Pervasive and Mobile Computing 16 (2015) 36–50

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks

Honglong Chen [a,b,*], Wei Lou [b,c]

[a] College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China
[b] Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong
[c] The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, PR China

ARTICLE INFO

Article history:
Received 11 March 2013
Received in revised form 13 January 2014
Accepted 21 January 2014
Available online 28 January 2014

Keywords:
Local eavesdropper
Location privacy
Wireless sensor networks

ABSTRACT

Wireless Sensor Networks (WSNs) are often deployed in hostile environments to detect and collect interested events such as the appearance of a rare animal, which is called event collection system. However, due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink and eventually capture them by eavesdropping on the sensor nodes' transmissions and tracing the packets' trajectories in the networks. Thus the location privacy of both the source and sink becomes a critical issue in WSNs. Previous research only focuses on the location privacy of the source or sink independently. In this paper, we address the importance of location privacy of both the source and sink and propose four schemes called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper. Simulation results illustrate the effectiveness of the proposed location privacy protection schemes.

1. Introduction

Recent advancement in wireless communications and Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low-cost Wireless Sensor Networks (WSNs), which are made up of a number of sensor nodes that are self-organized for various applications, such as mobile target detection [1], earthquake monitoring [2], and habitat monitoring [3]. In these applications, sensor nodes are deployed to detect the existence of an interested event, such as the appearance of a rare animal. The sensor nodes that detect the occurrence of the interested event will send the detection information to a sink (or base station) by multi-hop wireless communications. Such kind of systems is called event collection system [4], which is one of the important applications in WSNs.

Due to the open characteristic of wireless communications, it is not difficult to attack wireless sensor networks with the goal of either obtaining confidential data or simply disrupting the normal operations of the WSN applications [5–7]. In either case, they may involve threats to one of the following two types of WSN privacy, *content* privacy and *contextual* privacy [8]. The former refers to the confidentiality of the content of the packets passing between the nodes in the network. This is usually guaranteed by using methods of encryption and authentication [9]. The latter refers to the confidentiality of information about traffic patterns in the network, which may be used by adversaries to disrupt the network. The location privacy, i.e., the confidentiality of the location of either source, sink, or both, is a kind of contextual privacy.

* Corresponding author at: College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China. Tel.: +86 13573861376.
E-mail addresses: honglongchen1984@gmail.com, chenhl@upc.edu.cn (H. Chen), csweilou@comp.polyu.edu.hk (W. Lou).

1574-1192/$ – see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2014.01.006

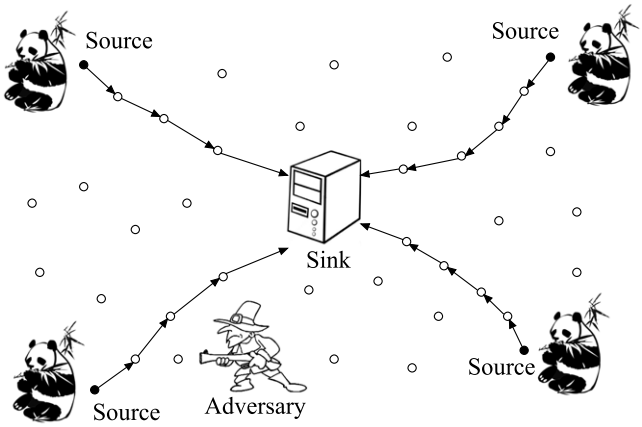

Fig. 1. End-to-end location privacy threat in the habitat monitoring system. The nodes which detect the appearance of the pandas will act as source nodes to send monitoring packets to the sink. The hunter will act as the adversary to attack the system by locating either the source or sink.

To illustrate how information about traffic patterns in a network might be exploited by an adversary, we consider a habitat monitoring application called "*Panda-Hunter*" [8] as shown in Fig. 1, in which a typical WSN is deployed to monitor the appearance of the pandas in the wild field. There is a central controller (sink in Fig. 1) and several pandas in the monitoring field. The sensor nodes which detect the appearance of the pandas will act as source nodes and will send the monitoring packets to the central controller via multi-hop wireless communications. The central controller can then analyze the life habit of the pandas after receiving the monitoring packets or further send the data to a powerful computer for more complex analysis. The scenario is obviously unsafe as the hunter (adversary in Fig. 1) is easily able to either locate a source by back tracing the packet transmissions hop-by-hop to capture the panda or locate the sink by following the flow of packet transmissions to threaten the central controller of the monitoring system. The challenge in this scenario is essentially to protect the end-to-end location privacy rather than merely protect the source or sink location privacy. Thus the end-to-end location privacy protection is a crucial contextual privacy problem in WSNs.

In this paper, we propose four end-to-end location privacy protection schemes to deliver messages from source to sink, which can protect against *local eavesdropper* that might break the location privacy of a source or sink, i.e., the end-to-end location privacy. Hereafter in this paper, we use terms *eavesdropper* and *adversary* interchangeably. The proposed four location privacy protection schemes are called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively. In the forward random walk scheme, every node relays a received packet to a node randomly chosen from its forward neighbors whose hop count to the sink is not larger than its own. To enhance the location anonymity of the source and sink, a tree topology is employed at the two ends of the delivery path respectively in the bidirectional tree scheme. In the dynamic bidirectional tree scheme, branches of the trees are generated dynamically to further improve the performance. However, in the bidirectional tree scheme, real messages are delivered along the shortest path, making it possible for the eavesdropper to infer the location of the source or sink by extending the line of the shortest path. To solve this potential threat, a proxy source and a proxy sink are adopted in the zigzag bidirectional tree scheme, which prevents the adversary from inferring the location of the source or sink easily.

The main contributions of this paper can be summarized as follows:

- We address the importance of simultaneously protecting the location privacy of both the source and sink;
- We propose four schemes to deliver messages from source to sink, which can protect the end-to-end location privacy against the local eavesdropper;
- We demonstrate the effectiveness of the proposed schemes through TOSSIM-based simulations.

The rest of this paper is organized as follows. Section 2 reviews the existing location privacy preserving techniques. Section 3 proposes the system scenario, adversary model and the metrics of location privacy protection. Section 4 describes our proposed four location privacy protection schemes. Section 5 evaluates the performance of the proposed schemes under the TOSSIM platform. Finally, Section 6 concludes this paper and puts forward the future work.

2. Related work

Location privacy protection [8,10–12] for WSNs has been a hot research topic during the past years. Most of existing schemes have addressed the location privacy protection of the source or sink independently:

Source location privacy protection: In [8,13], a source location privacy protection scheme was proposed, which uses the "*Panda-Hunter*" problem as an application scenario for monitoring-oriented sensor networks where the location privacy is important. The *Phantom routing* protocol makes use of a random walk to prevent attackers identifying the source. Xi et al. [10] proposed a two-way random walk routing protocol (from both the source and sink) called *greedy random walk*,