The Electricity Journal 29 (2016) 28–35

Contents lists available at ScienceDirect

The Electricity Journal

journal homepage: www.elsevier.com/locate/electr

Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security

Dong Jin[a,*], Christopher Hannon[a], Zhiyi Li[b], Pablo Cortes[a], Srinivasan Ramaraju[a], Patrick Burgess[b], Nathan Buch[c], Mohammad Shahidehpour[b]

[a] *Department of Computer Science, Institute of Technology, Chicago, United States*
[b] *Robert W. Galvin Centre for Electricity Innovation, Institute of Technology, Chicago, United States*
[c] *Silver Spring Networks, Chicago, United States*

ARTICLE INFO

Article history:
Available online 6 December 2016

Keywords:
Networked streetlights
Smart city
Cyber-security
Cyber-physical system

ABSTRACT

A wireless networked LED street lighting system with centralized and remote control technology has emerged as an innovative smart city application with great potential to reduce energy cost and enhance public safety. A pilot system integrated within a campus microgrid demonstrates the benefits of two smart city applications for public safety enhancement, while revealing multiple cyber-security challenges.

1. Introduction

The world is experiencing an evolution of the so-called Internet of Things (IoT)—making everything and everyone connected. IoT enables the marriage between information technology and physical infrastructures (e.g., the electricity grid, transportation, health systems, buildings, etc.) and lays a foundation to realize the vision of Smart Cities. To conform that Smart City vision, Illinois Institute of Technology (IIT) has designated the campus as a “Living Laboratory” for the smart grid and other energy technologies by building the first ever fully-functional campus microgrid on IIT’s Main Campus in Chicago (IIT campus, 2016). Recently, IIT has installed a networked LED streetlight system on the microgrid, the first in the city of Chicago and one of the first in the world (Shahidehpour et al., 2015).

Compared to traditional street lighting systems, the networked LED street lighting system with remote control capability provides many benefits, such as reduced energy consumption and operational cost, and real-time control and monitoring capability. Furthermore, the established networked infrastructure offers a platform that connects the streetlights to various IoT devices and data sources. This new platform enables many innovative smart city applications. In this article, we present two such applications we developed with the goal of public safety enhancement. One is an emergency response aid application by integrating the streetlights with the on-campus 911 emergency buttons (The Energy Times, 2016). The other is a mobile application to generate the safest walking path on campus by integrating the streetlights with numerous pedestrian-counting video sensors (Placemeter, 2016a).

While those new applications offer great utility for the public, they also open up another avenue for malicious cyber-attacks, such as denial of service (DoS) or unauthorized control, posing potential threats to the system security. Researchers have studied the applications and challenges in standardizing IoT devices (Bandyopadhyay and Sen, 2011). The standardization of IoT devices and communication protocols are important to establish a cyber-secure smart city. For instance, because of a lack of security standardization and regulation in IoT devices and their self-assimilating nature, many household IoT devices are targets of cyber-attack. Recently, large companies, such as Dyn (a DSN service provider), have been targeted in large-scale distributed denial of service (DDoS) attacks incorporating IoT devices (Peterson, 2016). While there has been some research into preventing DDoS attacks from IoT devices (Misra et al., 2011), these recent attacks affirm that cyber-security is still an open problem in IoT design. In considering the networked devices in a smart city such as streetlights, traffic lights, sensors, and more, security is a foremost concern. In this article, we conduct a cyber-security assessment of the networked streetlight system, and report the found security vulnerabilities in the remote control server and the wireless communication protocol. We also discuss the importance of understanding public reactions to the deployment of this

[*] Corresponding author.
E-mail address: dong.jin@iit.edu (D. Jin).

http://dx.doi.org/10.1016/j.tej.2016.11.011
1040-6190/© 2016 Elsevier Inc. All rights reserved.

networked streetlight system, and effective means to increase the sense of safety and trust to use such networked cyber-physical systems in the community.

The remainder of the article is organized as follows. Section 2 provides an overview of the networked streetlight systems including a pilot system deployed on the IIT campus. Section 3 elaborates the integration of the streetlight system with the IIT Microgrid. Section 4 describes the two smart city applications to enhance public safety based on the unique features of the new streetlight system. Section 5 presents the cyber-security evaluation of the system and discusses risks and countermeasures. Section 6 summarizes the article.

2. Networked streetlight system overview

2.1. A pilot networked streetlight system

Fig. 1 depicts the IIT street lighting control system. The architecture of the smart streetlights is a mesh network of streetlights that communicate at a 900 MHz frequency. The streetlights are controlled by an access point in the CSMART lab on the IIT Tower's 16th floor. The mesh network is made up of 18 streetlights. two of which are in the lab and 16 on campus by the student housing buildings. The lights utilize this mesh network to periodically send usage statistics such as current consumption, brightness, wattage, and scheduling information to the PI System Historian that tracks the data over time. The PI System Historian collects data by making an API call from the PI System Interface Node server to the Silver Spring Networks cloud-based control server. This API call is an encrypted proprietary signal and sent over the cellular network to the access point in the lab. The access point then sends the signal to the streetlights mesh network at 900 MHz. This same process can be used to control the lights in real time. Lights can be controlled as a dimming percentage with increments of 10%. Additionally, the lights allow for fine-grained control targeting individual lights or groups of lights.

2.2. Benefits

As our cities become smarter, our public infrastructure gains features to promote safety, increase intelligence, and reduce costs. Smart streetlights, composed of LED lights with networking components and sensors, are one key cyber-physical system for smart cities. Smart streetlights aim to integrate intelligence into the lights that can facilitate management and open new venues of smart applications. With traditional streetlights, utilities have little role in managing their operation beyond setting a static on-off schedule and replacing broken lights when they fail.

Smart streetlights, however, comprise a networked system with sensors that can relay usage statistics and operational state. This built-in intelligence enables management to receive notification that a light needs repair. Additionally, as the seasons change, it is easier to control the schedule of the light system. Street light management can control the brightness of the streetlights in real time based on environmental dynamics or for special events. This real-time control provides a platform for smart city applications that can be paired with many public data sources such as traffic, weather, and other IoT devices. Traditional streetlights use incandescent or fluorescent lights, which according to the U.S. Office of Efficiency & Renewable Energy are between 25 and 80% less efficient than LED lights, while LED lights last between 3 and 25 times longer, providing a financial incentive for smart LED streetlights (Energy.gov, 2016). Finally, since streetlights are ubiquitous throughout cities, the mesh network they form can provide a low-cost communication network infrastructure for future smart city sensors and IoT devices.

3. Integration of the streetlights with the IIT microgrid

Located 2.5 miles south of downtown Chicago, the Illinois Institute of Technology has successfully transformed its main campus into a microgrid (IIT campus, 2016). The layout of the IIT microgrid is depicted in Fig. 2. The total generation capacity is approximately 13 MW, consisting of two natural gas turbines with a total capacity of 8 MW, renewable energy-based generation with a total capacity of 1 MW, as well as small backup generation with a total capacity of 4 MW. It also possesses 1 MW capacity of energy storage and a hybrid AC/DC nanogrid that is able to island itself from the rest of the IIT microgrid and continue to operate. The IIT microgrid is composed of seven separate loops, each with smart switches for enhancing the reliability of power delivery. A master controller is implemented to optimize the microgrid-wide energy management at three levels, namely, the microgrid level, the micro-source/building level, and the load component/sub-building level. Note that the IIT microgrid is fully functioning, with self-healing capabilities. In particular, it has the capability of operating properly in island mode when it is isolated from the local utility. In fact, the IIT microgrid has introduced several benefits to the

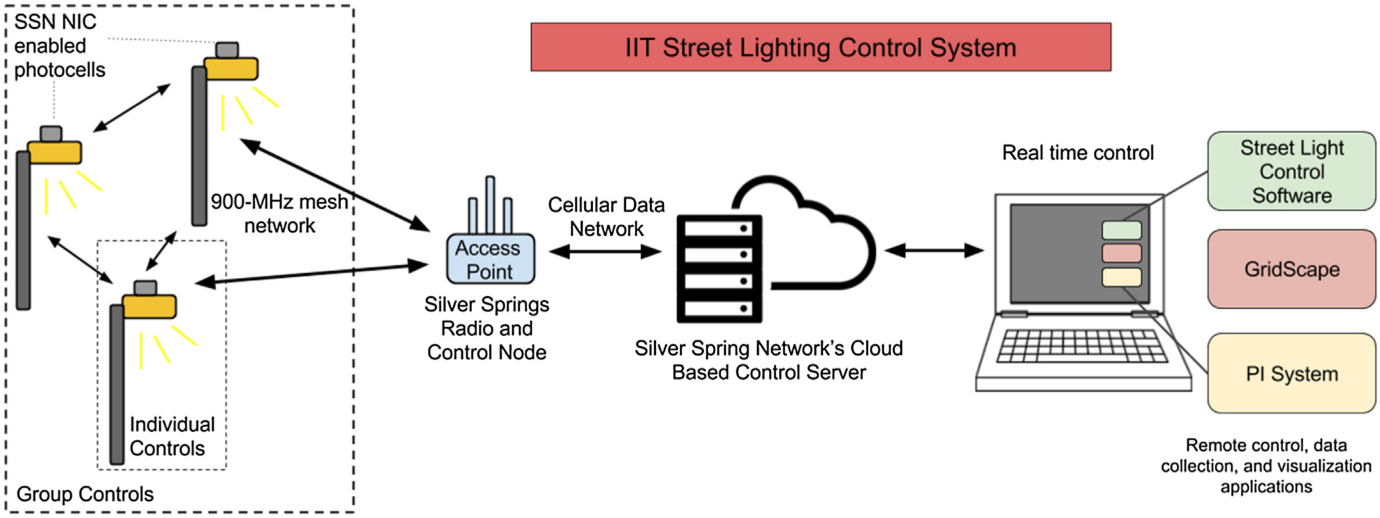
SSN NIC enabled photocells
900-MHz mesh network
Individual Controls
Group Controls
IIT Street Lighting Control System
Access Point
Silver Springs Radio and Control Node
Cellular Data Network
Silver Spring Network's Cloud Based Control Server
Real time control
Street Light Control Software
GridScape
PI System
Remote control, data collection, and visualization applications

Fig. 1. IIT's pilot networked street light system.