Pervasive and Mobile Computing 11 (2014) 244–260

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Fast track article

Using data mules to preserve source location privacy in Wireless Sensor Networks

Mayank Raj [a,*], Na Li [a], Donggang Liu [b], Matthew Wright [b], Sajal K. Das [a]

[a] Center for Research in Wireless Mobility and Networking (CReWMaN), Computer Science and Engineering Department, University of Texas at Arlington, United States

[b] The Information Security Lab (iSec), Computer Science and Engineering Department, University of Texas at Arlington, United States

ARTICLE INFO

Article history:
Available online 17 October 2012

Keywords:
Source location privacy
Data mules
Alpha-angle anonymity
Wireless Sensor Networks
Mule-Saving-Source protocol

ABSTRACT

Wireless Sensor Networks (WSNs) have many promising applications for monitoring critical regions, like military surveillance and wildlife monitoring. In such applications, it is critical to protect the location of the source sensor that generates the data, as exposure of this information usually reveals the location of the object being monitored. Traditional security mechanisms, like encryption, have been proven to be ineffective as the location of the source can also be revealed by analyzing the traffic flow in the network. In this paper, we investigate the source-location privacy issue. We first propose a realistic semi-global eavesdropping attack model and show its effectiveness in compromising an existing source-location preserving technique. Furthermore, to measure source location privacy against the semi-global eavesdropper, we define a model for α-angle anonymity. Additionally, we design a new protocol called Mule-Saving-Source (MSS) that preserves α-angle anonymity by adapting the conventional function of data mules. We theoretically analyze the delay incurred by using data mules in MSS, and we examine via extensive simulations the trade-off between the delay and privacy preservation under different data mule mobility patterns. We categorize the delay in MSS as being caused primarily due to the buffering time at the source sensor and the data mules. Motivated by this observation, we propose two modifications to MSS, Mule-Saving-Source-Shortest Path (MSS-SP) and Mule-Saving-Source-Two Level (MSS-TL), both aimed at reducing the total delay by reducing the buffering time at the data mule and source respectively. Through theoretical analysis, we examine the delay in the proposed modifications and evaluate their performance with the MSS protocol using a comprehensive set of simulations. Furthermore, to study the impact of the mobility model of the data mules on the MSS protocol, we compare the performance of the MSS protocol by changing the mobility model of data mules to a Random Waypoint based model.

1. Introduction

In recent years, WSNs have played an important role in a number of security applications, like remotely monitoring objects. In such applications, the location of the monitored object is tightly coupled with the sensor that detects it, called the data source. Therefore, preserving the location of the data source is important for protecting the object from being traced. Such a preservation cannot be simply accomplished by encrypting the data packets as the location of the data source can be disclosed by analyzing the traffic flow in WSNs.

* Corresponding author.
E-mail addresses: mayank.raj@mavs.uta.edu (M. Raj), na.li@mavs.uta.edu (N. Li), dliu@uta.edu (D. Liu), mwright@uta.edu (M. Wright), das@uta.edu (S.K. Das).

1574-1192/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.pmcj.2012.10.002

The problem of preserving source-location privacy can be explained using the "Panda-Hunter Game" [1], in which the sensors are deployed in the forest to monitor the movement of pandas. Each panda is mounted with an actuator which signals to the surrounding sensors in its communication range. When the sensor close to the panda receives the signal, it creates and sends data reports to the base station over the wireless network. A hunter who is monitoring the wireless communication between the sensors will be able to identify the direction of incoming traffic flow and trace back the data transmission path to locate the data source, thus catching the panda. In fact, any WSNs used for such monitoring applications are vulnerable to such kinds of traffic analysis based attacks.

There have been extensive techniques proposed to preserve source-location privacy against different attack models: *the local-eavesdropping model* and *the global-eavesdropping model*. Local-eavesdropping [1–4] assumes the attacker's ability to monitor the wireless communication is limited to a very small region, up to very few hops. In the global-eavesdropping model [5–7], the attacker is assumed to be capable of monitoring the traffic over the entire network. We believe both of them are unrealistic, because the former stringently restricts the attacker's ability while the latter exaggerates it, considering the resources and cost required for launching such an attack.

In this paper, we propose a more practical attack model, *the semi-global eavesdropping model*, in which the attacker is able to eavesdrop on wireless communications in a substantial area that is much smaller than the entire monitoring network. This attack model allows the attacker to gather substantially more information than a local eavesdropper. As shown in Section 3, this attack allows the attacker to overcome defenses that defeat a local eavesdropper. On the other hand, without the ability of monitoring the entire network, system designers can consider alternatives to network flooding and other approaches against the global eavesdropping model that suffer from a high communication overhead.

Under the semi-global eavesdropping model, we explore a novel protocol for preserving source-location privacy by using data mules. Traditionally, data mules are used in WSNs for reducing energy consumption due to the data transmission between sensors and facilitating communication in disconnected networks. A data mule picks up data from the data source and then delivers them directly to the base station. We adapt the functionality of data mules so that they not only maintain their traditional functionality, but also facilitate the preservation of the location privacy of data sources.

Our main contributions in this paper are summarized as follows: (1) we propose a new attack model, called semi-global eavesdropping; (2) we introduce a linear-regression based traffic analysis approach to enable the attacker to infer the direction of the data source and demonstrate its effectiveness by breaking an existing routing protocol of preserving source-location privacy; (3) we define the α-angle anonymity model for studying the source-location privacy; (4) we propose a novel protocol, called the Mule-Saving-Source protocol (MSS), that uses data mules to achieve α-angle anonymity; (5) we theoretically analyze the delay in the MSS protocol which includes the buffering time at the data source and the data mule; (6) we propose the Mule-Saving-Source-Shortest Path Protocol (MSS-SP), which aims at reducing the buffering time at the data mules as compared to MSS by modifying the data delivery path of the data mules; (7) we propose the Mule-Saving-Source-Two Level (MSS-TL), which aims at reducing the total delay by restricting the data mules to local areas in the network; (8) we study the impact of the mobility pattern of the data mule on the MSS protocol by changing the mobility model of the data mule to a Random Waypoint based mobility model; and (9) through theoretical analysis and a comprehensive set of experiments we show their effectiveness in reducing the total delay as well as drawing comparisons between them.

The roadmap of this paper is given as follows. We describe the system model and network scenario in Section 2. In Section 3 we introduce the attack model as well as our proposed linear-regression based approach to analyze traffic, followed by the α-angle anonymity model for preserving source location privacy. In Section 4, we present the Mule-Saving-Source protocol to protect the location of the data source. In addition, we theoretically analyze the data delay introduced by our protocol in Section 5. We evaluate the performance of the MSS protocol by analyzing the results from a comprehensive set of simulations in Section 6. The two proposed modifications to the MSS protocols are discussed in Sections 7 and 8 respectively. In Section 9, we study the impact of the choice of the mobility pattern of data mules on the delay in the MSS protocol. We discuss related works in Section 10 and conclude the paper in Section 11.

2. System model

The terrain of our underlying network is a finite two-dimensional grid, which is further divided into cells of equal size. The network is composed of one base station, static sensors, and mobile agents, called data mules.

2.1. Static sensors

All static sensors are homogeneous with the same lifetime and capabilities of storage, processing as well as communication. They are deployed uniformly at random in the cells, and assumed to guarantee the connectivity of the network.

2.2. Data mules

Data mules are the mobile agents which can be artificially introduced in the network [8]. We assume they move independently and do not communicate with each other. Also, they are assumed to know their own locations when they