2016 IEEE International Conference on Smart Grid Communications (SmartGridComm): Communications, Networks and Architectures to Enable the Smart Grid

iCenS: An Information-Centric Smart Grid Network Architecture

Reza Tourani†, Satyajayant Misra†, Travis Mick†, Sukumar Brahma‡, Milan Biswal‡ and Dan Ameme†⋆
†Department of Computer Science and ‡Electrical Engineering Department
New Mexico State University
{rtourani, misra, tmick}@cs.nmsu.edu, {sbrahma, milanb, danameme}@nmsu.edu

***Abstract*—Smart grid technologies will equip the electrical grid of the future with two-way information flow between grid entities and consumers. This bidirectional information flow facilitates improved grid monitoring, control automation, energy efficiency, and sustainability. Several smart grid networking architectures have been proposed recently. However, the majority of these are restricted to subdomains such as home area networks or substation networks, or are not scalable. There is a need for an overarching and inclusive communication architecture which accounts for all smart grid communication scenarios.**

In this paper, we propose *iCenS*, a holistic smart grid networking architecture. We identify various communication scenarios, elaborate on the suitability of iCenS, and discuss how it can be used to solve smart grid networking challenges. We also present simulation results demonstrating the scalability of our design and its effectiveness in serving various types of smart grid traffic.
Keywords: **Smart grid architecture, information-centric networking, networking architecture.**

I. Introduction

The US Department of Energy (DoE) defines the *smart grid* as a class of technology which provides bidirectional communication between the entities of the power grid, enabling effective remote control and automation aimed at improving efficiency, reliability, and grid protection [1]. Smart grids are anticipated to be the "holy grail" for solving the crisis of worldwide energy demand, which is expected to increase 70% by 2035 [2]. Smart grids will allow integration of distributed energy generation and storage resources (e.g., solar panels, wind turbines, electric vehicles, batteries) to allow the creation of self-sufficient local microgrids, where each customer can become both an energy producer and a consumer (prosumer).

Motivation: The smart grid is envisioned to integrate individual consumers into the energy market, allowing them to make intelligent energy transaction decisions. A bidirectional information flow capable of fine-grained and real-time demand-response, monitoring, and maintenance is also requisite. The biggest cog-in-the-wheel in the smart grid effort is the networking and communication architecture, which will facilitate the envisioned information flows. Hence, a scalable architecture that satisfies smart grid communication requirements such as high-volume network traffic, low-latency data delivery, and interoperability in heterogeneous networks, is imperative. There have been attempts in the past to design smart grid networking architecture [3], [4], [5], [6]. However, these approaches have either been restricted to looking at a specific subdomain, such as a home area network [7], do not scale for the large number of entities and communications that will happen in a smart grid, or are not backward compatible with current communication standards such as IEC 61850 [8]. We believe that there is a need for a holistic networking architecture that can meet the needs of all smart grid communication, be it for grid maintenance and management or for energy transactions and demand-response.

In this paper, we attempt to address this requirement by proposing *iCenS*, a novel networking architecture for the complete smart grid. Our architecture is inspired by the information-centric networking (ICN) communication paradigm [9], [10]. In an information-centric network, each piece of data is assigned a unique name. The data may be obtained by making a request using this name; contrast this to the host-centric paradigm in current networks, wherein a request must be destined to a particular address. ICN also allows named content to be cached at the network edge, closer to end users. Beyond caching, ICN provides facilities for data provenance and request aggregation, which are pertinent for smart grid communications. Several ICN architectures have been proposed, notably NDN [9] and PSIRP [10]. Despite their differences, these architectures all agree on the core tenents of name-based routing and content caching.

Our Contributions: We propose an information-centric networking architecture that is composed of a three-level logical hierarchy for information flow. We discuss the details of the iCenS architecture and illustrate how it can meet the communication requirements of smart grid. We also present a simulation-driven evaluation of the scalability of iCenS.

In Section II, we discuss the state of the art in information-centric networking and smart grid communication. In Section III, we elaborate on the detailed design of iCenS. Section IV presents how iCenS can be used to address the particular requirements of smart grid. In Section V, we present the results of our simulations. We conclude the paper in Section VI.

II. Related Work

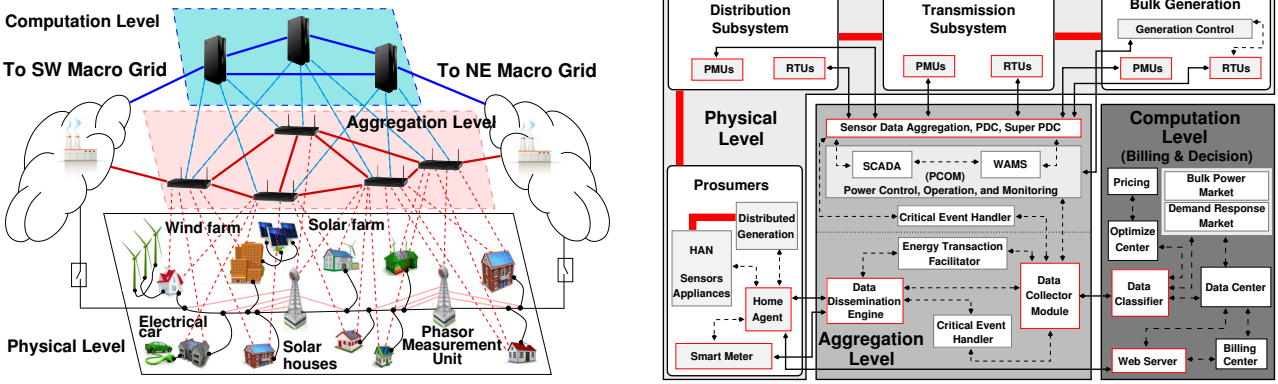
The proposed smart grid network architectures may be classified into two major groups: host-centric networks, and data-centric networks. We review some of the host-centric (IP-based) designs, then focus on the proposed data-centric architectures.

Smart grid IP-based architectures have been proposed in [4], [5]. However, these designs fail to address the communication requirements of a distributed energy market. In the distributed energy market, producers advertise their energy generation profiles and consumers advertise their demand details. For an informed decision, a consumer needs to be a part of producers' multicast trees. Creation and maintenance of a large number of multicast trees make the generic IP-based architectures non-scalable.

Sauter *et al.* [6] proposed a two-tier infrastructure which uses a combination of gateways and tunneling to achieve end-to-end communication. This gateway-based approach is proposed for the interconnection of heterogeneous networks. It requires a variety of protocol conversion modules, which unfortunately introduce latency and thus undermine the scalability of the

⋆ This work was supported in part by the US National Science Foundation Grants 1241809 and 1345232 and DoD ARO grant W911-NF-15-1-0393. The information reported here does not reflect the position or the policy of the federal government.

978-1-5090-4075-9/16/$31.00 ©2016 IEEE



(a) Schematic Diagram of the Architecture

(b) Constituents and the Interactions Diagram

Fig. 1: iCenS: The three level smart grid architecture.

proposed scheme. Kim *et al.* proposed a secure decentralized data-centric middleware for smart grid [3]. The architecture utilizes the publish-subscribe paradigm [10] along with a uniform-hashing scheme for data dissemination. This architecture has the same drawbacks of pure IP-based architectures, as it is designed as a data-centric overlay network on top of existing IP infrastructure.

SeDAX [11] exploits the same idea, by organizing information into topics; each topic is stored at a designated node as selected by a geographic hash function (GHF). The GHF chooses the closest node as the primary cache for the topic, and the second-closest node as a backup. Zhang *et al.* [7] proposed an information-centric approach for home communication. Exploiting the NDN architecture [9], the design was equipped with a publish-subscribe API for communication and management. Katz *et al.* suggested a data-centric energy infrastructure inspired by the Internet's design [12]. Despite the benefits of the data-centric design, the authors neither elaborate the architectural details nor address pitfalls of their architecture.

To our best knowledge, no proposal exists in the literature for a holistic architecture, which can meet all the communication requirements of the smart grid; and more importantly is compatible with the current protocols and standards (particularly, IEC 61850). In this paper, we propose an information-centric networking architecture, which fills this void.

III. iCenS: The Architecture

In this section, we propose our three-level smart grid networking architecture, iCenS. We start with the details of iCenS design as it is illustrated in Fig. 1, and then discuss the required modification of the IEC 61850 stack to achieve the full functionality of our design in Subsection III.B.

A. Three Level Conceptual Architecture

As illustrated in the schematic diagram in Fig. 1(a), iCenS is composed of three levels: the lowest level (physical level) consists of the physical devices. The consumers, producers, and prosumers devices reside at this level; so do the other devices that form part of the *greater-grid infrastructure*, that is, the distribution, transmission, and generation infrastructure. The aggregation level in the middle is composed of aggregator nodes. These nodes act as collectors of information from the physical level nodes and are capable to perform some initial monitoring and control operations and data aggregations. A node at a physical level is connected to more than one aggregation node to guarantee fault-tolerance. The highest level is the computation level, composed of computation nodes (cloud/data centers), which use gathered data to help perform precise demand-response, handle billing and statistical information for customers, and perform large scale grid monitoring and visualization.

In Fig. 1(b), we present a more detailed view of our proposed architecture, namely the constituents at each level and the interactions between them. The electrical flow, at the physical level, is indicated by the bold red lines in Fig. 1(b). The power network connects entities of the physical level while the communication network facilitates the communication among entities at all levels. The black solid arrows represent inter-level bidirectional information flow while the dashed arrows indicate bidirectional information flows within the same level.

All physical level entities except prosumers are equipped with monitoring elements such as synchrophasors, phasor measurement units (PMUs), remote terminal units (RTUs), and other sensors. We propose that generation control units collocated with bulk generators can be responsible for controlling demand-response, monitoring, and generation management. These units get information from the computation level, via the power control, operation, and monitoring unit in the aggregation level.

A prosumer may be equipped with one or more resident distributed generation (DG) elements (e.g., solar, wind, geothermal). It also has a home area network (HAN), a smart meter, and a home agent (which may be part of the smart meter). The home agent is connected to its DGs, the HAN, and the smart meter to coordinate local power generation, total home energy consumption, and buying/selling of energy, based on user-defined operating constraints. In cooperation with the smart meter, the home agent reports aggregated information to the data dissemination unit in the aggregation level.

The aggregation level can be logically visioned as two parts: one that facilitates aggregation for the prosumers and the other that facilitates aggregation for other information flow, broadly for wide-area monitoring (WAMS) and supervisory control and data acquisition (SCADA). The *data dissemination engine* classifies prosumers' data and forwards it to the corresponding units. The *energy transaction facilitator* aggregates the prosumers' power generation statistics (current and expected) and projected

consumption data. Critical/urgent messages, indicating events such as short-circuits and house power failures, are forwarded by the dissemination engine to the *critical event handler* for immediate remedial action. The dissemination engine forwards the consumption data to the *data collector module*.

Information from the greater-grid monitoring elements are aggregated by sensor aggregators, Phasor Data Concentrators (PDCs), and super PDCs, which reside in the aggregation level. These aggregators collect and transmit the information to the power control, operation, and monitoring (PCOM) system, which is envisioned as the integration of the SCADA and the WAMS systems, for grid monitoring, control, and management decisions. The power grid critical incidents are reported to a critical events handler by monitoring elements such as the sensors, PDCs, and super PDCs for timely remedial action.

The *data collector module* is the aggregation level's interface with the computation level. It collects information, such as prosumers meter reading, historical data of critical events, power infrastructure statistical data, and power marketing information from bulk generation and the distributed generators. The data collector module forwards the aggregated information to the *data classifier unit* in the computation level. Based on the nature of the data the classifier distributes the collected information to the data center and/or the *power market module* that deals with demand-response (demand-response submodule) and bulk markets (bulk power market submodule). Data can be stored in the cloud/data center for future analysis. The *billing center* interacts with the data center and the web server to provide customer-driven the billing information on consumption, which is accessible through the web server.

The *optimization center*, by receiving the demand information, periodically runs an optimization function to schedule the generators for bulk production and calculates the energy price with the collaboration of the *pricing* module. The power market module, composed of the bulk power market and the demand-response market submodules, interacts with the classifier for the required information to manage the power market. The market module forwards the demand-response market information, via the data classifier and the data collector module, to the energy transaction facilitator to handle the demand-response market. The bulk power market related decisions will be forwarded to the generation management unit of the bulk generators via the data classifier, data collector, and PCOM. The data center is directly connected to the market module to store marketing information.

Smart grid communication can be broadly differentiated into customer-centric (e.g., metering) and grid-centric (e.g., grid monitoring and control). However, the communications requirements comprise a broad spectrum. On one side, the urgent messages corresponding to critical short-term grid-state and stability information have deadline of 4-16 ms [13]. On the other side, there are long-term grid-state or billing messages, needed at the computation level for long-term decision making, with relaxed deadlines of 10 ms to a few minutes. Our architecture will enable this whole spectrum as we shall show in this subsection.

Research on ICN grid communication have shown the advantages of fiber-optic, Ethernet, and WiMAX for urgent communications [14], [15]. We foresee the latency guarantees for energy transactions to be in the order of few seconds, allowing the use of multiple wireless communication technologies [16].

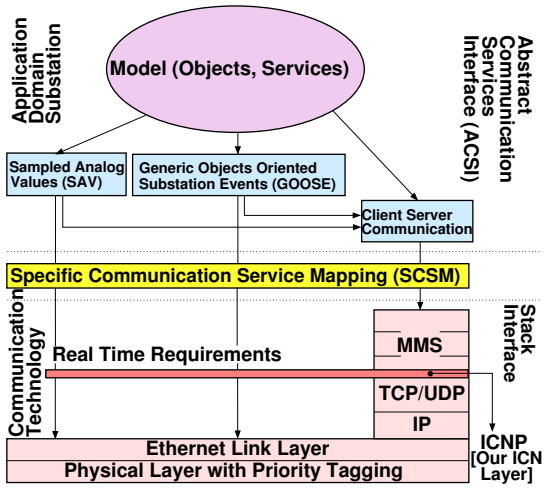


Fig. 2: The IEC 61850 Protocol Stack with the plugged-in ICN Layer

There are many other communication scenarios: for instance, prosumers can be part of an energy stock market and can negotiate prices iteratively. A producer can employ similar iterative negotiations with a set of consumers. A group of consumers/producers can form a cooperative that bids together. In all cases, each message will be useful for multiple entities, e.g., a producer's supply profile can be used by several customers, making in-network caching an attractive proposition—the motivation for leveraging the ICN paradigm.

Next we discuss our architecture's implementation details. We enhance the standard TCP/IP model in the context of the widely used IEC 61850 standard [8] to incorporate the ICN-paradigm.

B. Extended TCP/IP stack based on IEC 61850

The IEC 61850 standard is well entrenched in the grid for inter-device and device to substation communications. For backward compatibility we use the IEC 61850 communication stack as our foundation. Fig. 2 shows our resulting network stack, including the two additions to the current IEC 61850 stack—the thin Information-Centric Network Protocol (ICNP) layer and the UDP protocol alongside the existing TCP protocol. The ICNP layer, is above the transport layer to leverage the information-centric nature of communications and enable concurrent use of several communication technologies. In IEC 61850, urgent messages bypass the top layers of the network stack to go directly to the Ethernet. In our design, urgent messages will pass through the ICNP layer to help improve their delivery reliability. This reliability can be achieved by concurrent communication over multiple communication technologies.

Reliable and timely communications are essential functionalities to ensure the same global market view for all prosumers—a precursor to sustainable energy trading. The best way to maintain a synchronized global view is to aggregate and disseminate all supply and demand profiles. Prosumers will communicate energy trading information to their corresponding aggregation nodes as non-urgent messages. The energy transaction facilitator module (Ref. Fig. 1(b)) of the aggregation node collects these information and forwards it to the demand-response market unit. The computation nodes push the consolidated information (includes analysis and energy directives) to the aggregation nodes

(form an overlay network). Each prosumer's agent will obtain data from one or more of its nearby aggregation nodes.

A consumer agent's energy-inquiry message elicits an energy-response message from one of its aggregation node(s) that contains the supply information units given the fact that all the aggregation nodes receive the demand-response profile from the computation level. When the consumer has identified a set of possible producers for negotiation, it negotiates with the producer(s) through one of its aggregation node and the corresponding aggregation node(s) the producer(s) is associated with. In order to support this communication, our design melds concepts from Named Data Networking (NDN) [9] and the Publish-Subscribe Internet Routing Paradigm (PSIRP) [10]. The device agents will act as the *subscribers* of information, while the aggregation and computing nodes operate as *publishers*.

IV. Addressing Networking Challenges using iCenS

For a smart grid communication architecture to be effective, it must address the challenges of meeting the QoS, reliability, security, and privacy requirements of the grid. In this section, we discuss how iCenS addresses these challenges and how we plan to implement it moving forward.

A. Addressing QoS and Reliability Requirements

1) Concurrent Use of Multiple Communication Technologies for QoS and Reliability: Approaches such as differentiated services (DiffServ) and the concurrent use of multiple communication technologies are very useful to ensure QoS and reliability for smart grid communications. Internet-like differentiated services models have been proposed for smart grid data communication [17], [18], but they alone will not be able to meet the grid's stringent reliability and bandwidth requirements. We believe that the node-agnostic ICN paradigm best leverages a node's multiple interfaces to enable concurrent data transmission [16] for better bandwidth utilization and reliability.

In ICNs (especially NDN) the same data can be transmitted by a node over several interfaces with the help of the strategy layer. A node's forwarding information base (FIB) can stores quality indices for each interface, such as packet-loss rates, bit-error rates, signal-to-interference-and-noise ratios, and bandwidths. These indices may be constantly updated by virtue of a cross-layer protocol. Additionally, a node uses the number of successful receptions as a quality index for each interface. In our architecture, we propose the use of a weighted-mapping function that will take the Differentiated Service Code Points (DSCP) value of a message and the quality indices of available interfaces as input and will output the interfaces on which to transmit a message to meet the desired single-hop guarantees.

2) Leveraging Caching to Improve QoS and Reliability: Information-centric addressing facilitates in-network caching and reduces redundant transmission of popular data in the network. For caching to be effective, it is important to correctly identify the items to be cached and those to be evicted to make room for newly arriving item(s). All messages in the microgrid, other than the time-critical disturbance messages, are candidates for in-network caching. The challenge is to identify the nature of cacheable microgrid traffic and design a novel caching framework that reduces traffic load on the network core.

Preliminary analyses show a few unique characteristics of microgrid communications: a majority of the communications will have delay constraints; energy profiles can become unusable before their normal expiry time due to interim energy transactions (e.g., a producer selling a portion of its energy); and compared to Internet traffic popularity (request frequency), microgrid messages will be more dynamic due to frequent energy transactions and accompanying changes in energy profiles. A Zipf-like distribution may be sufficient to describe the popularity of physical nodes (i.e., a few popular producers/prosumers and many unpopular ones), however actual content objects are expected to have dynamic popularity over time.

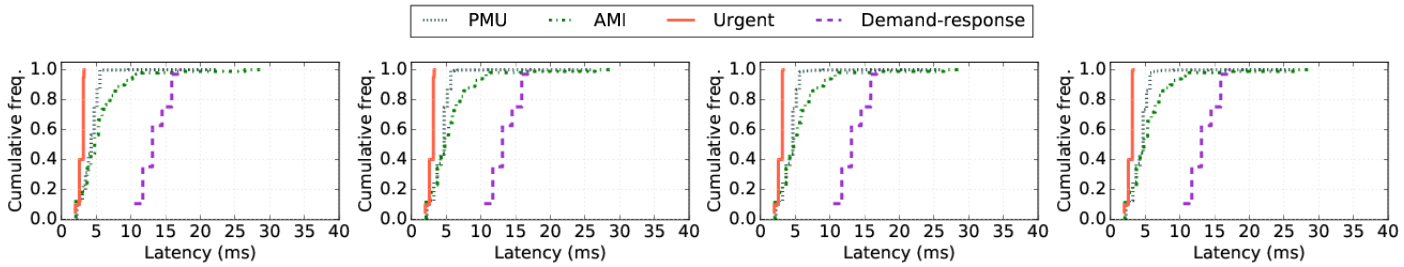
B. Security and Privacy

Important security requirements of a smart grid are: prevention of denial of service (and DDoS) attacks, secure communication and authentication of all messages, and user privacy, especially during energy trading. Our architecture can help address some of these problems.

1) Ensuring Data Availability for Communicating Entities: Mechanisms that handle DoS/DDoS attacks in a microgrid help to ensure data availability. Rate-limiting, which is inherently supported by NDN, is an effective approach to thwarting DoS/DDoS attacks. This strategy can be augmented by pattern analysis to enable early attack detection [13]. Traditional DOS attacks are ineffective in NDN, since a duplicate request is aggregated into a single entry in each router's Pending Interest Table (PIT) without being forwarded again. However in iCenS, aggregation nodes are vulnerable to localized DoS/DDoS attacks, e.g., a malicious agent constantly requesting energy supply profiles. We envision mitigating this threat with a token bucket scheme – an aggregation node can thereby restrict the number of requests which each of its constituent physical nodes can send within some unit of time. Jamming by outside attackers, especially with discrete low-intensity jammers, is another possible DoS mechanism. With the availability of multiple communication technologies at each node, it would be exceedingly difficult to jam all available channels. In addition, frequency-hopping and DSSS techniques can be easily integrated into such architecture.

2) Ensuring Secure and Private Communications: We assume that a Public Key Infrastructure (PKI) exists so agents may share symmetric keys with their aggregation node(s), and use keyed message authentication codes (MACs) [19] or asymmetric signatures to ensure the provenance of data. However, existing encryption techniques are too slow and could result in the violation of the tight deadlines imposed on urgent grid communications. An alternative approach would be using MACs to prevent false data injection [13], which does not address the confidentiality of these transmissions. Considering the importance of the transmitting data, both source authentication and message confidentiality are critical.

In our architecture, we consider different approaches to ensuring user privacy in demand/supply communication and negotiations. One way to enhance privacy is to use a secure naming scheme, wherein the data name prefix is replaced by a hash. To further strengthen user privacy, an aggregation node can create aggregated profiles, representing all the customers connected to it. This aggregated profile does not contain customers' identities, and will be signed by the aggregation node with its own private keys. The same procedure can be performed at the decision level if the aggregation nodes cannot be trusted.



(a) Scenario 1 (b) Scenario 2 (c) Scenario 3 (d) Scenario 4

Fig. 3: Empirical CDFs of delivery latency for each type of data in each scenario. No major increases in latency can be observed as the frequency of transmission increases. Latency for urgent messages approaches the theoretical lower bound.

The proposed PKI-based secure group communication scheme for smart grid is cumbersome for member addition/revocation [13] and compute-intensive for physical agents, which may be low-power devices (e.g., a 16-600 MHz ARM processor with 1-2 MB RAM). iCenS exploits the enhanced broadcast encryption scheme proposed in [20], [21] for a novel secure group-communication protocol which is accessible to low-power mobile devices; in this scheme, a majority of the computational burden is shifted from the clients to the server.

3) Strengthening User Privacy and Provenance: If an aggregation node is compromised, user information can be leaked, so enhancing identity privacy by using pseudonyms instead of identities is important. Proposed approaches, such as privacy preserving aggregation [22] and load profile obfuscation using rechargeable batteries at homes [23] are expensive. Instead, there are proposed hierarchical architectures, which use K-anonymity or conditional anonymity [24], [25]. If a customer is undifferentiable from 'K' other customers connected to a aggregation node (popularly termed K-anonymity), then its privacy and load information can be preserved. Furthermore, there are lightweight anonymous communication proposals [26] that can be leveraged. We propose to use granular agent ID, such as at the block/street level, or a hashed-ID prefix that changes frequently. These mechanisms are easily implementable in our architecture.

V. Simulation & Evaluation

We have implemented a subset of the proposed iCenS design by extending ndnSIM, an NDN module for the ns-3 network simulator. To reduce the high-volume data delivery costs (future scale of demand-response), we extended NDN with a sparse-tree multicast capability. We restricted multicast flows to the minimum spanning tree of the aggregation network to prevent them from interfering with the delivery of higher-priority traffic (urgent messages). Similarly, urgent traffic were given priority access to the shortest paths to the computation level.

Additionally, we added support for payloaded interests to enhance quality-of-service for high-priority flows destined to aggregation and compute nodes. In most cases, data intended for aggregation or compute nodes can be accepted by any node in the respective class. The prefix-based routing used by interests allows us to take advantage of this fact to ensure that these packets will be forwarded to the closest node of the required destination class. This also eliminates overhead which would be incurred by treating physical nodes as producers, such as route establishment and multicast tree maintenance costs.

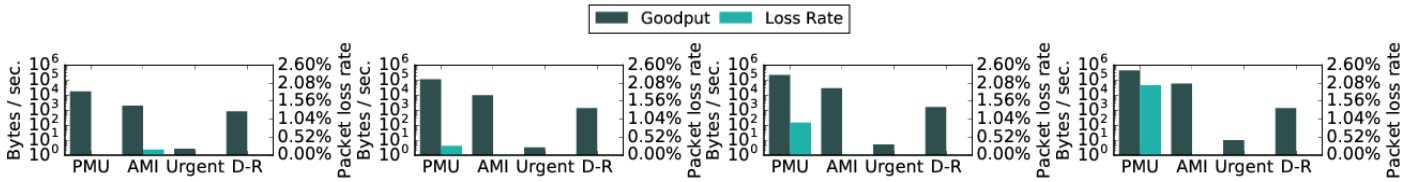
For our simulations, we created a 10-node full mesh computation (com) level and a 100-node scale-free aggregation (agg) level. The two were merged by preferential attachment, then 1000 physical (phy) nodes were attached to the edge of the aggregation network. Out of these, 980 were designated as home agents, and 20 as PMUs.

We modeled four types of traffic in each scenario: PMU, AMI, urgent, and demand-response. The PMU and AMI traffic originate from phy nodes (PMUs and home agents, respectively), are aggregated by agg nodes who forward the aggregates to the com nodes. Urgent traffic originates from PMUs and is delivered to com nodes, while demand-response traffic is disseminated from com nodes to home agents. While all other flows use payloaded interests, demand-response uses multicast delivery.

We configured PMU packets to be 90 bytes; this is sufficient to include voltage, current, phases, and timestamp values with high precision, possibly encoding these readings for multiple transmission or distribution lines in one packet. AMI packets were 60 bytes – these transmissions contain less detail than PMU transmissions, however we have still made them sufficiently large in order to model the possibility of auxiliary data (e.g., metadata or authentication materials). Urgent packets were also 60 bytes; these packets likely include some detailed measurements, but are smaller than typical PMU packets – urgent messages are generally alarms notifying of outage and are potentially accompanied with a measurement snapshot. Finally, demand-response packets were 1024 bytes long. Global demand-response profiles will likely be larger than this in a realistic deployment; however, we sought to avoid the necessity of implementing payload fragmentation in our model. Therefore, we chose this size, which was the largest possible without necessitating fragmentation in ndnSIM. Because other types of traffic use dedicated paths (and the intervals between transmissions of demand-response profiles is sufficiently long), we expect that transmitting larger packets would not be problematic.

We tested four scenarios, with different transmission rates: **(1)** PMU messages every 0.1 s (10 pkts/sec), AMI messages every 6 s, urgent messages every 360 s, demand-response every 600 s. **(2)** PMU every 0.017 s (60 pkt/sec), AMI every 2 s, urgent every 240 s, demand-response every 300 s. **(3)** PMU every 0.008 s (120 pkt/sec), AMI every 1 s, urgent every 120 s, demand-response every 60 s. **(4)** PMU every 0.004 s (240 pkt/sec), AMI every 1 s, urgent every 120 s, demand-response every 60 s. In each case, we simulated 3600s of activity.

Fig. 3 gives the distributions of latencies for each type of traffic flow. The latencies given for PMU and AMI packets are



(a) Scenario 1 (b) Scenario 2 (c) Scenario 3 (d) Scenario 4

Fig. 4: Goodput rates (left axis) and loss rates (right axis), for each type of traffic. Though the loss rate increases with transmission rate, it remains below 2% in all cases.

the total latencies from the origin phy nodes to the destination com nodes. Processing delay at the agg node is not included in our model, thus not reflected in the plot. As we have explicitly reserved paths for urgent messages, these are delivered the fastest (typically between 2.0 ms and 3.3 ms); however, PMU and AMI data also reaches the com layer in a timely manner. We observe excellent scalability with increasing transmission rates; there is no significant increase in latency despite an increase in the amount of traffic – the distribution shifts only slightly to the right. Note that the minimum delay observed in our scenario (1.99 ms) is very close to the theoretical minimum obtainable on this network – the shortest path from a phy node to a com node is two hops; each hop incurs a constant 0.5 ms propagation delay, and a minimum transmission delay of 0.48 ms (60 bytes for urgent packets, at 1 Mbps); thus we would expect a minimum delay of 1.96 ms. Our results indicate that urgent messages are not significantly affected by queuing delay, represented by the compressed steps in the CDF (red-solid line), which demonstrates scalability.

Fig. 4 shows the bandwidth utilization and loss rates for each flow type. We can see that as bandwidth consumption increases, loss rates increase but remain quite low and primarily affect PMU transmissions (which are the most frequent. Note that the loss rates never exceed 2%, even when PMUs are transmitting at 120 samples per second. Importantly, no loss is ever incurred for urgent messages.

VI. Conclusion

In this paper, we presented a novel information-centric networking architecture (iCenS), which is designed to handle the growing requirements of smart grid communications. We discussed the advantages of the iCenS architecture including scalability on transmitting large traffic volumes, backward compatibility with TCP/IP networking model and especially the IEC 61850 standard, and network interoperability in a heterogeneous multi-layered network. We discussed how iCenS can be leveraged to address QoS, reliability, and security and privacy concerns. We also presented results from a proof-of-concept simulation to demonstrate scalability.

References

[1] Energy.gov: Office of electricity delivery and energy reliability, 2013. http://energy.gov/oe/technology-development/smart-grid.

[2] World Energy Outlook, 2012. http://www.worldenergyoutlook.org/.

[3] Y. Kim, M. Thottan, V. Kolesnikov, and W. Lee. A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine*, 48(11):58–65, 2010.

[4] H. Liang, B. Choi, A. Abdrabou, W. Zhuang, and X. Shen. Decentralized economic dispatch in microgrids via heterogeneous wireless networks. *IEEE Journal on Selected Areas in Communications*, 30(6):1061–1074, 2012.

[5] H. Liang, B. Choi, W. Zhuang, and X. Shen. Stability enhancement of decentralized inverter control through wireless communications in microgrids. *IEEE Trans. on Smart Grid*, 4(1):321–331, 2013.

[6] T. Sauter and M. Lobashov. End-to-end communication architecture for smart grids. *IEEE Trans. on Industrial Electronics*, 58(4):1218–1228, 2011.

[7] J. Zhang, Q. Li, and E. Schooler. ihems: An information-centric approach to secure home energy management. In *IEEE International Conference on Smart Grid Communications*, pages 217–222, 2012.

[8] International Standards and Conformity Assessment for all electrical, electronic and related technologies. http://www.iec.ch/smartgrid/standards/.

[9] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, and R.L. Braynard. Networking named content. In *ACM CoNEXT 2009*, pages 1–12. ACM, 2009.

[10] S. Tarkoma, M. Ain, and K. Visala. The Publish/Subscribe Internet Routing Paradigm (PSIRP): Designing the Future Internet Architecture. *Towards the Future Internet*, page 102, 2009.

[11] Y. Kim, J. Lee, G. Atkinson, H. Kim, and M. Thottan. SeDAX: A scalable, resilient, and secure platform for smart grid communications. *IEEE Journal on Selected Areas in Communications*, 30(6):1119–1136, 2012.

[12] R. Katz, D. Culler, S. Sanders, S. Alspaugh, Y. Chen, S. Dawson-Haggerty, P. Dutta, M. He, X. Jiang, L. Keys, et al. An information-centric energy infrastructure: The berkeley view. *Sustainable Computing: Informatics and Systems*, 1(1):7–22, 2011.

[13] W. Wang and Z. Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 2013.

[14] R. Khan and J. Khan. Wide area pmu communication over a wimax network in the smart grid. In *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pages 187–192, 2012.

[15] Y. Xu and W. Wang. Wireless mesh network in smart grid: Modeling and analysis for time critical communications. *IEEE Trans. on Wireless Communications*, 12(7):3360–3371, 2013.

[16] R. Tourani, S. Misra, and T. Mick. IC-MCN: An Architecture for an Information-Centric Mobile Converged Network. *IEEE Communications Magazine*, 2016.

[17] J. Deshpande, E. Kim, and M. Thottan. Differentiated services qos in smart grid communication networks. *Bell Labs Technical Journal*, 16(3):61–81, 2011.

[18] W. Sun, X. Yuan, J. Wang, D. Han, and C. Zhang. Quality of service networking for smart grid distribution monitoring. In *IEEE International Conference on Smart Grid Communications*, pages 373–378, 2010.

[19] A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of applied cryptography*. CRC press, 2 edition, 2010.

[20] S. Misra, R. Tourani, and N. Majd. Secure Content Delivery in Information-Centric Networks: Design, Implementation, and Analyses. In *ACM SIGCOMM ICN Workshop*, pages 73–78. ACM, 2013.

[21] S. Misra, R. Tourani, F. Natividad, T. Mick, N. Majd, and H. Huang. AccConF: An access control framework for leveraging in-network cached data in ICNs. *arXiv preprint arXiv:1603.03501*, 2016.

[22] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Trans. on Parallel and Distributed Systems*, 23(9):1621–1631, 2012.

[23] D. Varodayan and A. Khisti. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1932–1935, 2011.

[24] D. Huang, S. Misra, M. Verma, and G. Xue. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. on Intelligent Transportation Systems*, 12(3):736–746, 2011.

[25] S. Misra and G. Xue. Efficient anonymity schemes for clustered wireless sensor networks. *Intl. Journal of Sensor Networks*, 1(1):50–63, 2006.

[26] R. Tourani, S. Misra, J. Kliewer, S. Ortegel, and T. Mick. Catch Me If You Can: A Practical Framework to Evade Censorship in Information-Centric Networks. In *Proceedings of the International Conference on Information-Centric Networking*, pages 167–176. ACM, 2015.