Information Sciences 429 (2018) 390–405

Contents lists available at ScienceDirect

Information Sciences

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

A matrix-based cross-layer key establishment protocol for smart homes

Yuexin Zhang[a], Yang Xiang[a,c], Xinyi Huang[b,c,*], Xiaofeng Chen[c], Abdulhameed Alelaiwi[d]

[a] School of Software and Electrical Engineering, Swinburne University of Technology, Hawthorn, VIC 3122, Australia
[b] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China
[c] State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China
[d] King Saud University, Riyadh, 11543, Saudi Arabia

ARTICLE INFO

Article history:
Received 11 March 2017
Revised 25 September 2017
Accepted 17 November 2017
Available online 21 November 2017

Keywords:
Key establishment
Security
Matrix
Cross-layer
Smart homes
Internet of things

ABSTRACT

Wireless communications in smart homes are vulnerable to many adversarial attacks such as eavesdropping. To secure the communications, secret session keys need to be established between home appliances. In existing symmetric key establishment protocols, it is assumed that devices are pre-loaded with secrets. In practice, however, home appliances are manufactured by different companies. As a result, it is not a practical assumption that the appliances are pre-loaded with certain secrets when they leave companies. Motivated by these observations, this paper presents a matrix-based cross-layer key establishment protocol without the secret sharing assumption. Specifically, in our protocol, home appliances extract master keys (shared with the home gateway) at the physical layer using the wireless fading channels. Then, the home gateway distributes key seeds for home appliances by making use of the extracted master keys. Completing these operations, any two appliances can directly establish a secret session key at higher layers. Additionally, we prove the security of the proposed protocol and analyse the performance of it by comparing the new protocol with other closely related protocols. The comparison shows that appliances in our protocol can establish secret session keys when they do not pre-share any secrets, and it is achieved without introducing significant energy consumptions.

1. Introduction

Nowadays, an increasing number of consumer devices are equipped with wireless interfaces. Specifically, it is estimated that 50 to 100 billion devices will be wirelessly connected to the Internet of Things/Internet of Everything (IoT/IoE) by 2020 [22]. According to the IOT ANALYTICS,[1] smart homes stand out as the most prominent IoT application. Typically, smart homes integrate smartness into houses for the purpose of achieving comfort, healthcare, safety, security, and energy conservation [1]. Additionally, a variety of use cases can be enabled by smart homes, including light control system, appliance

[*] Corresponding author.
E-mail addresses: zhangyuexin87@hotmail.com (Y. Zhang), yxiang@swin.edu.au (Y. Xiang), xyhuang@fjnu.edu.cn (X. Huang), xfchen@xidian.edu.cn (X. Chen), aalelaiwi@ksu.edu.sa (A. Alelaiwi).
[1] Please refer to https://iot-analytics.com/10-internet-of-things-applications/.

https://doi.org/10.1016/j.ins.2017.11.039
0020-0255/© 2017 Elsevier Inc. All rights reserved.

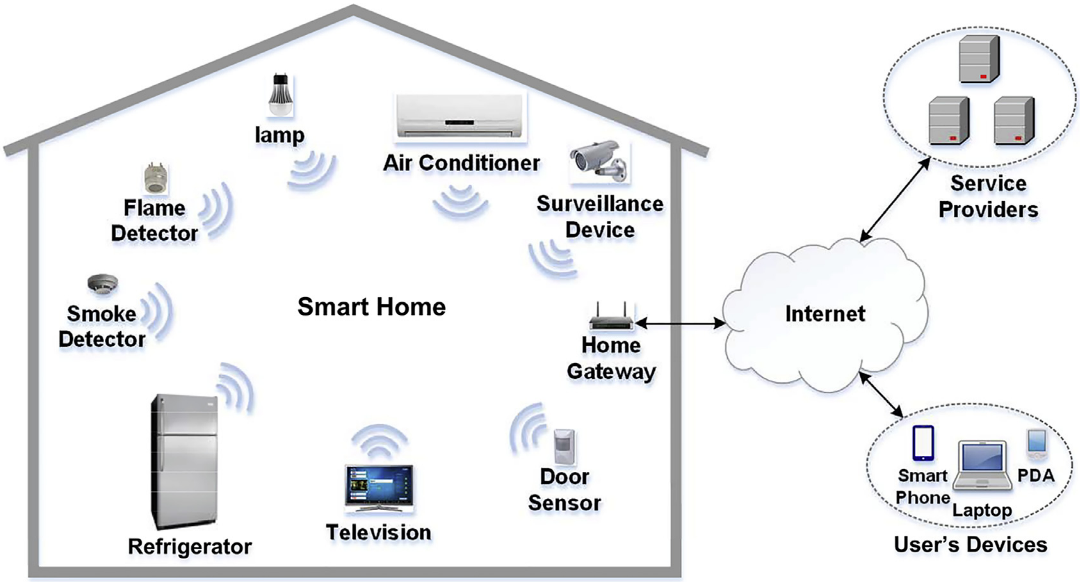

Fig. 1. The architecture of smart homes.

control system, smart energy system, and security and safety system. Thus, the smart home is a promising business/research field, and it attracts more and more attentions.

In practical applications, a smart home is implemented in a centralized architecture [31] (Fig. 1 shows the architecture of the smart home). From Fig. 1 we can see that, the smart home consists of two types of entities, i.e., the home gateway and the home appliances (or the home products). Specifically, the home gateway in the smart home serves as a bridge between home appliances and the residents, and it provides interoperability and control for the home appliances. The home appliances are heterogeneous devices, including low cost sensors, smart lights, smart thermostats and cameras, and other appliances integrated with intelligence. These appliances are able to wirelessly communicate with each other using certain Home Area Network (HAN) protocol, such as X10, ZigBee, and Z-Wave [15,25]. In practical applications, the home appliances sense the surrounding environment, and infer the current conditions based on the sensed data. Using context awareness and predefined constraints, smart homes can optimize residents' comfort based on the conditions of the home environment. Furthermore, residents can remotely control home appliances using smart phones, laptops, or through designated web apps by sending commands to the home gateway [15].

Different kinds of smart home appliances, manufactured by different companies, already flood the market. Such as Amazon Echo (the smart digital assistant), Nest Cam (the smart home security camera), and Nest Learning Thermostat (the smart thermostat). These appliances often become the targets of malicious attackers [16]. Additionally, the sensed data and commands are wirelessly transmitted, which contributes to the vulnerabilities of home networks. For instance, an adversary can control the home appliances by maliciously heating or cooling at the extreme temperatures. This increases utility costs and leads to additional strain on the heating, ventilating and air conditioning systems. Some attacks may produce physical harm to the home system or residents' safety. For example, an adversary may maliciously request all home appliances to get switched on or switched off. Such attacks may threat the lives of the residents if the life support equipment is hacked [2,4,17].

To secure the communications in smart homes, cryptographic keys need to be established. Until now, many key establishment protocols have been proposed. Specifically, conventional key establishment protocols are designed at higher layers, and they can be classified into two main types, i.e., asymmetric key establishment protocols and symmetric key establishment protocols [6]. In the asymmetric key establishment protocols, costly computation operations (such as the modular exponentiation operations) need to be executed. Recall that some of the home appliances are energy-constraint devices. Thus, it is preferred to design key establishment protocols in symmetric key setting. In symmetric key establishment protocols, it is assumed that devices are pre-loaded with certain secrets. Using the pre-loaded secrets, two devices can establish a secret session key with certain probability. However, existing symmetric key establishment protocols cannot be directly implemented in smart homes scenarios. It is due to the reason that in practice, home appliances are produced by different factories. As a result, it is not a practical assumption that these appliances are pre-loaded with certain secrets when they leave factories. Motivated by these observations, this paper aims to design a new symmetric key establishment protocol without the secret sharing assumption.

Recently, it becomes an increasing interest to extract secret keys at the physical layer by taking advantage of the characteristics of wireless channels. Specifically, in the typical multipath environments, the wireless channels between two devices,