Wireless Networks

Min Chen
Shigang Chen

RFID Technologies for Internet of Things

Springer

Wireless Networks

Series editor

Xuemin (Sherman) Shen
University of Waterloo, Waterloo, Ontario, Canada

More information about this series at http://www.springer.com/series/14180

Min Chen • Shigang Chen

RFID Technologies for Internet of Things

Springer

Min Chen
Department of Computer and Information
University of Florida
Gainesville, FL, USA

Shigang Chen
Department of Computer and
Information Science
University of Florida
Gainesville, FL, USA

This work is supported in part by the National Science Foundation under grants CNS-1409797 and STC-1562485.

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-319-47354-3 ISBN 978-3-319-47355-0 (eBook)
DOI 10.1007/978-3-319-47355-0

Library of Congress Control Number: 2016954315

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Chapter 1
Introduction

1.1 Internet of Things

Internet of Things (IoT) [26] is a new networking paradigm for cyber-physical systems that allow physical objects to collect and exchange data. In the IoT, physical objects and cyber-agents can be sensed and controlled remotely across existing network infrastructure, which enables the integration between the physical world and computer-based systems and therefore extends the Internet into the real world. IoT can find numerous applications in smart housing, environmental monitoring, medical and health care systems, agriculture, transportation, etc. Because of its significant application potential, IoT has attracted a lot of attention from both academic research and industrial development.

1.2 RFID Technologies

Generally, every physical object in the IoT needs to be augmented with some auto-ID technologies such that the object can be uniquely identified. Radio Frequency Identification (RFID) [12] is one of the most widely used auto-ID technologies. RFID technologies integrate simple communication, storage, and computation components in attachable tags that can communicate with readers wirelessly over a distance. Therefore, RFID technologies provide a simple and cheap way of connecting physical objects to the IoT—as long as an object carries a tag, it can be identified and tracked by readers.

RFID technologies have been pervasively used in numerous applications, such as inventory management, supply chain, product tracking, transportation, logistics, and toll collection [1, 3, 8, 10, 16–19, 21–24, 27, 29, 32, 35, 37–39]. According to a market research conducted by IDTechEx [30], the market size of RFID has reached $8.89 billion in 2014, and is projected to rise to $27.31 billion after a decade.

M. Chen, S. Chen, *RFID Technologies for Internet of Things*,
Wireless Networks, DOI 10.1007/978-3-319-47355-0_1

Typically, an RFID system consists of a large number of RFID tags, one or multiple RFID readers, and a backend server. Today's commercial tags can be classified into three categories: (1) passive tags, which are powered by the radio wave from an RFID reader and communicate with the reader through backscattering; (2) active tags, which are powered by their own energy sources; and (3) semi-active tags, which use internal energy sources to power their circuits while communicating with the reader through backscattering. As specified in EPC Class-1 Gen-2 (C1G2) protocol [12], each tag has a unique ID identifying the object it is attached to. The object can be a vehicle, a product in a warehouse, an e-passport that carries personal information, a medical device that records a patient's health data, or any other physical object in IoT. The integrated transceiver of each tag enables it to transmit and receive radio signals. Therefore, a reader can communicate with a tag over a distance as long as the tag is located in its interrogation area. However, communications amongst RFID tags are generally not feasible due to their low transmission power. The emerging networked tags [13, 14] bring a fundamental enhancement to RFID tags by enabling tags to communicate with each other. The networked tags are integrated with energy-harvesting components that can harvest energy from surrounding environment.

The widespread use of RFID tags in IoT brings about new issues on efficiency, security, and privacy that are quite different from those in traditional networking systems [7, 36]. This book presents several state-of-the-art RFID protocols that aim at improving the efficiency, security, and privacy of the IoT.

1.3 Tag Search Problem

Given a set of IDs for the wanted tags, the tag search problem is to identify which wanted tags are existing in an RFID system [9, 11]. Note that there may exist other tags that do not belong to the set. As an example, a manufacturer finds that some of its products, which have been distributed to different warehouses, may be defective, and wants to recall them for further inspection. Since each product in the IoT carries a tag, and the manufacturer knows all tag IDs of those defective products, it can perform tag search in each warehouse to identify the products that need to be recalled.

To meet the stringent delay requirements of real-world applications, time efficiency is a critical performance metric for the RFID tag search problem. For example, it is highly desirable to make the search quick in a busy warehouse as lengthy searching process may interfere with other activities that move things in and out of the warehouse. The only prior work studying this problem is called CATS [40], which, however, does not work well under some common conditions (e.g., if the size of the wanted set is much larger than the number of tags in the coverage area of the reader).

We present a fast tag search method based on a new technique called filtering vectors. A filtering vector is a compact one-dimension bit array constructed from tag IDs, which can be used for filtering unwanted tags. Using the filtering vectors,

we design, analyze, and evaluate a novel iterative tag search protocol, which progressively improves the accuracy of search result and reduces the time of each iteration to a minimum by using the information learned from previous iterations. Given an accuracy requirement, the iterative protocol will terminate after the search result meets the accuracy requirement. We show that our protocol performs much better than the CATS protocol and other alternatives used for comparison. In addition, our protocol can be extended to work under noisy channel with a modest increase in execution time.

1.4 Anonymous RFID Authentication

The proliferation of RFID tags in their traditional ways makes their carriers trackable. Should future tags penetrate into everyday products in the IoT and be carried around (oftentimes unknowingly), people's privacy would become a serious concern. A typical tag will automatically transmit its ID in response to the query from a nearby reader. If we carry tags in our pockets or by our cars, these tags will give off their IDs to any readers that query them, allowing others to track us. As an example, for a person whose car carries a tag (automatic toll payment [35] or tagged plate [34]), he may be unknowingly tracked over years by toll booths or others who install readers at locations of interest to learn when and where he has been. To protect the privacy of tag carriers, we need to invent ways of keeping the usefulness of tags while doing so anonymously.

Many RFID applications such as toll payment require authentication. A reader will accept a tag's information only after authenticating the tag and vice versa. Anonymous authentication should prohibit the transmission of any identifying information, such as tag ID, key identifier, or any fixed number that may be used for identification purpose. As a result, there comes the challenge that how can a legitimate reader efficiently identify the right key for authentication without any identifying information of the tag?

The importance and challenge of anonymous authentication attract much attention from the RFID research community. Many anonymous authentication protocols have been designed. However, we will show that all prior work has some potential problems, either incurring high computation or communication overhead, or having security or functional concern. Moreover, most prior work, if not all, employs cryptographic hash functions, which requires considerable hardware [2], to randomize authentication data in order to make the tags untrackable. The high hardware requirement makes them not suited for low-cost tags with limited hardware resource. Hence, designing anonymous authentication protocols for low-cost tags remains an open and challenging problem [4].

In our design, we make a fundamental shift from the traditional paradigm for anonymous RFID authentication [5]. First, we release the resource-constrained RFID tags from implementing any complicated functions (e.g., cryptographic hashes). Since the readers are not needed in a large quantity as tags do, they