EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

A Practical Group Authentication Scheme for Smart Devices in IoT

Anxi Wang[1], Jian Shen[1,*], Leiming Yan[1], Yongjun Ren[1], and Qi Liu[1]

[1] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China 210044; anxi_wang@126.com, s_shenjian@126.com

Abstract

Internet of things (IoT) is used to provide real-time data collection and analysis of the target area by the cooperation of low-cost devices. The authentication towards multiple devices has become the research hot-spot considering of the requirement in real applications. Sensitivity and privacy of data have caused widespread concerns because low-cost devices are neither tamper-proof nor capable of performing public key cryptography efficiently. However, many researchers only focus on the authentication between two devices in the network. They ignore the authentication among group devices attached to one network. In this paper, we propose A Practical Group Authentication Scheme for Smart Devices in IoT. Note that one device group to be authenticated consists of a group of smart devices. The personal digital assistant (PDA) as the group leader controls authentication operations in its group. From the security analysis, our scheme can resist to various attacks. In addition, the performance analysis shows that our scheme has lower computational cost than the existing scheme.

Keywords: Internet of things, group devices authentication, lightweight, practical.

Received on DD MM YYYY, accepted on DD MM YYYY, published on DD MM YYYY

doi: 10.4108/_____

1. Introduction

Internet of things (IoT) is the reasonable association of physical devices, vehicles, buildings, and other things which are equipped with electronics, software, sensors, actuators and so on. IoT enables these intelligent objects to collect and exchange data [3] [2] [11] for different usages. Nowadays, IoT can be widely used in all walks of life. It can collect the distributed information and connects everything in the world, so applications of IoT mainly includes the following areas: health-care, transport, logistics, smart home, and so on. Note that IoT has very broad application prospects and markets in these areas.

In IoT, each user can use electronic tags to connect real devices to the network. In the network, users can find one thing's specific location, running state and other parameters of interest. The cloud servers are usually used in IoT as service providers [14] to provide storage and computation services. Internet users on the network can use IoT for personnel management, centralized control, remote control and other similar control systems. At the same time, other major breakthroughs to smart cities can be achieved based on analysing the collected data [13]. With the development of Internet technology, IoT can be widely used in smart home, so as to provide people with a higher quality of life. However, security issues cannot be ignored, such as the theft of sensitive data leading to personal privacy leaks, illegal invasion of smart home, etc. In addition, devices used in IoT are usually lightweight and have restrictions on resources such as storage, computation and so on. So, applying non-lightweight public-key cryptography (PKC) to these devices is challenging. What's more, owing to the limit on the storage, the size of key should not be large. Compared with traditional systems, IoT is an easy target for attackers because communications are done in wireless

* Corresponding author