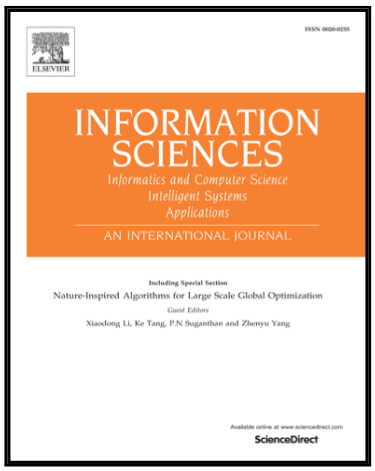

Source-Location Privacy Full Protection in Wireless Sensor Networks

Na Wang, Junsong Fu, Jiwen Zeng, Bharat K. Bhargava

PII: S0020-0255(18)30158-0
DOI: 10.1016/j.ins.2018.02.064
Reference: INS 13469

To appear in: *Information Sciences*

Received date: 30 May 2017
Revised date: 26 February 2018
Accepted date: 27 February 2018

Please cite this article as: Na Wang, Junsong Fu, Jiwen Zeng, Bharat K. Bhargava, Source-Location Privacy Full Protection in Wireless Sensor Networks, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.02.064

Source-Location Privacy Full Protection in Wireless Sensor Networks

Na Wang[a], Junsong Fu[b], Jiwen Zeng[a,*], Bharat K. Bhargava[c]

[a]*School of Mathematical Science, Xiamen University, China*
[b]*School of Electronic and Information Engineering, Beijing Jiaotong University,China*
[c]*Department of Computer Science, Purdue University, USA*

Abstract

In many scenarios, the locations of monitored targets need to be reported by source nodes, but should remain anonymous in wireless sensor networks. Source-location privacy protection is an important research topic. Many schemes have been designed based on different adversarial models. In this paper, a scheme named Source-location Privacy Full Protection (SPFP) is proposed. We consider a more practical adversarial model − a smart adversary − which is a combination of global and local models. To defend against the new adversary, first, we design a lightweight message sharing scheme that is based on congruence equations. Second, each message is mapped to a set of shares. The short lengths of the shares enable them to be processed and transmitted in an energy-efficient manner. The correctness and security of the scheme are proved in theorems. In addition, the proposed message sharing scheme can tolerate the unreliability of the sensor nodes and provides a more reliable data transmission mechanism for networks. Third, the source node constructs a cloud around itself based on the shares and dummy packages to hide its location. The radio actions of the nodes in the cloud are carefully arranged to conceal the real shares from the adversaries and render the nodes in the cloud statistically indistinguishable. Last, a random routing algorithm is seamlessly integrated into our scheme to deliver the real shares from the fake source nodes to the sink node, where the original message is reconstructed based on the received shares. The simulation results illustrate that our scheme can provide adequate protection of source-location privacy with a slight increase in energy consumption.

Keywords: Source-location privacy protection, message sharing, wireless sensor networks, energy-efficiency.

1. Introduction

Wireless sensor networks (WSNs) are composed of a large number of wirelessly linked smart devices that can collaborate to perform various tasks. Due to developments in sensor technology, circuit engineering, information techniques and artificial intelligence, WSNs have been extensively employed

*Corresponding author
Email addresses: 12120067@bjtu.edu.cn (Junsong Fu), jwzeng@xmu.edu.cn (Jiwen Zeng), bbshail@purdue.edu (Bharat K. Bhargava)
URL: wangna@stu.xmu.edu.cn (Na Wang)