NDN Network Environment: Enterprise Building Automation and Monitoring Systems

Jeff Burke

Abstract

The abstract.

I. Introduction

As part of the NSF-supported NDN "Next Phase" research from 2014-2016, the NDN project team has selected two network environments, **Open mHealth** and **Enterprise Building Automation & Management**, and one application cluster, **Mobile Multimedia**, to drive our research, verify the architecture design, and ground evaluation of the next phase of our project. The two environments represent critical areas in the design space for next-generation Health IT and Cyberphysical Systems, respectively. They also extend work started in the previous NDN FIA project on participatory sensing and instrumented environments to focus on specific application ecosystems where we believe NDN can address fundamental challenges that are unmet by IP. Based on the successful initial results of previous NDN research, we have identified Mobile Multimedia as an application area of cross-cutting relevance, motivated not only by the network environments above but our team's desire to further develop NDN by using it for our everyday communication.

This technical report provides background information on the **Enterprise Building Automation and Management** network environment including key application challenges faced using IP and describes the design for a pilot application that the NDN team is building. It serves as the primary design document for this application.

A. EBAMS Background

For our purposes, Enterprise Building Automation and Management covers the intersection of three critical sub-areas: *industrial control systems* (ICS), including supervisory control and data acquisition (SCADA) and so-called smart grid [2], *enterprise networking*, and the *Internet of Things* (IOT) movement [1]. Enterprise BAS and BMS are environments that bring both critical infrastructure considerations of ICS with exciting visions for the everyday built environment of IoT. In this domain, significant engineering challenges have emerged along with the promise offered by the convergence of networking in ICS with traditional IT, a sea change described by NIST in their ICS security review [7].

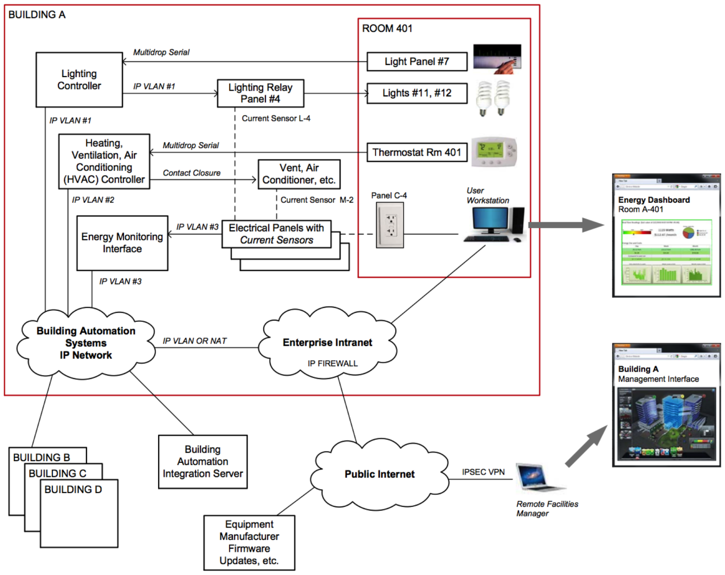

Fig. 1. *Example of building automation and management components, including sensors, controllers, and interfaces to both the public Internet and an enterprise intranet. Securely integrating these heterogeneous components, while simplifying application development, is an important challenge posed by this network environment.*

BAS and BMS are software/hardware systems that perform control, monitoring and management of heating, ventilation and air conditioning (HVAC), lighting, water, physical access and other building components. Their distributed, heterogeneous nature leads to a variety of challenges. The IP protocol suite is increasingly used to network their components and as such is now a fundamental substrate of new buildings. However, IP networks suffer from limitations that impact innovation and trust in networked building systems, which we believe can be addressed with NDN.

BAS/BMS pose complementary challenges to those of mHealth. They integrate hundreds to thousands of data collection and control points often implemented by special-purpose embedded devices and managed by a single enterprise. Some devices are mobile and others are fixed; some devices are power-constrained and wireless while others are hard-wired and continuously communicating. Figure 1 shows a few components of a typical system, including thermostats used for adjusting HVAC, lighting control and energy monitoring.

Security is a fundamental and critical challenge [3]. Like other ICS, BAS/BMS typically employ physical or logical isolation of the network as a primary security measure, which limits interoperability and integration.[1] They also use a mixture of proprietary and open protocols, only a few of which offer intrinsic security. In many networks, there is no intrinsic security at lower layers, and only channel- and perimeter-based security above that, via SSL/TLS, VPNs, and routing configuration. Given the importance of integrating subsystems for applications such as energy management, fault detection, and synchronization, network segregation and closed protocols are not a viable long-term approach. Figure 1 shows an environment that supports access to control and monitoring from intranet web sites, but makes "air gaps" impossible and logical network separation hard to engineer and maintain for normal enterprises.

For application developers, there is a fundamental mismatch in BAS/BMS between how network applications are authored (typically data-centric) vs. fieldbus and IP network abstractions (host- and device-centric). Addressing is spread across many layers, most of which are not routable. There is a great heterogeneity in protocols, especially at the fieldbus level. Typically, application developers and platform manufacturers implement abstraction layers in middleware [5], often complex, proprietary, and challenging to configure.

In addition to the protocols themselves, significant application logic is bound up in network configuration not accessible to developers or users: 1) VLANs, IP subnetting, and routing configurations enforce boundaries between systems; 2) firewall configurations describe brittle rules for system access, which can be difficult to change; 3) keys and certificates for SSL connections and VPNs may identify connections; 4) VPN configuration and enterprise authentication hold remote network access permissions. None of these are typically visible or accessible to application software in traditional systems. In fact, they represent important system control logic that is often replicated ad-hoc in application configurations. A simple example is how an application must be configured to know that 192.168.2.1/24 is lighting and 192.168.3.1/24 is HVAC, which is site-specific and meaningless to an application. Such configurations also bring brittleness to changing topologies and devices.

Our selection of digitally-controlled cyberphysical systems as a network environment is inspired by the practical goal of enabling more efficient operation of buildings, improved comfort and control for occupants, and new opportunities for understanding the interactions between elements of our built environment.

B. Relationship to NDN-IoT

The EBAMS research has much in common with the "Internet of Things" (IoT) vision and related NDN research. For now, we consider IoT applications separately (and not in this document), motivated from consumer experience and smart home deployments. That research focuses on a bottom-up approach to networking devices using NDN, including issues such as NDN support on resource-constrained devices, bootstrapping and name assignment. The EBAMS network environment focuses on enterprise-scale networking of industrial control and monitoring technologies.

C. Collaboration

UCLA Facilities Management has agreed to act as domain experts and help define the practical requirements of this network environment. UCLA's currently deployed building management system has approximately 150,000 points of monitoring across the campus, potentially growing to over 400,000 points in the next five years. It is the largest installation on the West Coast for Siemens building systems after Microsoft. UCLA's IT, DDC (direct digital control), and engineering staff will interact with the NDN team to enumerate their requirements, challenges, and limitations. As part of the previous EAGER award, UCLA FM has already helped us install a dedicated Siemens electrical demand monitoring system for a laboratory space for research. We expect they will also help us install a

[1] In many cases, systems are left exposed to the Internet inadvertently. Only a few searches on http://shodanhq.com/ make this abundantly clear.

dedicated server that will provide near real-time access to 20,000 points worth of data from campus' operational systems, probably about 10 buildings worth of data. We plan to use this server as a gateway to our own NDN testbed.

D. *Proposed Milestones 2014-2016*

- Review limitations in current IP-based architecture, for Facilities Management needs. (Y1)
- Design NDN namespace, repository, trust and communication model for use cases, such as energy management, new building commissioning, feedback control. (Y1; updated in Y2)
- Implement low-level NDN applications, such as energy management data gathering. (Y1)
- Preliminary embedded platform support. (Y2)
- Integrate live UCLA building data into the NDN testbed, mirroring data from 10-20 UCLA buildings. (Y2)
- Implement high-level NDN application for enterprise building monitoring, based on the above data, applying distributed 3D visualization work done in the first FIA project. (Y2)

II. Related Work

A. *Previous work by the NDN team*

This network environment continues work that began in the original NDN project on authenticated lighting control and was extended through an EAGER in 2012-2013 to explore sensing and building management. The current and ongoing research, its results, and our evolving testbed are described in Section **??**.

B. *Suggested reading*

Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST Special Publication (2013): 800-82 Revision 1.

Shang, W., Ding, Q., Marianantoni, A., Burke, J., Zhang, L. Securing Building Management System Using Named Data Networking. (to be released as a TR), 2013.

Burke, J. Gasti, P., Nanthan, N., Tsudik, G. Securing Instrumented Environments over Content-Centric Networking: the Case of Lighting Control. Proc. IEEE NOMEN, April 2013.

Dawson-Haggerty, Stephen, et al. "BOSS: building operating system services." Proceedings of the 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI). 2013.

III. Pilot Application

To do (??)

A. *Research Objectives*

Naming and application design. The NDN architecture can reflect application knowledge (and needs) directly. Application logic for accessing devices can be captured in naming patterns and cryptographic signatures directly supported by the network. To support BA system integration, we aim to lower the cognitive distance between network protocol details and application requirements, so that complex BAS applications are easier to write, debug, and maintain. For example, an NDN-based BAS would use hierarchical naming rather than addresses and port numbers, removing the need for middleware to translate. We will have to develop consistent, granular, application-specific naming of data sources and control points, to support changing topologies and device configurations. NDN-network-based BAS could also make routing or forwarding decisions based on application-level semantics, essentially impossible in IP networks.

Trust and security. The trust model for this environment will emerge from the administrative organization of the enterprise and functional relationships among components. We believe these relationships can be expressed in the data and control namespaces, allowing straightforward trust verification in the applications. Extending our prior work in authenticated control, we plan to develop a system security approach that secures the data directly through cryptographic signatures on data packets and optional encryption of content. As a result, anyone equipped with the right credential (in the trust framework) can securely access, configure, and/or control devices using the same data name from any location in the enterprise. NDN-capable devices can then communicate on the network with authenticated messages, rather than relying on connection-level or physical segregation, or authentication present for user interface only.

Embedded and real-time support. To examine how NDN will work at all layers of BAS and BMS, we must consider embedded and real-time systems, many of which have recently transitioned to IP-based communication. Embedded platform support through both gateways and lightweight stacks for low-capability devices, including ”hard” real-time communication when appropriate support exists at lower layers [4], [6].

B. Application Requirements

Naming and application design

- Reflect system and physical world knowledge in the naming
- Simplify application development (seeking evaluation approaches)

Trust and security

- Base on real administrative organization at UCLA
- Trust model? Hierarchical may work but may be in a different namespace from the data (see Wentaos work so far)

Storage in the network

- Support the basic reporting requirements of the campus operators

IV. Testbed

Connect UCLA Facilities Management BMS to NDN testbed with new version of Wentaos existing code. Provide NDN-JS based viewer.

V. Design

Develop repository design and basic trust approach for offline report generation and online real-time viewing of the data as typically used by Fac Mgmt.

A. Naming

B. Storage

Repository requirements

C. Trust

VI. Open Challenges

VII. Conclusion

Acknowledgment

References

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[2] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid—the new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, 14(4), 2011.

[3] Eric D Knapp. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress, 2011.

[4] Jork Loeser and Hermann Haertig. Low-latency hard real-time communication over switched ethernet. In *Proc. of Euromicro Conference on Real-Time Systems*, pages 13–22, 2004.

[5] T. Sauter. The three generations of field-level networks - evolution and compatibility issues. *IEEE Transactions on Industrial Electronics*, 57(11):3585–3595, 2010.

[6] Tor Skeie, Svein Johannessen, and Oyvind Holmeide. Timeliness of real-time IP communication in switched industrial Ethernet networks. *IEEE Transactions on Industrial Informatics*, 2(1):25–39, 2006.

[7] Keith Stouffer, Joe Falco, and Karen Scarone. Guide to industrial control systems (ICS) security. Technical Report 800-82, National Institute of Standards and Technology (NIST), June 2011.