

Accepted Manuscript

A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things

Guangjie Han, Lina Zhou, Hao Wang, Wenbo Zhang, Sammy Chan



PII: S0167-739X(17)31034-8

DOI: <http://dx.doi.org/10.1016/j.future.2017.08.044>

Reference: FUTURE 3639

To appear in: *Future Generation Computer Systems*

Received date: 18 May 2017

Revised date: 7 July 2017

Accepted date: 23 August 2017

Please cite this article as: G. Han, L. Zhou, H. Wang, W. Zhang, S. Chan, A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things, *Future Generation Computer Systems* (2017), <http://dx.doi.org/10.1016/j.future.2017.08.044>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

A Source Location Protection Protocol Based on Dynamic routing in WSNs for the Social Internet of Things

Guangjie Han^a, Lina Zhou^a, Hao Wang^a, Wenbo Zhang^b, Sammy Chan^c

^aDepartment of Information and Communication Systems, Hohai University, 200 North Jinling Road, Changzhou 213022, China; hanguangjie@gmail.com, zhouln1993@gmail.com, wanghaohu@outlook.com

^bSchool of Information Science and Engineering, Shenyang Ligong University, China; E-mail:zhangwenbo@yeah.net.

^cDepartment of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong; E-mail:eeschan@cityu.edu.hk.

Abstract

With the development of the Internet of Things (IoT), a more humanity-related network called the Social Internet of Things (SIoT) is now evolving. WSNs are also part of the Social Internet of Things (SIoT), a new application of the Internet of Things (IoT). Considering the characteristics of sensor nodes, including limited resource, limited communication capability, and an uncontrollable environment, location privacy protection is a challenging problem for WSNs. In this paper, we propose a source location protection protocol based on dynamic routing to address the source location privacy problem. We introduce a dynamic routing scheme that aims at maximizing paths for data transmission. The proposed scheme first randomly chooses an initial node from the boundary of the network. Every package will travel a greedy route and a subsequent directed route before reaching the sink. Theoretical and experimental results show that our scheme can preserve source location privacy and defeat various privacy disclosure attacks (eavesdropping attack, hop-by-hop trace back attack, and direction-oriented attack) without affecting the network lifetime.

Keywords: source location privacy, Social Internet of Things, wireless sensor networks, cyber attacks

1. Introduction

The Internet of Things (IoT) has developed a lot in recent years [1-2], and the Social Internet of Things (SIoT), a new application of IoT, is now evolving. The SIoT is a larger social network, connecting people and people, people and objects, and objects and objects. Using the perceptual monitoring technology of IoT, every building, car, or shopping mall can post a message automatically, realizing the interaction of people and a specific object. One part of SIoT can be a wireless sensor network (WSN), sensing the state of an object or monitoring an event in the network. Since SIoT enables interaction of an object with people or another object, there will be wireless communication between objects and people. In that case, The use of wireless communication media means that anyone with powerful radio transceivers can attack the network. Because of this vulnerability, SIoT faces security threats such as information eavesdropping, data fabricating, node compromising, and route disrupting. These network attacks threaten either content privacy, the confidential data of a message, or contextual privacy, information about the surrounding network. All these problems make privacy protection of the SIoT becomes essential.

Download English Version:

<https://daneshyari.com/en/article/6873241>

Download Persian Version:

<https://daneshyari.com/article/6873241>

[Daneshyari.com](https://daneshyari.com)