Software Defined Intelligent Building

Rui Yang Xu, Xi’an Jiaotong-Liverpool University, Suzhou, China
Xin Huang, Xi’an Jiaotong-Liverpool University, Suzhou, China
Jie Zhang, Xi’an Jiaotong-Liverpool University, Suzhou, China
Yulin Lu, Xi’an Jiaotong-Liverpool University, Suzhou, China
Ge Wu, University of Wollongong, Australia
Zheng Yan, Aalto University, Espoo, Finland & Xidian University, China

ABSTRACT

The networks of intelligent building are usually consist of a great number of smart devices. Since many smart devices only support on-site configuration and upgrade, and communication between devices could be observed and even altered by attackers, efficiency and security are two key concerns in maintaining and managing the devices used in intelligent building networks. In this paper, the authors apply the technology of software defined networking to satisfy the requirement for efficiency in intelligent building networks. More specific, a protocol stack in smart devices that support OpenFlow is designed. In addition, the authors designed the lightweight security mechanism with two foundation protocols and a full protocol that uses the foundation protocols as example. Performance and session key establishment for the security mechanism are also discussed.

Keywords: Intelligent Building, OpenFlow, Security, Smart Devices, Software Defined Networks

1. INTRODUCTION

An intelligent building (Bo et al., 2014; Huang et al., 2015; Zhang et al., 2014; Li et al., 2013; Son et al. 2011; Bruno et al., 2014) can monitor and control security, lighting, fire safety and many other systems in a building. It can significantly improve occupant comfort, simplify operation of building systems, and reduce energy consumption and operating costs.

The foundation of intelligent building is the large number of smart devices. These devices are usually connected, and form a very large network. The network is named as intelligent building network (IBNet) in this paper.

DOI: 10.4018/IJISP.2015070105
However, one challenge here is the IBNet management. So far, many smart devices only support on-site configuration and upgrade. Consequently, it is time-consuming to update configurations (e.g., routing policies and security rules) one device by one device.

In this paper, the researchers propose software defined networking (SDN)-based IBNet to eliminate the problem mentioned above. Recent years, SDN (Bruno et al. 2014; Kretutz et al., 2013; Lantz et al. 2010; Druskoy et al., 2013; Handigol et al., 2012) is proposed as the next generation network technology, and it can be easily managed. Thus, the researchers expect that with this new technology, the IBNet can also be easily managed. However, the research questions are:

1. Is SDN architecture proposed for general networks suitable for IBNet?
2. Can protocol stacks in smart devices be extended to support SDN protocols?
3. How can the researchers balance requirements of security (Huang et al. 2015) and performance in the newly designed network?

In order to study these questions, the authors build a prototype: SBuilding. The prototype is inspired from SDN: network devices become programmable in SBuilding. SBuilding is compared to other networking technologies, the advantages are summarized.

The main problem in SBuilding is OpenFlow (McKeown et al. 2008; Vu et al., 2012). OpenFlow is the most widely used protocol suite between a SDN controller and network devices. However, the standard version of OpenFlow does not support smart devices.

In order to solve this problem, the authors have designed a protocol stack in smart devices to support OpenFlow. Also, the authors have integrated lightweight security mechanisms in the extended OpenFlow to secure the communications. Both theoretical analysis and practical evaluation are used to confirm that the performance of these mechanisms are acceptable.

In summary, main contributions of this paper are as follows:

1. A SDN-based IBNet (SNet) for intelligent building is proposed. Its advantages and disadvantages comparing to several current network architectures are analyzed;
2. OpenFlow is extended to support smart devices in intelligent buildings. Its security mechanisms are also designed;
3. The researchers use the model checking approach, which is a formal verification technology, to verify proposed security mechanisms;
4. Performance of extended OpenFlow is studied; the advantages and disadvantages are summarized.

This paper is organized as follows. In Section II, SNet is introduced. In Section III, lightweight security mechanisms are explained. Section IV and Section V discuss the security and performance of proposed protocols respectively. Section VI shows a use case of our system. Section VII gives a key management scheme for distributed the keys. Finally, a conclusion is made in Section VIII.

### 2. SYSTEM OVERVIEW

Here, SDN technologies are used in IBNets. The newly designed network, which is named as SDN-based IBNet (SNet), aims at providing an easily manageable network for intelligent buildings.
Information Security Effectiveness: Conceptualization and Validation of a Theory

A Survey of Risk-Aware Business Process Modelling