iCASM: An Information-Centric Network Architecture for Wide Area Measurement Systems

Gelli Ravikumar, *Member, IEEE*, Dan Ameme, *Student Member, IEEE*, Satyajayant Misra, *Member, IEEE*, Sukumar Brahma, *Fellow, IEEE* and Reza Tourani, *Member, IEEE*

***Abstract*—Wide Area Measurement Systems (WAMS) use an underlying communication network to collect and analyze data from devices in the power grid, aimed to improve grid operations. For WAMS to be effective, the communication network needs to support low packet latency and low packet losses. Internet Protocol (IP), the pervasive technology used in today's communication networks uses loop-free best-paths for data forwarding, which increases the load on these paths causing delays and losses in delivery. Information-Centric Networking (ICN), a new networking paradigm, designed to enable a data-centric information sharing, natively supports the concurrent use of multiple transmission interfaces, in-networking caching, as well as per-packet security and can provide better application support. In this paper, we present *iCASM*, an ICN-based network architecture for wide area smart grid communications. We demonstrate through simulations that *iCASM* achieves low latency and 100% data delivery even during network congestion by leveraging multiple available paths; thus significantly improving communication resiliency in comparison to an IP-based approach. *iCASM* can be used immediately on today's Internet as an overlay.**

***Index Terms*—Network Architecture, Quality of Service, Reliability, Smart Grid, Convergence, Control, WAMS.**

NOMENCLATURE

Term	Meaning
PMU	Phasor-measurement unit.
PDC	Protocol Data Concentrator.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
IP	Internet Protocol.
ICN	Information-centric Networking.
NDN	Named-data Networking.
FIB	Forwarding Information Base (Forwarding Table).
PIT	Pending Interest Table.
CS	Content Store.
ECMP	Equal-Cost Multi-Path.
WECC	Western Electricity Coordinating Council

I. INTRODUCTION

Most traditional control applications in today's power systems use either local measurements or information derived from Supervisory Control And Data Acquisition (SCADA) systems, which receive unsynchronized scalar data once every 2-4 seconds. Wide Area Measurement Systems (WAMS) aim to enable control with synchronized, low-latency grid-wide measurements for control. WAMS [1] primarily consist of Phasor Measurement Units (PMUs) deployed strategically across power networks. In a WAMS network, PMUs measure voltage and current phasors, as well as frequency and rate of change of frequency, and send these data to PDCs to be stored in a database. All these data are transmitted over a communication network and used for enhanced real-time operation, control and protection of power systems [2].

With PMUs transmitting at data rates of 120 frames per second (fps) for 60Hz systems (likely to increase to 240 fps in near future), control and wide-area protection applications can be designed to respond in a much shorter time-frame (almost real-time), thus increasing system reliability. PMU data, therefore, can form a strong enabler for the power grid to move towards more automatic and real-time control [3].

The success of WAMS driven control and protection will however depend heavily on the communication infrastructure, which is responsible for transmission of data between PMUs, Phasor Data Concentrators (PDCs), and Wide-Area Controllers (WACs) at sub-second rates, in real-time. There has been a rapid increase in the deployment of PMUs around the world. For instance, China had deployed 2500 PMUs by 2015 [4], the North American power grid had deployed 2500 networked PMUs by 2017 [5], and India initiated a project in 2012 for the deployment of 1669 PMUs [6]. The data volume is expected to grow rapidly as the future smart grid deploys PMUs, PDCs, and WACs in large-scale, driven by the need for more synchrophasor data collection. Using a shared communication infrastructure, such as the Internet– the most scalable approach–could lead to network congestion. This could affect control signals triggered during emergencies that need to be transmitted reliably and with minimum latency even during congestion.

Motivation: There have been some efforts by utilities to use private, dedicated fiber-optic networks, but this is not a scalable solution for all utility providers—consider large rural areas in the US, Europe, or developing countries. Further, with the increased deployment of distributed energy resource (DERs), such as solar panels on rooftops of houses, remote solar/wind farms, and offshore wind farms, the communication network will grow in size and communication volumes will also increase. These traffic will have to contend with other traffic (experienced as congestion or delay effects). This will be true even in a dedicated, private optical network.

As is evident from the history of most communication networks, once the network is in place, applications grow in their requirements to consume all the available network resources. In the smart grid context, for example, the current generation of numerical relays that will be deployed with all new installations will in most likelihood have synchrophasor capability, which will need transmission as well, for various

Gelli Ravikumar is with Iowa State University, USA. Satyajayant Misra and Dan Ameme are with New Mexico State University, USA. Sukumar Brahma is with Clemson University, USA. Reza Tourani is with Saint Louis University, USA. (E-mail: gelli@iastate.edu, {danameme,misra}@cs.nmsu.edu, sbrahma@clemson.edu, and reza.tourani@slu.edu).

real-time applications, not necessarily just for protection. Thus, it is imperative that the solutions are future-proof in terms of operating despite network congestion—our attempt in this paper.

Operation, control, and protection applications in the smart grid translate into communication requirements, such as low latency, low frame/packet loss, low errors, high security, and efficient handling of large volumes of measurement and control-signal data. In IP-based communication (standard approach today), data forwarding is based on using the best, loop-free path. This increases network congestion on the best-path as traffic volume increases. Other available paths are unutilized until a path change is triggered in the network.

Despite the transmission control protocol's (TCP's) capability in reliable communication, error detection, and retransmission, the TCP/IP stack falls short in making intelligent forwarding decisions based on the network condition. IP routing protocols use the best path (as the only path allowed to be used), resulting in network congestion and delayed data delivery on that path. This is particularly true if the various destinations of the data are in the same general region in the network, then all the flows end up sharing several links, which leads to congestion and non-characterizable delays. This requires a rethink of the network architecture for the smart grid.

Today's Internet applications are more interested in content and its provenance rather than the location of data. This is particularly true as content is being created by a plethora of devices (e.g, sensors, smartphones) connected at the network edge. This has resulted in the proposal of ICN [7] as a new, more efficient networking paradigm for the Internet. The novel (key) features in the ICN paradigm include in-network caching, data provenance, inherent multicast support, capability of using multiple interfaces concurrently, and improved mobility support. These features can be leveraged to make the ICN paradigm more suitable for meeting the diverse needs of smart grid applications.

In this paper, we propose an ICN-based smart grid network architecture, which uses an intelligent forwarding strategy that allows intermediate routers to leverage multiple communication interfaces concurrently to improve network latency and reliability requirements in WAMS, particularly for time sensitive/critical communications. By conducting experiments in both ICN and IP, we obtain empirical evidence which proves that ICN is more suited for WAMS network communications.

Contribution: The ***key*** contributions of our research are:

- The proposal of, *iCASM*, an information-centric network architecture that supports reliable and timely dissemination of data for grid control and protection.
- The demonstration that with *iCASM*, packet losses can be significantly reduced, and packet delivery latency can be lowered even during network congestion.

The rest of the paper is organized as follows. Section II reviews the state-of-the-art network designs for wide-area monitoring and control applications. Section III discusses the IP-based and proposed ICN-based WAMS communications. Section IV proposes *iCASM* design strategy for WAMS communications. Section V demonstrates experiment-based validation and significant observations, followed by conclusion in Section VI.

II. State-of-the-Art of Network Designs for Wide-Area Monitoring and Control Applications

In [8], the authors presented a Wide-Area Control (WAC) method which aims to utilize the available wide area measurements for the development of suitable control signals in order to enhance the performance of the generators' local controllers. These control signals intend to overcome the lack of global observability at the local controllers.

Stahlhut *et al.* [9] evaluated the impact of latency on WAC systems using dedicated communication channels. However, this dedicated approach is not cost-effective as the size of the network scales to accommodate an increasing number of devices. Furthermore, failure of the dedicated channel will affect PMU data transmission. If redundant dedicated channels are provisioned to cater for failures the cost of network deployment increases further. For economic reasons, future network designs should consider using a shared network infrastructure (e.g., the Internet) for transmitting PMU data. But, a shared network infrastructure is more prone to congestion, thus Quality of Service (QoS) mechanisms together with forwarding strategies should be deployed to support improved data delivery.

Gridstat [3], is a middleware framework based on API abstractions with its data plane specialized to support QoS. It has been proposed to meet the dissemination needs of the power grid. Even though QoS can ensure that critical packets are delivered, in a shared network where other applications are also marked as critical, the capacity reserved for such critical flows can be exceeded during peak traffic periods and thus cause congestion and packet loss. In [10], the authors proposed the extension of Content-Centric Networking (CCN) with Software-Defined Networking (SDN) principles to provide QoS to the different data flows that exist in smart grids. However, the proposal was not evaluated using any form of experimentation; also SDN is known to have scalability issues [11] due to its centralized control logic–particularly challenging in multi-domain networking.

Chenine *et al*. [12] modeled and simulated Wide Area Monitoring and Control System (WAMC) in an IP-based network by creating a scenario in which background data was introduced into the network to congest communication links at 50-70%. Based on the results, the authors suggested increasing bandwidth and prioritizing packets as solutions to minimize network latency. In [13], it was shown that link failures and congestion affect grid stability. The use of Resource Reservation Protocol (RSVP) and Multi-Protocol Label Switching (MPLS) for bandwidth reservation and packet prioritization was proposed in [14]. The experimental results suggested that packet prioritization alone is not enough to maintain low packet loss but rather overall link capacity needs to be increased. Increasing bandwidth/capacity requires additional cost and is not an effective solution for temporary congestion (micro-bursts). Further the authors of the two works did not evaluate the effect of packet loss.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2971429, IEEE Transactions on Smart Grid

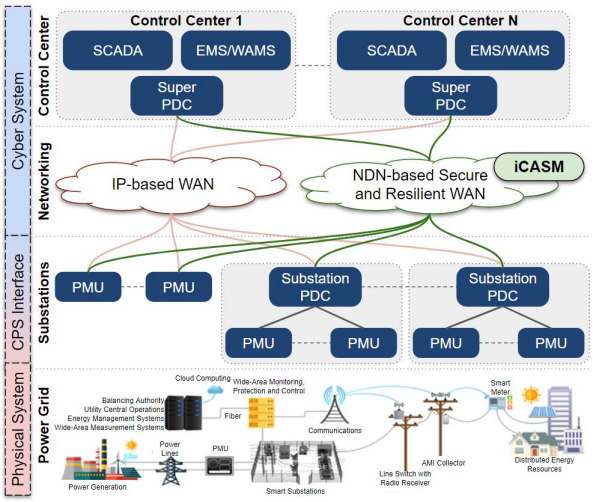


Fig. 1: IP-based and Proposed ICN-based CPS for WAMS

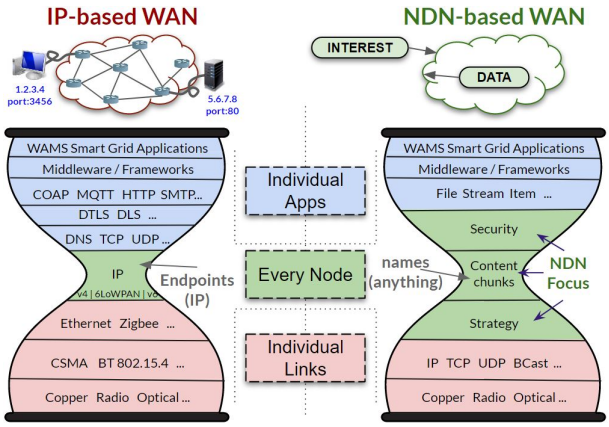


Fig. 2: Protocol Stack and Networking for IP-based and NDN-based WAMS Communication for Smart Grid Applications

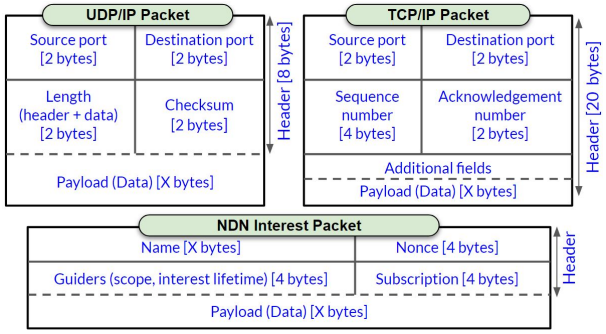


Fig. 3: Packet Schematic: UDP/IP, TCP/IP and NDN (*Interest*)

Deng *et al*. [15] also proposed an IP-based solution using MPLS traffic engineering and QoS implementation. Their approach also cannot handle congestion on best-route paths (e.g., by packet re-routing). Thus, packet drops will occur with high probability when the traffic rate tends to approach the link capacity on best-route paths, consequently increasing the latency. Multicast routing proposed by [16] for decentralized control reduced network traffic overhead. Likewise, Multipath Transmission Control Protocol (TCP) [17], and Equal-Cost Multi-Path (ECMP) [18] aim to use diverse network paths but all these still rely on best-paths for data flows.

Tourani *et al*. [19] proposed the use of ICN as an architecture of choice for smart grid networks, which is more promising, their proposal was neither compared to any specific smart grid application nor compared it with TCP or User Datagram Protocol (UDP) for validation.

III. IP-based and Proposed ICN-based WAMS Communication

The conventional IP-based and proposed ICN-based Cyber-Physical System (CPS) layered framework for WAMS is depicted in Fig. 1. Our architecture is based on Named Data Networking (NDN) [20], an architecture based on the ICN paradigm. Fundamentally, the packet structure, routing and forwarding of the data, and the capability of routers are different between the IP and NDN paradigms. The protocol stacks and basic networking principles for IP and NDN are shown in Fig. 2. Fig. 3 shows the schematics of the packets in IP and in NDN. The payload (PMU data) can be configured to be the same size. The header length, which varies in each protocol, thus becomes a significant contributor to network latency. An NDN *Interest* packet as defined in [20] does not include the payload field. However, we have used payloaded *Interest* as implemented in [19] to simulate the push-based mechanism for sending PMU data to PDCs.

A. Communication Systems

1) IP-based Communication: An IP packet is made up of a header and a payload (PMU data), where the header includes an *source* and *destination* IP address fields with fixed size and would act as a representative of the data source and data destination to facilitate peer-to-peer IP-based packet routing. The size of packet headers differ based on the type of transport layer protocol used and also on the data payload. The two transport protocols used in the IP are TCP [21] and UDP [22]. UDP header size is 8 bytes while TCP header has a minimum length of 20 bytes. The payload size can vary based on factors such as data segmentation size of an application and Maximum Transmission Unit (MTU) of a network's links.

TCP is a connection-oriented protocol which achieves communication reliability by re-transmitting lost packets. In contrast, UDP is a connection-less protocol, which offers unreliable communication with a lower packet delivery rate. Though the re-transmission feature in TCP is important to ensure high reliability, it also introduces additional network latency for the re-transmitted packets.

2) NDN-based Communication: NDN has two types of packets, *Interest* and *Data*. An NDN packet is also made up of a header and a payload, where the header includes a *name* field with variable size and would act as a representative of the data to be retrieved and facilitates NDN-based packet routing. The length of the header depends on the namespace used to identify the requested data. An NDN namespace is a hierarchical representation of the names by which data can be accessed over an NDN network. For example, the name */wecc/california/sandiego/pmu1* can be used to retrieve details about *pmu1* in San Diego, California, which is part of the Western Electricity Coordinating Council (WECC) power grid. In NDN, a node that needs data sends an *Interest* into

TABLE I: IP-based and proposed NDN-based (*iCASM*) WAMS Communication Properties

	IP-based WAMS Network Design Properties	NDN-based WAMS Network Design Properties
Packet Header Size	8 bytes for UDP and 20 bytes for TCP	Depends on the size of namespace
Packet Payload Size	Depends on the application	Depends on the application
Connection	UDP is connection-less and unreliable. TCP is connection-oriented and reliable	NDN is connection-less and has no dedicated transport layer. Transport and reliability mechanisms are moved into applications.
Network Size (End hosts)	Limited to the IPv4 or IPv6 address space	Unlimited, as it depends on the unconstrained namespace
Security	End-to-end channel is secured and authenticated.	Data chunks are directly secured and individually authenticated.
Communication	Client-server model, host-centric (address-centric), conversation oriented, peer-to-peer model, distributed model	Distributed model, information-centric, content interest oriented
Unicast and Multicast	Unicast is by default. Multicast needs an explicit implementation and is not trivial	Implicit - Simple and based on routing strategy chosen
Domain Name Service (DNS)	It works on DNS by translating names to IP addresses	It works on forwarding the *Interest* request to neighboring intelligent routers. NDNS is named-DNS
Information dissemination	Can be inefficient (multiple packets in unicast)	Large scale and more efficient
Router	It stores the addresses of next hops, and thus establishes a loop-free shortest path. Propagation based on IP prefix.	It has Forwarding Information Base (FIB), Pending Interest Table (PIT) and Content Store (CS). Establishes multiple paths that can be utilized concurrently to avoid congestion based on forwarding strategy. Propagation based on name-prefix.
Network content storage	No in-network content storage	In-network storage at router's content cache (CS) that facilitates low latency for popular content
Bandwidth and Throughput	No optimization of Bandwidth and congestion may occur	Optimization of Bandwidth and mitigates congestion using different routing strategies.

the network for a particular name. The network's built-in intelligence retrieves the requested data either from the content provider or an intermediate node caching the content replica corresponding to the name.

An NDN router maintains three data structures namely Content Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB). The CS is used to temporarily cache *Data* packets that a router has received. The PIT is used to store *Interest* not yet satisfied by a *Data* packet. If a request has not been satisfied after a configured time-out value, the PIT entry is deleted to free up space. The FIB is populated by a named-based routing protocol (e.g., Named-data Link State Routing Protocol (NLSR) [23]) and maintains forwarding information to help routers transmit packets using appropriate network interfaces. Additionally, an NDN router also implements a Forwarding Strategy module which is used to make decisions on how packets should be forwarded (TCP/IP has no equivalent layer in the OSI stack). The NDN architecture is such that it can be deployed on top of other transport protocols such as (TCP or UDP) or run natively on link layer protocols, such as Ethernet [24].

B. PMU Packet Data Routing

IP uses either unicast or multicast routing to select communication paths for PMU packets. Unicast is used to forward packets to a single host (one-to-one communication). Multicast, on the other hand, enables in-network packet replication and delivery to multiple hosts, which have subscribed to receive the data (one-to-many communication). IP-based communication can leverage load-sharing mechanism, in which a forwarding node changes the outgoing interfaces for successive packets or flows, to distribute traffic load. However, this load-sharing mechanism can neither send the same packet on multiple interfaces nor utilize all available paths concurrently.

In contrast, NDN's forwarding strategy allows a forwarding node to decide how PMU packets are forwarded (in the *strategy layer*). This feature enables NDN to outperform IP in packet delivery. This flexibility has an added advantage of allowing the design of various forwarding strategies for different applications. NDN allows different forwarding strategies to be applied to different *names/namespaces*, which can be used to support QoS implementations.

While IP was designed to work as a host-centric communication architecture, NDN is designed to enable networks to work more like content distribution networks with no requirement for host-to-host communication. Table I shows the IP-based and proposed NDN-based WAMS communication properties.

IV. *iCASM* Design: Proposed NDN-based Resilient Strategy for WAMS-based Applications

The proposed NDN-based WAMS smart grid architecture (*iCASM*), enables a node (e.g., an NDN router) to send a packet over multiple of its available outgoing interfaces concurrently. We leverage this feature to enable more reliable packet delivery with low latency when congestion occurs on best-route paths. Additionally, we consider to include the QoS requirements into *names* so that routers along a path can provide prioritized forwarding treatment to urgent or emergency packets during network congestion.

Each NDN node stores the interfaces through which it can retrieve a content (name of a service) from the network in its forwarding table. The strategy layer then allows a node to deploy a desirable forwarding strategy (e.g. all available interfaces, best paths, etc.) to forward each packet. In our framework, all available paths between any source and destination pair are potential transmission routes. We do not propose a new method to compute optimized transmission

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2971429, IEEE Transactions on Smart Grid

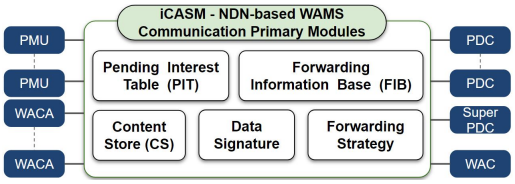


Fig. 4: *iCASM*: NDN-based WAMS Communication Modules

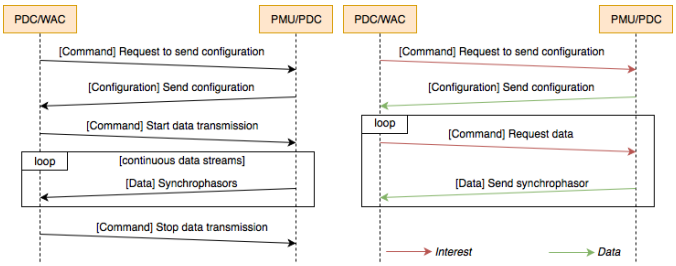
routes (available routing protocols can be used for filling the forwarding information base at the routers to this effect), we use a strategy where a router can forward packets on all available interfaces, based on the assumption that PMU packets are time sensitive.

In this paper, our aim is to show how NDN can enhance packet delivery success in a dynamic network. We considered WAMS monitoring and control data as high-priority (urgent) flows, hence the routers will forward the corresponding packets on all available interfaces when they receive a packet–significantly increasing the probability of timely delivery. We do not provide any preferential treatment to our control application packets (an area of potential future work). The other flows are fictitious congestion flows that are deployed to demonstrate resiliency. In a real-world smart grid, a node will decide which (and how many) interfaces to use as per the need of the flow requesting service. By utilizing multiple-interface forwarding, redundant network capacity (bandwidth) is not left unused but rather used to support improved packet delivery and low latency during peak traffic periods. As previously shown in [25], a selection of a subset of available interfaces can also be made to meet a desired optimization objective, without sending on all interfaces. However, in this paper, for simplicity, we assume all interfaces are used.

Fig. 4 shows the primary modules to simulate NDN-based WAMS communication across the PMUs, PDCs, and Wide-Area Control Actuators (WACAs). Fig. 5 shows the data interactions between PMUs and PDCs/WACs. Fig. 5a shows the interaction in IP. Before a PMU starts transmitting data, there is an initial handshake between the PMU and PDC/WAC to determine the format of the data packets. Once this handshake is completed, the PDC/WAC sends a command frame to the PMU to start transmitting data. If data transmission is to be terminated, the PDC/WAC again sends a command to the PMU to stop sending data. Fig. 5b shows similar communication process for the case of NDN. The difference being that each *Data* packet is sent in response to an *Interest* packet from the PDC/WAC. Thus, there is no explicit request to stop data transmission in NDN.

A. Reliability

TCP offers reliability at the expense of additional latency due to re-transmissions. NDN's multiple-interface forwarding strategy has the potential of providing lower latency but with better reliability by optimal use of redundant links. We are proposing the multiple-interface strategy to be used for important and critical data in a smart grid network, such as real-time PMU data exchange in WAMS. Other non-critical data exchange in smart grid that allow higher network latency and less reliability may be forwarded using unicast or other customized strategies. It can be argued that our approach is equivalent to the IP-broadcast feature, however, broadcast traffic in IP is limited to only the local area network (LAN) and gets dropped by egress-routers connecting to other networks. Further, in *iCASM* a node does not have to use all its interfaces, in most cases a subset of available interfaces would suffice [25]–multicast and not broadcast.



(a) Communication in IP (b) Communication in NDN

Fig. 5: Communications between PMUs and PDC/WAC

B. Security

The observability, controllability, and stability of a power grid does not only depend on reliable packet delivery and low latency. Network and data security are other key requirements. The communication network for the smart grid should be designed to mitigate security attacks on both data in transit and data at rest. The NDN architecture introduces the concept of signed *Interest* and *Data* packets, which guarantees data integrity and provenance. Data integrity is the use of validation mechanisms to detect when data has been compromised or altered. Data provenance allows data to be traced back to its producer, enabling the assurance that the data originator cannot deny ownership.

In NDN, the packets can be individually encrypted as independent units with the conventional encryption algorithms, such as advanced encryption standard (AES) and triple data encryption standard (TDES). Contrary to NDN, the traditional IP architecture employs encryption in the end-to-end tunnel concept (e. g., using secure socket layer) to provide end-to-end data security. Consequently, in IP, intermediate routers are blind to the content they are forwarding and cannot verify signatures for provenance or integrity, thus are unable to mitigate attacks such as Denial-Of-Service (DoS) attacks.

We point out that our proposed multiple-interface forwarding strategy is susceptible to DoS or Distributed DOS (DDoS) attacks. This can be in the form of *Interest* flooding attack in which the attacker(s) sends *Interest* packets at very high rate into the network using the same namespace used by legitimate WAMS nodes to congest all the available paths. NDN can limit such downstream-initiated DoS/DDoS attacks by aggregating requests for the same data. However, in our case, where the data goes in the payloaded *Interest* from a PMU, there is no scope for aggregation (each *Interest* is unique); this creates a potential for DoS. Proposed mitigation techniques, such as traffic rate-limiting at a forwarding router, including advanced techniques suggested by [26], [27] can be employed. Security is, however, not the main focus of this paper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2971429, IEEE Transactions on Smart Grid

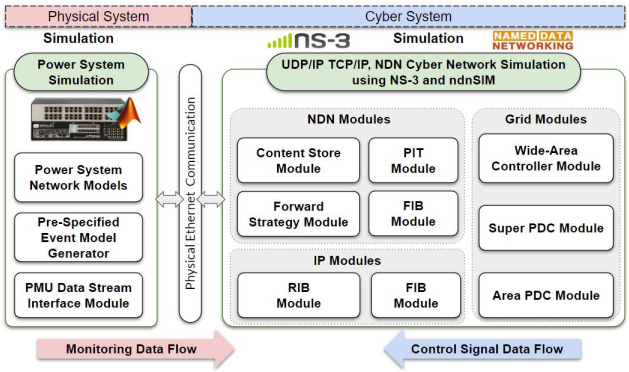


Fig. 6: iCASM Testbed Implementation Architecture

TABLE II: Different Simulation Cases for TCP, UDP & NDN

	Description	Reason for Test Case
Case 1	No congestion	Network operating under ideal conditions
Case 2	Link congestion introduced for 2% of the total simulation time	Network experienced peak traffic momentarily
Case 3	Link congestion introduced for 50% of total simulation time	Network experienced peak traffic for noticeable period

V. Evaluation and Validation of IP and NDN for WAMS Application

Fig. 6 shows our design for the integrated power and network system simulation. The experiments include MATLAB-based power system simulator (Power System Simulation Module) including PMUs, and IP- and NDN-based networking simulator (Cyber System Simulation Module) including PDCs and customized Central Controller.

A. Power System Simulation Module - IEEE-39 Bus Test Case

We used the IEEE-39 bus power system model [28] shown in Fig. 7. We have derived a substation-branch topology model from the bus-branch topology to characterize a suitable communication network topology, resulting in 27 substation nodes. The grouped buses under a substation are highlighted in blue rectangles. The cyber network topology has a router deployed at each substation and in the network core as shown in the figure and is used to test the proposed NDN-based and IP-based [29] approaches for a WAC application. Each of the ten generators is equipped with multi-band Power System Stabilizer (PSS). A wide-area PSS (WAPSS) [30], acting as a WACA, is deployed at each generator to process WAC signals received from control center (WAC loop). The data flow is: PMUs $\rightarrow$ area PDCs $\rightarrow$ super PDC $\rightarrow$ WAC $\rightarrow$ WACA.

B. Cyber System Simulation Module - IEEE-39 Bus Test Case

We have modeled the above mentioned cyber system on the ns-3 [31] and ndnSIM [32] network simulators. The PMUs send data to PDCs at 60 packets/sec, which is consistent with the current generation of PMUs. We created temporary path congestion in the communication network to evaluate the resiliency of the compared protocols in our experiments. Each of the two congestion injection nodes send 5000 packets/sec using packets of size 1024 bytes resulting in 5.12 Mbps throughput which is sufficient to congest the core network links. The links used to connect the nodes in our experiments

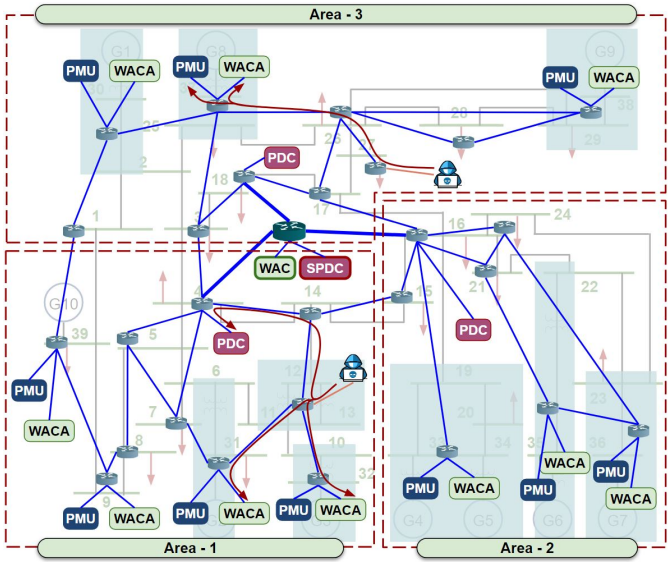


Fig. 7: Superimposed Cyber over Power System for IEEE-39

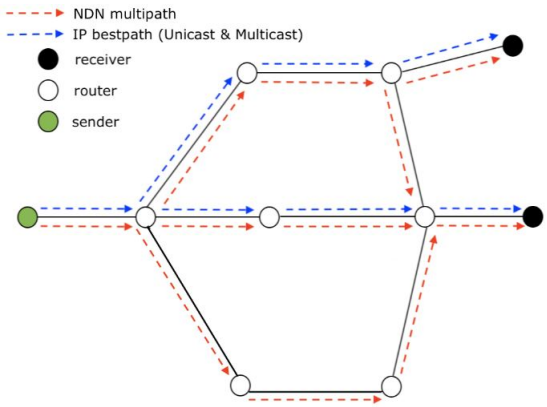


Fig. 8: Packet forwarding strategies in NDN and IP

use the Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) [24] Layer-2 medium access protocol.

To better evaluate the protocols, we have conducted three experiments as shown in Table II. Total simulation time for each scenario is 300 secs. For Case 1, we did not introduce any congestion into the network. In Case 2, we congested some of the best path links for a short time (2% of the total simulation time). The congested best paths are indicated by the flow arrows shown in Fig. 7. In Case 3, we made the congestion last longer (50% of the total simulation time).

Our simulation uses the native NDN deployment over Ethernet (standalone NDN mode). This is done with the aim of having a fair comparison with the IP protocol as well as evaluating the architecture in its native form. Our assertion is that TCP and UDP are not needed, but in fact add extra overhead to communications. We did not use NDN's in-networking caching in our experiments because our flows involve real-time communications. However, other power system use-cases might find caching capability useful especially in publish-subscribe scenarios (e.g., EMS business and market transactions).

In our experimentation, the *Data* payload sizes used for NDN, UDP, and TCP simulations were configured to be 100 bytes, which is larger than the typical PMU frame size

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2971429, IEEE Transactions on Smart Grid

(40 to 70 bytes), with the aim of demonstrating scalability for possible future frame sizes. Our experiments used the ns-3 implementation of default TCP and UDP protocols without any changes. For the IP (TCP and UDP) simulations, routing is dynamically calculated based on the least cost path between any source and destination pair. Similarly, in NDN simulations, the least cost paths are selected dynamically. The dynamic route selection algorithms are ns-3 and ndnSIM default implementations.

Fig. 8 shows the forwarding strategies used in our experiments. It illustrates a scenario when one sender transmits the same information to two receivers. Notice that the IP paradigm follows a loop-free path whereas NDN paradigm utilizes multiple paths to reach the destination. We have considered unicast in IP experiments and multiple interface forwarding in NDN. We did not experiment with IP multicast since, as stated in Section II, the resultant packet forwarding effect becomes the same as IP unicast.

C. Power and Cyber System Interface

We derived substation topology for the IEEE-39 bus topology, where each substation node includes a bus or a set buses connected via transformers. Subsequently, we have designed a network topology with 27 routers for the 27 substations, 10 WACAs and 10 PMUs at generator substations, 3 area PDCs, 1 super PDC, 1 WAC, and 2 adversary nodes for congestion injection as shown in Fig. 7.

In the simulation, PMUs send data to PDCs in Area-1 and Area-3 only as these are the areas we introduced congestion into the network. The routers forward SCADA data, WAMS data and non-periodic IT data that may cause traffic congestion. The WACAs, PMUs, PDCs, WAC and background data injection nodes are connected to the routers using links having 5 Mbps bandwidth and 1 ms propagation delay. The core of the network consisting of interconnected routers, has 4 Mbps links with 1 ms propagation delay. We made the link capacity in the network-core to be less than those of the end-nodes to better simulate congestion on the best-route links.

D. Discussions and Analysis of Results

1) Communication Network Metrics: For evaluation, we have conducted detailed analysis on the a) network latency and b) packet loss metrics. Fig. 9 shows the packet loss comparison across the three cases experimented for TCP, UDP, and NDN. With no network link congestion (Case 1), both UDP and NDN have 0% packet loss, which is expected. TCP experienced a negligible amount of packet loss (0.003%). For Case 2 (short duration link congestion), TCP and UDP recorded 0.05% and 0.52% packet losses, respectively with NDN having zero loss. As we increase the congestion period (Case 3), we observed TCP and UDP recording 0.71% and 19.52% packet losses, respectively. This is expected. These losses were recorded while we congested only few network paths in our experiments (flow arrows shown in Fig. 7). Some of the PMU to PDC flows used paths that were not affected by the congestion. When the number of congested paths increased, a lot more packets will be lost. Importantly, NDN recorded 0% packet loss

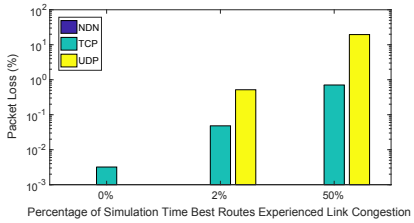


Fig. 9: Packet Loss Comparison (NDN has 0% loss)

regardless of network congestion even without any specific preferential scheduling based treatment to any PMU packets in our simulation. This demonstrates the efficacy of the strategy of NDN.

Fig. 10 shows the Cumulative Distributive Function (CDF) of network latency for the three congestion cases. In all three cases, UDP recorded the least network latency (the green UDP curve is closest to the Y-axis), followed by TCP, and then NDN. This is expected since UDP has the smallest header size (8 bytes), followed by TCP (20 bytes), and NDN (40 bytes). It is worth mentioning that in Case 3, NDN delivered 100% of its packets under 30 ms while UDP and TCP delivered 75% and 80% of their packets under 30 ms, respectively. Note that the upper bound delay of 1 second causes the line for UDP and TCP to snake towards $X = 1$ second for $Y = 1.0$ representing several packet losses (particularly for TCP, which reaches $X = 1$ second). The network latency for TCP increases considerably when congestion lasts for longer duration due to re-transmission of lost packets. Even with increased latency, a lot more packets were delivered in TCP than in UDP as shown in Fig. 9. For all cases, NDN latency is not visibly affected by congestion (all packets delivered in under 30 ms).

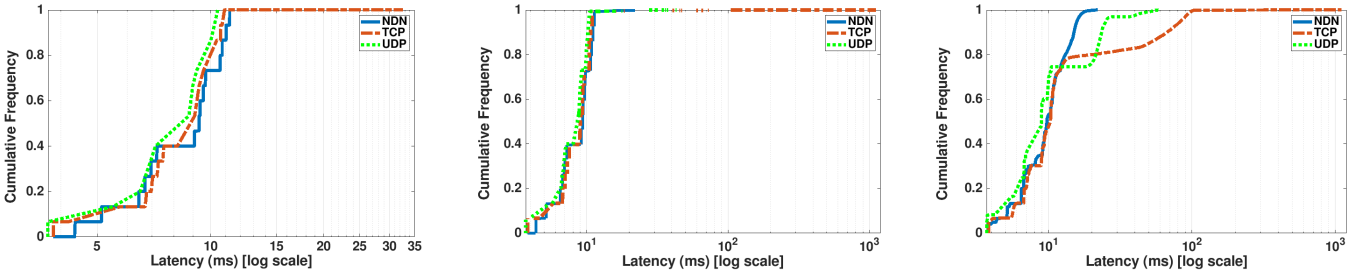
Table III shows the mean latencies observed for delivered packets. The mean latencies of TCP and UDP are very far from that of NDN in the congestion scenarios. The median latencies being similar imply that the latencies affect a small portion of packets (we do not simulate serious congestion), but the latencies and losses are significant.

TABLE III: Mean and Median Latency For *Delivered Packets*

	NDN		TCP		UDP	
	Mean	Med.	Mean	Med.	Mean	Med.
Case 2 (No Congestion)	8ms	9ms	8ms	9ms	8ms	8ms
Case 2 (Congestion)	10ms	10ms	18ms	10ms	13ms	8ms
Case 3 (No Congestion)	8ms	9ms	8ms	9ms	8ms	8ms
Case 3 (Congestion)	10ms	10ms	24ms	10ms	13ms	8ms

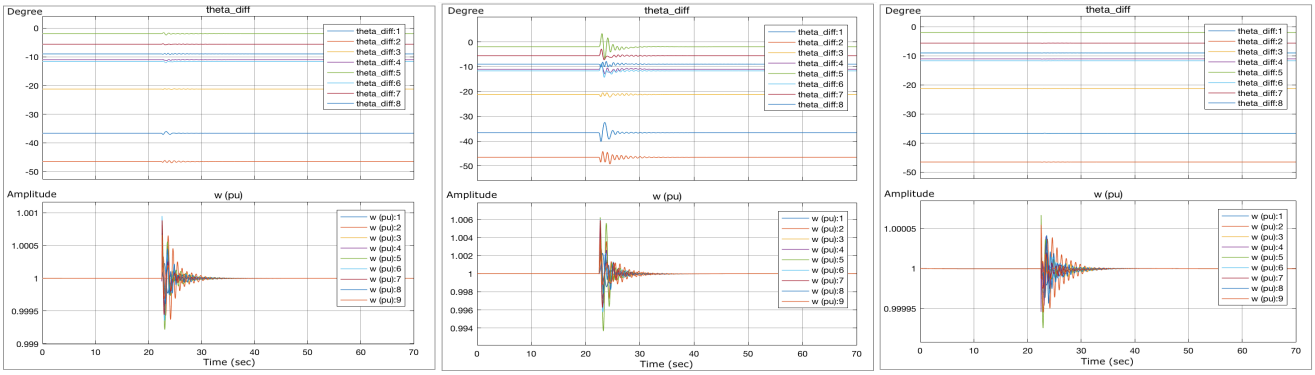
2) Grid Impact Characteristics: High latency and high packet losses affect the performance of wide-area control loop. We designed a MATLAB-based model to assess how latency and packet losses of the wide area measurement and control signals impact the grid when disturbances occur. Angle stability assessment is carried out on the IEEE 39-bus system for a three-phase bolted fault scenario at different clearing times and operating conditions. We used latency and packet loss statistics from the network simulations, representing network dynamics, as input into the WACA to illustrate how *iCASM* and the equivalent IP-based network perform. It was observed that the network dynamics resulting in *iCASM* had lesser adverse impact on the essential angle stability than IP.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2020.2971429, IEEE Transactions on Smart Grid



(a) 0% Congestion (b) 20% Congestion (c) 50% Congestion

Fig. 10: Latency Comparison for Different Congestion Duration on a 300 sec Simulation



(a) TCP (b) UDP (c) NDN

Fig. 11: Effect of IP-based (TCP & UDP) and NDN-based Architecture on Grid Stability

For our analysis, we used the results obtained from simulation Case 3 as referenced in Table II, where network congestion lasted 50% of the simulation time. To account for both latency and packet loss metrics, we assigned a 1 sec latency penalty (as a smoothing function) to each packet loss. For all three protocols (TCP, UDP, NDN), we computed the mean latency between PMU and PDC packet transfer. This mean latency is fed into the MATLAB model as the period of time the WAC has to wait for signals to be able take a control action when disturbance data is sent from the PMUs.

Fig. 11 shows the generator response–rotor angles (degrees) and frequency (per unit)–for a three-phase bolted fault at 22.5 s, cleared in 100 ms, under congested case, using the three protocols. We assumed that fault detection time at PMU is instantaneous. Clearly the control action is the best with *iCASM* (Fig. 11c), as the oscillation peak is significantly reduced (due to faster, more reliable bidirectional packet delivery). Thus, it can be concluded that *iCASM* provides faster, reliable, and resilient transmission under network congestion, which results in better dynamic performance of the WAMS.

Note that when all the links in the network are equally congested, the use of multiple paths may not provide significant advantage. But we note that the stochastic nature of the traffic and queuing may result in the proverbial, "whole is greater than the sum of the parts." With routers using the *iCASM* strategy, there is a much better chance that a packet will make it to the destination.

3) Impact on other Traffic: The PMU data gets access to all interfaces for transmission from a router (this is how we define high priority), this could result in other data getting delayed. As we show in our simulations (also true in practice), the PMU messages we are using for control do not consume a lot of bandwidth as is seen from the data flows. If all 10 PMUs are transmitting at 60 packets/sec the total PMU traffic bandwidth in the network is 0.48 Mbps; with the least link bandwidth in the network being 4 Mbps (over 85% of the bandwidth is still available on a link). In addition, if used for urgent event and control messages, which are infrequent, only a few messages need to reach the PDC/super PDC. Further, other grid transmissions tend to not have a delay requirement and can be delivered reliably with retransmissions. Thus, non-PMU messages may experience some, insignificant increased delay on account of our special treatment of PMU messages.

VI. Conclusion

In this paper, we presented an evaluation of network latency and packet loss for a WAMS application used in smart grids. We proposed *iCASM*, an NDN architecture in which network routers concurrently forward the same packet on multiple interfaces in order to utilize available redundant network paths and offer higher reliability and lower latency than IP in terms of packet delivery. Using MATLAB, we modeled the latency and packet losses of the measurement signals impact on the power grid in terms of recovery time after disturbances and show our architecture's efficacy.

Acknowledgment

Research supported by US NSF awards #1800088; #1719342; #1345232, #1914635, EPSCoR Cooperative agreement OIA-1757207; and US DoE SETO award number DE-EE0008774 grant. Opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the federal government.

REFERENCES

[1] R. Hasan, R. Bobba, and H. Khurana, "Analyzing naspinet data flows," in *IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1–6.

[2] V. Terzija and *et al.*, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, 2011.

[3] C. H. Hauser, D. E. Bakken, and A. Bose, "A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid," *IEEE Power and Energy Magazine*, vol. 3, no. 2, pp. 47–55, 2005.

[4] T. Bi, J. Guo, K. Xu, L. Zhang, and Q. Yang, "The impact of time synchronization deviation on the performance of synchrophasor measurements and wide area damping control," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1545–1552, July 2017.

[5] Synchrophasors and the grid. U.S. Department of Energy. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/09/f36/2_Modern%20Grid-networked%20Measurement%20and%20Monitoring%20Panel%20-%20Alison%20Silverstein%2C%20NASPI.pdf

[6] Unified real time dynamic state measurement. Power Grid Corporation of India Ltd. [Online]. Available: http://www.cea.nic.in/reports/committee/scm/allindia/agenda_note/1st.pdf

[7] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, 2012.

[8] L. Zacharia, L. Hadjidemetriou, and E. Kyriakides, "Integration of renewables into the wide area control scheme for damping power oscillations," *IEEE Transactions on Power Systems*, 2018.

[9] J. W. Stahlhut, T. J. Browne, G. T. Heydt, and V. Vittal, "Latency viewed as a stochastic process and its impact on wide area power system control signals," *IEEE Trans. on Power Systems*, vol. 23, no. 1, pp. 84–91, 2008.

[10] N. Youssef, Y. Barouni, S. Khalfallah, J. Slama, and K. Driss, "Mixing sdn and ccn for content-centric qos aware smart grid architecture," in *IEEE/ACM Quality of Service Conference (IWQoS)*, 2017.

[11] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (sdn)," *Computer Networks*, vol. 112, pp. 279–293, 2017.

[12] M. Chenine, E. Karam, and L. Nordstrom, "Modeling and simulation of wide area monitoring and control systems in ip-based networks," in *Power & Energy Society General Meeting (PES)*. IEEE, 2009, pp. 1–8.

[13] S. Müller and *et al.*, "Interfacing power system and ict simulators: Challenges, state-of-the-art, and case studies," *IEEE Tran. on Smart Grid*, 2016.

[14] M. Chenine, I. Al Khatib, J. Ivanovski, V. Maden, and L. Nordström, "Pmu traffic shaping in ip-based wide area communication," in *IEEE Critical Infrastructure (CRIS)*, 2010, pp. 1–6.

[15] Y. Deng and *et al.*, "Communication network modeling and simulation for wide area measurement applications," in *IEEE ISGT Conference*, 2012, pp. 1–6.

[16] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE JSAC*, vol. 30, no. 6, pp. 1097–1107, 2012.

[17] A. Ford, C. Raiciu, M. Handley, S. Barre, J. Iyengar, *et al.*, "Architectural guidelines for multipath tcp development," *IETF, Informational RFC*, vol. 6182, pp. 2070–1721, 2011.

[18] C. Hopps. (2000, Nov.) Analysis of an equal-cost multi-path algorithm. IETF, RFC 2992. [Online]. Available: https://tools.ietf.org/html/rfc2992

[19] R. Tourani, S. Misra, T. Mick, S. Brahma, M. Biswal, and D. Ameme, "icens: An information-centric smart grid network architecture," in *IEEE SmartGridComm Conference*, 2016, pp. 417–422.

[20] L. Zhang and *et al.*, "Named data networking," *ACM SIGCOMM CCR*, vol. 44, no. 3, pp. 66–73, 2014.

[21] J. Postel *et al.*, "Transmission control protocol rfc 793," 1981.

[22] J. Postel, "User datagram protocol," *Isi*, 1980.

[23] A. Hoque and *et al.*, "NLSR: Named-data link state routing protocol," in *ACM SIGCOMM Information-Centric Networking Workshop*, 2013, pp. 15–20.

[24] IEEE, "IEEE standards for local area networks: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications," *ANSI/IEEE Std 802.3-1985*, pp. 1–146, Dec 1984.

[25] G. Panwar, R. Tourani, T. Mick, A. Mtibaa, and S. Misra, "DICE: Dynamic multi-RAT selection in the ICN-enabled wireless edge," *ACM SIGCOMM CCR*, vol. 47, no. 5, pp. 67–72, 2017.

[26] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *IFIP Networking Conference*. IEEE, 2013, pp. 1–9.

[27] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding DDoS attacks in named data networking," in *IEEE Conference on Local Computer Networks (LCN)*, 2013, pp. 630–638.

[28] T. Athay, R. Podmore, and S. Virmani, "A practical method for the direct analysis of transient stability," *IEEE Transactions on Power Apparatus and Systems*, no. 2, pp. 573–584, 1979.

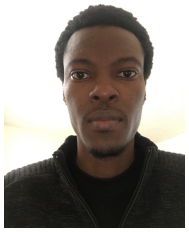
[29] G. Ravikumar, G. Ramya, S. Misra, S. Brahma, and S. A. Khaparde, "ipacs: An integrative power and cyber systems co-simulation framework for smart grid," in *IEEE PES General Meeting*, July 2017, pp. 1–5.

[30] I. Kamwa, S. R. Samantaray, and G. Joos, "Optimal integration of disparate c37.118 pmus in wide-area pss with electromagnetic transients," *IEEE Trans. on Power Systems*, vol. 28, pp. 4760–4770, Nov 2013.

[31] G. Carneiro, "Ns-3: Network simulator 3," in *UTM Lab Meeting*, 2010.

[32] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnsim 2: An updated ndn simulator for ns-3," NDN-0028, R2, Tech. Rep., 2016.

Gelli Ravikumar Gelli Ravikumar is an Assistant Research Professor in the ECE Department of Iowa State University (ISU), USA. Prior to this he was a postdoctoral researcher at the ISU and at New Mexico State University, USA. He received a Ph.D. degree in the Electrical Engineering department at the Indian Institute of Technology Bombay (IIT-B), India. His research expertise is in the areas of power system control and analysis, system stability, AI and machine learning, attack-resilient control algorithms, and smart grid CPS security.



Dan Ameme Dan Ameme completed his M.S. in Computer Science at NMSU in 2018 and is continuing as a PhD student. His research interest is in the smart grid.

Satyajayant Misra (SM'05, M'09) is an associate professor in computer science at New Mexico State University. He completed his Ph.D. in Computer Science from Arizona State University, Tempe, AZ, USA, in 2009. His research interests are in wireless networks, the Internet, and smart grid architectures and protocols. He served on several IEEE/ACM journal editorial boards and conference executive committees including editorship in IEEE IoT Journal and IEEE Wireless Communication Magazine. He has authored over 80 peer-reviewed publications.

Sukumar Brahma Sukumar Brahma (M'2004, SM'2007, F'2020) received his B.E. from Gujarat University, Ahmedabad in 1989, Master of Technology from IIT Bombay in 1997 and PhD from Clemson University in 2003; all in Electrical Engineering. He is the Dominion Energy Distinguished Professor and director of Clemson University Electric Power Research Association (CUEPRA) at Clemson University. He is the past Chair of IEEE Power and Energy Society's Distribution System Analysis Subcommittee and Power and Energy Education Committee. He is a member of the Power System Relaying and Control committee and an editor for IEEE Transactions on Power Delivery.

Reza Tourani received his B.S. in computer engineering from IAUT, Tehran, Iran, in 2008, M.S. in computer science from NMSU, Las Cruces, NM, USA, in 2012 and Ph.D. in 2018. He is an assistant professor in computer science at St. Louis University. His research interests include smart grid communication architecture and protocol, wireless protocols design and optimization, future Internet architecture, and privacy and security in wireless networks.