Accepted Manuscript

Universal and secure object ownership transfer protocol for the Internet of Things

Biplob R. Ray, Jemal Abawajy, Morshed Chowdhury, Abdulhameed A Alelaiwi

PII: S0167-739X(17)30218-2
DOI: http://dx.doi.org/10.1016/j.future.2017.02.020
Reference: FUTURE 3338

To appear in: *Future Generation Computer Systems*

Received date: 9 May 2016
Revised date: 21 December 2016
Accepted date: 8 February 2017

Please cite this article as: B.R. Ray, J. Abawajy, M. Chowdhury, A.A. Alelaiwi, Universal and secure object ownership transfer protocol for the Internet of Things, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.02.020

Universal and Secure Object Ownership Transfer Protocol for the Internet of Things

Biplob R. Ray[1], Jemal Abawajy[2*], Morshed Chowdhury[2] and Abdulhameed A Alelaiwi[3]
[1]*Centre for Intelligent Systems, School of Engineering and Technology, CQUniversity, Australia.*
[2]*School of Information technology, Deakin University, Australia.*
[3]*Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh, KSA*
b.ray@cqu.edu.au, {*jemal, muc}@deakin.edu.au}, aalelaiwi@ksu.edu.sa
** Corresponding author*

Abstract— In this paper, we address the problem of ownership transfer of RFID tagged objects in Internet of Things (IoT) in a secure manner. In application domains such as supply chain management, RFID tagged objects are required to securely change hands several times during their life cycle. To this end, we propose a novel ownership transfer mechanism that securely transfers an RFID tagged objects in Internet of Things (IoT). An important property of the proposed approach is that the proposed ownership transfer mechanism ensures the security of both the RFID tagged objects and the object owners. We analysed the proposed object ownership transfer protocol both qualitatively and quantitatively to evaluate its effectiveness. The analysis shows that the proposed protocol is more secure and requires less computation as compared to existing similar protocols.

Index Terms—Internet of Things (IoT), Ownership validation, Protocol, RFID, Secure ownership transfer.

1 Introduction

INTERNET of Thing (IoT) system consists of pools of globally distributed objects. To collect and locate specific information of an object from this pool, the IoT system requires the identification of each object separately. Therefore each object in the IoT pool needs to be attached and represented by a unique identification. Furthermore, this unique identification leads the IoT system to connect, interact, and cooperate between global objects to achieve a dynamic global information network [1, 2]. With various strengths such as recognition speed, non-line-of-sight operation, capability to identify many objects in one read as well as networking capability, Radio Frequency Identification (RFID) technology has become an attractive solution to address objects' unique identification need in the IoT [3].

However, the business model of IoT dictates that objects in this global network may be owned by different parties at different points in time [2, 6, 7]. Thus, the ownership of an RFID tag requires it to be physically and digitally transferred over to different partners many times as the control on tagged items changes [6, 7]. The internal state of the RFID tags must also reflect these ownership and control changes precisely. This makes secure ownership transfer of the RFID tagged objects an important aspect for the IoT system. Specifically, once RFID tag ownership is transferred to a new owner, only the current owner should be able to interrogate the tag while others should be prevented from communicating with the tag. Moreover, the privacy of both the new and previous owners of the tag must be protected. Therefore, it is imperative that the ownership transfer protocol for RFID tagged object must be able to ensure privacy and security requirements of both the current and previous owners of the object.

The need for secure ownership transfer of RFID tagged objects is well recognized and a number of ownership transfer protocols have recently been proposed [8] [9] [10] [11] [12] [13] [14]. However, existing protocols suffer from a number of vulnerabilities, for example they do not validate an ownership transfer request. Furthermore, these existing proposals do not support all possible ownership transfer scenarios such as one to one, one to many, many to one and many to many [15,16,17]. Therefore, they do not support universal ownership transfer and are not ready to address the need of the IoT. Adapting a separate protocol for each scenario is expensive, a waste of resources and increases the complexity of a large scale distributed system like the IoT. To have an IoT ready ownership transfer protocol, it must be capable of protecting the required security properties of business entities while being universal (supporting all RFID tag ownership transfer scenarios) at the same time [6, 7].

In this paper, we propose a secure and universal object ownership transferring protocol to transfer ownership of an object for the IoT. The main contributions of the proposed work are summarized as follows:

- Validate genuineness of an ownership request and the ownership right of a new partner to own a set of objects
- Ownership transfer and test protocol using simple number theories, the transitivity property and the multiplicative inverse of modular arithmetic to secure IoT system
- A universal ownership transfer to support the IoT

The rest of the paper is organized as follows. In Section 2, we analyse existing similar work in the literature. We present detail system model, system requirements, assumptions and definitions of key concepts in Section 3. The detail of the proposed protocol is presented in Section 4. The security analysis and the comparative study of our protocol against baseline protocol is presented in Section 5. The conclusion is presented in Section 6.

2 Related Work

Although much work has been done to provide privacy and anonymity of RFID systems, the secure ownership transfer protocol has only recently received attention from the research