we are working to provide an integrated framework, dubbed NDNoT, to support IoT over NDN. NDNoT provides solutions to auto configuration, service discovery, data-centric security, content delivery, and other needs of IoT application developers. Utilizing NDN naming conventions, NDNoT aims to create an open environment where IoT applications and different services can easily cooperate and work together. This presentation will help to introduce the basic components of our framework and explains how these components function together.

Blockchain-based Decentralized Public Key Management for Named Data Networking

Kan Yang (University of Memphis) <kan.yang@memphis.edu>
Jobin J. Sunny (St. Jude Children's Research Hospital) <jjsunny@memphis.edu>
Lan Wang (University of Memphis) <lanwang@memphis.edu>

Named Data Networking (NDN) uses public-key based identities and trust models to achieve data-centric security. Each NDN data packet is signed by its producer, and any data consumer can check the data integrity and authenticity by following a chain of trust to verify that the data is signed by a public key associated with the data producer. Such trust chains typically end at an application-specific trust anchor whose public key is either preconfigured into the software package or can be verified through some means outside the application. As these trust anchors play a critical role in ensuring the security of NDN applications, it is highly desirable to develop a public key management system to register, query, update, validate, and revoke their public keys. However, traditional public key management system such as Public Key Infrastructure (PKI) and Web-of-Trust (WoT) suffer from various problems. In this paper, we propose BC-PKM, a public key management system for NDN that takes advantage of the decentralized and tamper-proof design features of Blockchains. We further prove that BC-PKM can resist a variety of attacks from adversaries that compromise less than half of the public key miners. Moreover, we demonstrate a prototype that implements the proposed API of BC-PKM.

Distributed Ledger over NDN for A Real-world Solar System

Zhiyi Zhang (UCLA) <zhiyi@cs.ucla.edu>
Vishrant Vasavada (UCLA) <vishrantvasavada@gmail.com>
Randy King (Operant Solar) <randy.king@operantsolar.com>
Lixia Zhang (UCLA) <lixia@cs.ucla.edu>

Distributed blockchain system has great potentials in cybersecurity systems for its built-in robustness, incorruptibility, and publicity. Named Data Networking (NDN) secures communication at the network layer by requiring all data packets to be signed when produced, ensuring data authentication and integrity. Therefore, an NDN Data packet naturally serves as an unforgeable and undeniable record of an entity's behavior. We are now working to build a distributed ledger over NDN for a real-world solar system (Operant Solar) that requires a distributed ledger system to record the energy production and consumption. In our system, we directly use NDN Data packets as the blocks and link Data packets together through names, thus each block can directly be fetched from the Internet by the name without knowing where to fetch. We use signature signing/verification to place proof-of-work, and make the record in a question-answer mode to prevent compromised attackers from keeping adding fake records to the system.

Session 3: NDN for Vehicular Networks

Vehicular Named Data Networking

Dennis Grewe (Robert Bosch GmbH) <dennis.grewe@de.bosch.com>
Claudio Marxer (University of Basel) <claudio.marxer@unibas.ch>
Christopher Scherb (University of Basel) <christopher.scherb@unibas.ch>
Marco Wagner (Robert Bosch GmbH) <marco.wagner3@de.bosch.com>
Christian Tschudin (University of Basel) <christian.tschudin@unibas.ch>

Named Data Networks (NDN) oer the service to deliver information based on the content's name. This means, clients are released from holding server locations and request content in a connection oriented fashion. As an extension of NDN, Named Function Networking (NFN) allows users to request for derived, i.e. dynamically produced, data. In NFN, named functions are published, which can be applied to any available content on demand of a user. For this purpose, a user composes a data name which encodes the application of named function(s) to certain data. It is the task of the network to compute and deliver the result. Behind the scenes, the network implements a forwarding strategy which decides where a computation is executed. Recently, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure(V2I) connectivity transitioned from a vision of the future to reality. Applications in such environments vary from large-scale traffic flow control systems to local propagation of road conditions. We present a network stack for the data exchange in the automotive IoT. Based on the Named Function Networking (NFN) principles, the communication model is not restricted to propagation of static data but natively supports computation-offloading to other nodes. We present solutions and report on experiments with real cars on a test course.

Connectivity and Location-aware Routing Scheme (CLRS) for Connected and Autonomous Vehicles (CAVs)

Muktadir Chowdhury (University of Memphis) <mrchwdhr@memphis.edu>
Junaid Ahmed Khan (University of Memphis) <junaid.khan@memphis.edu>
Lan Wang (University of Memphis) <lan.wang@memphis.edu>

Routing or forwarding data packet in Connected Vehicles is a challenging task and data retrieval rate can be very low due to highly dynamic topology and intermittent connectivity. Most of the data forwarding strategies in the literature are location-based accompanied with limited flooding when location information is not available. For efficient communication and data retrieval in the vehicular network, we propose a hybrid forwarding solution, called CLR, that will enable vehicles to choose next-hop based on both the vehicle's centrality score as well as its location. Rather than flooding when location information is not available, CLR uses centrality score to forward packet. To overcome the shortcomings of IP in mobile environment, CLR is based on a data-centric network called Named Data Network (NDN). CLR will be compared against both location-aware forwarding strategy (GPSR and NAVIGO) and centrality-based forwarding strategy (STRIVE) in the literature.

Data-Centric MAC for Robust Multicast in Vehicular Networks

Mohammed Elbadry (Stony Brook University) <mohammed.salah@stonybrook.edu>
Bing Zhou (Stony Brook University) <bing.zhou@stonybrook.edu>
Fan Ye (Stony Brook University) <fan.ye@stonybrook.edu>
Peter Milder (Stony Brook University) <peter.milder@stonybrook.edu>
YuanYuan Yang (Stony Brook University) <yuanyuan.yang@stonybrook.edu>

Data-centric networks provide content instead of address (what vs. where) based communication primitives, and have been argued to be the proper candidate for data dissemination in high mobility vehicular networks (e.g., delivering road side accident video clips to affected drivers in both directions). However, current Medium Access Control (MAC) layers filter incoming frames based on destination addresses, not content. The data-centric network community has resorted to MAC broadcast, with high and greatly varying frame loss rates. We propose V-MAC, a data-centric MAC layer that filters frames by content. It supports one to many multicast at MAC level, and ensures a uniform and controllable small frame loss rate across all receivers, despite their varying reception qualities. We have created a V-MAC prototype using Raspberry Pis and WiFi dongles. Experiments under extremely noisy environment show

that it reduces frame loss from 50% (broadcast) to less than 10%, and consistently among multiple receivers.

Session 4: NDN in Mobile AdHoc Networks

Peer-to-Peer File Sharing in Mobile Ad hoc Networks over NDN

Spyridon Mastorakis (UCLA) <mastorakis@cs.ucla.edu>
Tianxiang Li (UCLA) <tianxiang@cs.ucla.edu>
Lixia Zhang (UCLA) <lixia@cs.ucla.edu>

Mobile Ad hoc NETworks (MANETs) are network environments, where intermittent connectivity and unpredictable node mobility are the norms. In such environments, sharing files among the nodes is challenging. In this presentation, we discuss the design of a peer-to-peer file sharing application in MANETs over NDN. We use our previous work, nTorrent, which is a peer-to- peer file sharing application in wired NDN networks, as the starting point of our design. However, our design fundamentally departs from nTorrent to efficiently address the communication challenges in MANETs, such as network partitions, short-lived ad hoc node encounters, and lossy links. Our design proposes a space-efficient approach for nodes to let others know about the torrent data they are missing, and leverages NDN's data-centric security to achieve data authentication and integrity. We study a number of different design decisions to achieve efficient data dissemination with the fewest possible packet transmissions to minimize energy consumption, and we evaluate the effect of each design decision through simulations.

Distributed Dataset Synchronization in Mobile Ad Hoc Networks over NDN

Tianxiang Li (UCLA) <tianxiang@cs.ucla.edu>
Spyridon Mastorakis (UCLA) <mastorakis@cs.ucla.edu>
Xin Xu (UCLA) <xinxu129@cs.ucla.edu>
Haitao Zhang (UCLA) <haitao@cs.ucla.edu>
Lixia Zhang (UCLA) <lixia@cs.ucla.edu>

Mobile Ad-hoc Networking (MANETs) is characterized by dynamic movements of mobile nodes and intermittent connectivity among them, creating unique challenges to running applications over MANET. In response to this challenge, we developed DDSN, a Distributed Dataset Synchronization protocol over Named Data Networking (NDN). Taking wireless ad hoc, intermittent connectivity as the norm and utilizing NDN advantages, DDSN enables nodes running the same applications to synchronize their shared application dataset whenever they encounter each other securely and efficiently. We evaluated the DDSN design through extensive experiments, and the results show that DDSN can achieve resilient and timely dataset synchronization over lossy and intermittent connectivity. We also compared DDSN with TCP/IP based MANET solutions, both qualitatively through the design analysis and quantitatively via experimental results.

Toward Multi-Hop Long-Range D2D Communication via Information Centric Ad Hoc Networks

Yaoqing Liu (Clarkson University) <liu@clarkson.edu>
Anthony Dowling (Clarkson University) <dowlinah@clarkson.edu>

Mobile wireless ad hoc networks (MANETs) do not rely on an infrastructure to operate and can disseminate information quickly without worrying about single point of failure, thus can be used for a variety of applications, such as disaster relief, vehicular communication, smart agriculture, etc. However,

the challenges affecting MANETs, including ubiquitous connectivity, dynamic routing, and flexible mobility, span from various layers of the current TCP/IP protocol stack. A particularly daunting challenge is to enable adaptive communication and interoperability over multiple heterogeneous wireless links. To circumvent existing constraints, the poster leverages Named Data Networks (NDN), an emerging information-centric network architecture, to interconnect diverse wireless links at the network layer and implements flexible routing and forwarding strategies for efficient information dissemination. The system focuses on implementing an interface between NDN and LoRaWAN, and interconnecting LoRaWAN and WiFi via NDN Forwarding Daemon (NFD) into a ubiquitous ad hoc network, which bears very long-range and multi-hop capabilities for Device-to-Device (D2D) communication. Many compelling applications, such as disaster relief, smart cities, etc., can benefit from the technology. Field experimental results show that the newly built ad hoc network can easily cover a radius of several kilometers and make full use of NDN features to maximize utilization of heterogeneous wireless links and to enhance efficiency of information dissemination. In the poster, we will demonstrate the research results using NDN-enabled devices for a number of multi-hop long-range experiments and share the experiences we learned from the study.

Session 5: Routing and Forwarding

High-Speed NDN-DPDK Forwarder

Junxiao Shi (NIST) <junxiao.shi@nist.gov>
Lotfi Benmohamed (NIST) <lotfi.benmohamed@nist.gov>

NDN-DPDK forwarder is a high-speed NDN forwarder developed with Data Plane Development Kit (DPDK). This presentation explains the motivation, design, and current status of this project. NDN protocol's reference implementation, the NDN Forwarding Daemon (NFD), is designed to be modular and extensible, but is not optimized for performance. The NDN community needs a high-speed forwarder that would be useful to data-intensive science applications that require the distribution of large amounts of scientific data, and to enable NDN adoption for general usage such as video streaming services. NDN-DPDK forwarder adopts four techniques to be fast: (1) processes packets in parallel on multiple CPU cores, fully utilizing available CPU resources on the target hardware; (2) uses pre-allocated memory pool, avoiding costly memory allocations during packet processing; (3) incorporates better data structures; (4) communicates with Network Interface Cards (NICs) directly, bypassing the kernel. As of Jul 2018, NDN-DPDK has achieved a forwarding throughput in excess of one million Interest-Data exchanges per second. This was measured on a server equipped with two Intel E5-2680V3 processors, 512GB memory in two channels, and Mellanox ConnectX-5 100Gbps network cards. NDN-DPDK codebase includes a traffic generator to perform this test. In the future, NDN-DPDK forwarder will be integrated into a complete system that includes a management and measurement framework.

A New Way of Traffic Engineering in NDN

Klaus Schneider (The University of Arizona) <klaus@cs.arizona.edu>
Beichuan Zhang (The University of Arizona) <bzhang@cs.arizona.edu>
Lotfi Benmohamed (NIST) <lotfi.benmohamed@nist.gov>

Today's network providers use Traffic Engineering (TE) in order to steer traffic from heavily used paths towards lightly used ones, aiming to use their existing net- work in the most efficient way. The most common approaches for IP traffic engineering are 1) tuning the link weights of a hop-by-hop routing protocol [1], 2) splitting traffic among pre-established end-to-end tunnels (like MPLS) [2], and 3) using

centralized control via Software-Defined Networking [3]. However, each of these approaches comes with drawbacks, respectively, 1) hard-to-predict global side- effects of changing link weights, 2) manual setup of label-switched paths and slowly- adjusting bandwidth reservations, and 3) requiring a centralized control plane. In this presentation, we show that NDN can offer an additional way of traffic engineering, one which does not suffer these drawbacks. We show that our new way of NDN TE can a) simplify configuration (avoiding manual configuration or having to pre-establish paths) and b) improve performance (maximizing user utility and using the available network resources more efficiently), while also supporting important NDN features such as multi-destination routing and ubiquitous in-network caching. To achieve this, we make use of hop-by-hop multipath routing, NDN's stateful forwarding plane, and explicit probing of the path (congestion) state. More specifically, we address the research questions of how to coordinate routers which make independent forwarding decisions, how to ensure stability and avoid oscillations, and lastly how to determine when traffic should be split among multiple paths and when it shouldn't.

NDNCONF: Network Configuration Management System for NDN based on NETCONF protocol

Rajender Kumar (Florida International University) <rkuma013@fiu.edu>
Alexander Afanasyev (Florida International University) <aa@cs.fiu.edu>

Internet is rapidly growing and a variety of services are provided by the heterogeneous network devices developed by different companies. For faster information processing and efficient data delivery, it is very important to have some tools, mechanism or protocols for configuration management of these heterogeneous devices. Due to recent changes in network technology, network operators do not only have to deal with network devices configuration, but also they have to manage various aspect of services. Thus, management of services and various network devices is a major factor which affects the cost of networks. In the past, SNMP and CLI (Command Line Interface) are used for configuration of network devices. But due to introduction of heterogeneous equipment and requirements of automation in configuration management, these solutions are no longer used for configuration management. IETF introduces a new standard called NETCONF (NETwork CONFiguration) for efficiently managing the configuration of different network devices. The Network Configuration Protocol (NETCONF) defined in RFC4741 provides new mechanisms to install, manipulate, and delete the configuration of network devices. NETCONF protocol is based on XML data encoding scheme for encoding the protocol messages and configuration related data. Our understanding of design and architecture of NDN states that NDN can be used in place of IP-based architecture with the current state-of-the-art heterogeneous types of equipment for accessing data over Internet. Thus, as we stated above, it becomes necessary that there should be some kind of protocol to efficiently configure different types of equipment over the Internet for NDN. To the best of our knowledge, there is no protocol (equivalent to Netconf) implemented on the NDN paradigm for configuration management. So, we decide to work in this direction to design a protocol, called NDNCONF (NDN version of Netconf), for configuration management over NDN network so that different network devices can easily be configured and used in the network. We design a Yang model for different classes of management module of NFD. We provide an architecture of NDNCONF protocol for NDN network configuration management. NDNCONF protocol provides new mechanisms to view, manipulate, and delete the configuration of network devices over the NDN network. Our NDNCONF protocol is based on XML data encoding scheme for encoding the protocol messages and configuration related data. Our NDNCONF protocol uses the client -server architecture for configuration management in which a network device acts as a server and an application or another device acts as client and they can be connected using existing secure transport protocols over the NDN. In NDNCONF, built on top of NDN, all response can be properly authenticated at the network packet level and commands can leverage trust

schema to realize various control permissions at fine granularity. Client gives commands (in the form of interest packets) to get or edit the configuration data, which are processed by the server device and resultant configuration or state data is transferred to client in a data packet. Client uses the simple interest to retrieve state data and command interest to edit the configuration data. Thus, NDNCONF is a variant of the Netconf for the NDN network.

Session 6: NDN support for new deployments

NDN Supporting Ultra-Dense Networks

Xiaoyan Hong (University of Alabama) <hxy@cs.ua.edu>
Pawan Subedi (University of Alabama) <psubedi@crimson.ua.edu>

Dense presences of IoT devices as well as high population of mobile phones are likely future scenarios. Under the 5G paradigm of Ultra Dense Networks (UDN), there is also a high density of access points (APs), or called base stations (BS), via the deployment of macro-cell, micro-cell, fermtocell, and user devices acting as APs. Thus in addition to small cell stations, relay APs and distributed remote radio heads are all components in the network architecture. One of the network paradigm to achieve the resource management, interference management, mobility management and security aspect in such dense networks is User-Centric Ultra-Dense Network (UUDN). In this architecture, each device is treated as the center, surrounded by a small pseudo-celled network which is created such that the network provides multiple access points (AP Group, or APG) for the device. The UUDN architecture has a functional unit of Local Access Server (LAS) at wireless edge with control plane for APG management and user plane for data communications. LASs connect to the core network service centers. The UUDN architecture, if implemented using the traditional IP network, will encounter the same problems in dealing with mobility, content sharing, security, etc., as those identified and motivated Named-Data Network Internet Architecture. As such, in this work, we present an implementation blueprint of UUDN using Named-Data Networking. The goal is to demonstrate the benefits of NDN in supporting UUDN model for ultra-dense networks. The name conventions of the control messages, the communications among the main types of devices in the UUDN, and various tables will be prototyped. The presentation/demo will show a three-nodes scenario that is general enough to extend to multiple IoT scenarios, for examples, Intelligent Transportation System and smart home systems.

Automated Neighbor Discovery to Run NDN Anywhere

Arthi Padmanabhan (UCLA) <artpad@cs.ucla.edu>
Lan Wang (University of Memphis) <lanwang@memphis.edu>
Lixia Zhang (UCLA) <lixia@cs.ucla.edu>

NDN is designed as a "universal overlay" that operates over existing infrastructure, which allows it to be deployed incrementally. To run over IP, NDN allows its packets to be sent using IP tunnels. NDN's use of IP tunnels can be leveraged in situations where establishing NDN connectivity through normal methods is not feasible. Some networks prohibit multicast, unicast, or both within the local network, leaving NDN nodes isolated. This presentation introduces the NDN Neighbor Discovery service (NDND), which details the communication required for NDN nodes in such networks to establish connectivity through the use of a rendezvous server.

NDN for Data Intensive Science

Susmit Shannigrahi (Colorado State University) <susmit@colostate.edu>

In this talk, we discuss the progress of the SANDIE project since the last NDNComm. The SANDIE project aims to integrate NDN and SDN concepts with the existing High Energy Particle Physics workflows for efficient data distribution, in-network strategic caching, and request redirection to the nearest replica, among other novel mechanisms. In addition, we expect that integrating NDN/SDN with current workflows will reduce the complexity of data management software, such as xtootd, that are currently used in the HEP domain. We discuss how we have inferred the network topology with detailed metrics such as link capacity, RTT delay, the available bandwidth for US-CMS. We then use this topology to simulate delay reduction by strategically adding in-network caches at Tier-2 sites in the US. We also analyzed real data from CMS and found that they display a significant locality of reference. Consequently, our simulations showed that we should be able to reduce the average data distribution delay by 48% using NDN and the VIP caching algorithm. Having simulated the improvements, we are extending the ndn-sci testbed to deploy our algorithms in a real environment. We are also working on integrating an NDN plugin with xrootd that will allow the xrootd system to redirect requests and utilize caches in the network transparently. In this talk, I discuss these updates as well as how we plan to study NDN's benefits using real HEP data requests once we integrate NDN to the existing production xrootd system.

Posters and Demos

IoT+NDN+Wireless: Experimental Insights from Using 802.11 Infrastructure and Ad-hoc Modes

Travis Machacek (New Mexico State University)
Abderrahmen Mtibaa (New Mexico State University)
Reza Tourani (New Mexico State University)
Satyajayant Misra (New Mexico State University)

A Raspberry Pi Based Data-Centric MAC for Robust Multicast in Vehicular Networks

Mohammed Elbadry (Stony Brook University)
Bing Zhou (Stony Brook University)
Fan Ye (Stony Brook University)
Peter Milder (Stony Brook University)
YuanYuan Yang (Stony Brook University)

Bootstrapping Trust in NDN-Based Vehicular Network Using SWIFT Trust

Sanjeev Kaushik Ramani (Florida International University)
Manusri Viswanath (Rensselaer Polytechnic Institute)
Jalena Jones (Claflin University)
Alex Afanasyev (Florida International University)

Named-based Access Control

Zhiyi Zhang (UCLA)
Yingdi Yu (UCLA)
Alex Afanasyev (Florida International University)
Lixia Zhang (UCLA)

Get an NDN certificate with NDNCERT protocol
Zhiyi Zhang (UCLA)
Alex Afanasyev (Florida International University)

Upcoming Changes in NDN Protocol
Alex Afanasyev (Florida International University)

Optimal Cache Allocation under Network-Wide Capacity Constraint
Van Sy Mai (NIST)
Stratis Ioannidis (Northeastern University)
Davide Pesavento (NIST)
Lotfi Benmohamed (NIST)

NDN for Public Safety Deployable Networks
Davide Pesavento (NIST)
Junxiao Shi (NIST)
Edward Lu (NIST)
Lotfi Benmohamed (NIST)
Maxwell Maurice (NIST)

ANTD NDN-IoT Testbed: Smart Building Sensing
Edward Lu (NIST)
Junxiao Shi (NIST)
Davide Pesavento (NIST)
Kerry McKay (NIST)
David Cooper (NIST)
Lotfi Benmohamed (NIST)

HomeCam Browser-based Home Surveillance Camera
Junxiao Shi (NIST)

Performance evaluation of the NDN-DPDK forwarder
Siham Khoussi (NIST),
Junxiao Shi (NIST)
Ayoub Nouri (Grenoble University)
James Filliben (NIST)
Lotfi Benmohamed (NIST)
Saddek Bensalem (Grenoble University)

PSync deployment on IoT sensor testbed
Ashlesh Gawande (Uinversity of Memphis)
Lan Wang (University of Memphis)

Named Query Framework for Named Data Networking of Things
Muhammad Atif Ur Rehman (Hongik University Sejong Campus, South Korea)
Rehmat Ullah (Hongik University Sejong Campus, South Korea)
Byung-Seo Kim (Hongik University Sejong Campus, South Korea)

Leveraging Named Data Networking in Edge Computing
Rehmat Ullah (Hongik Univeristy Sejong Campus, South Korea)
Byung-Seo Kim (Hongik Univeristy Sejong Campus, South Korea)

NDN Supporting Ultra-Dense Networks
Xiaoyan Hong (University of Alabama)
Pawan Subedi (University of Alabama)

ICE-AR Application Progress
Peter Gusev (UCLA REMAP)

An Overlay NDN Architecture for Application-Driven Satellite-Terrestrial Integration
Yating Yang (Beijing Institute of Technology)
Tian Song (Beijing Institute of Technology)

Distributed Network Measurement Protocol (DNMP): A Secure Role-Based Approach
Kathleen Nichols (Pollere, Inc)

Vehicular Named Data Networking
Dennis Grewe (Robert Bosch GmbH)
Claudio Marxer (University of Basel)
Christopher Scherb (University of Basel)
Marco Wagner (Robert Bosch GmbH)
Christian Tschudin (University of Basel)