Information Sciences 321 (2015) 205–223

Contents lists available at ScienceDirect

Information Sciences

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

Probabilistic receiver-location privacy protection in wireless sensor networks

Ruben Rios [a,*], Jorge Cuellar [b], Javier Lopez [a]

[a] Universidad de Málaga, NICS Lab, Campus de Teatinos, 29071 Málaga, Spain
[b] Siemens AG, Otto-Hahn-Ring 6, 81739 Munich, Germany

ARTICLE INFO

Article history:
Received 31 March 2014
Received in revised form 7 January 2015
Accepted 24 January 2015
Available online 4 February 2015

Keywords:
Wireless sensor network
Security
Privacy
Traffic analysis
Node capture

ABSTRACT

Wireless sensor networks (WSNs) are continually exposed to many types of attacks. Among these, the attacks targeted at the base station are the most devastating ones since this essential device processes and analyses all traffic generated in the network. Moreover, this feature can be exploited by a passive adversary to determine its location based on traffic analysis. This receiver-location privacy problem can be reduced by altering the traffic pattern of the network but the adversary may still be able to reach the base station if he gains access to the routing tables of a number of sensor nodes. In this paper we present HISP-NC (Homogenous Injection for Sink Privacy with Node Compromise protection), a receiver-location privacy solution that consists of two complementary schemes which protect the location of the base station in the presence of traffic analysis and node compromise attacks. The HISP-NC data transmission protocol prevents traffic analysis by probabilistically hiding the flow of real traffic with moderate amounts of fake traffic. Moreover, HISP-NC includes a perturbation mechanism that modifies the routing tables of the nodes to introduce some level of uncertainty in attackers capable of retrieving the routing information from the nodes. Our scheme is validated both analytically and experimentally through extensive simulations.

1. Introduction

Wireless sensor networks (WSNs) [30] are highly distributed networks comprising two types of devices, namely, the sensor nodes and the base station. The sensor nodes are small battery-powered computers, which have the ability to measure the physical phenomena (e.g., temperature, vibration, radioactivity) occurring in their vicinity and to wirelessly communicate with other devices nearby. The base station is a resourceful wireless-enabled device in charge of gathering the data coming from different sources and processing them in order to gain insight about the phenomena being monitored.

Due to the number of sensors they can incorporate, these networks are extremely versatile, which makes them suitable for countless application scenarios where sensor nodes are unobtrusively embedded into systems for monitoring, tracking and surveillance operations. Many of these applications are extremely sensitive and thus security and privacy become essential properties [27]. Extensive work has been done on the protection of sensor networks from the physical to the application layer but privacy preservation has only recently drawn the attention of the research community due to the imminent adoption of this technology in scenarios involving businesses, individuals and valuables assets.

* Corresponding author.
E-mail address: ruben@lcc.uma.es (R. Rios).

http://dx.doi.org/10.1016/j.ins.2015.01.016
0020-0255/

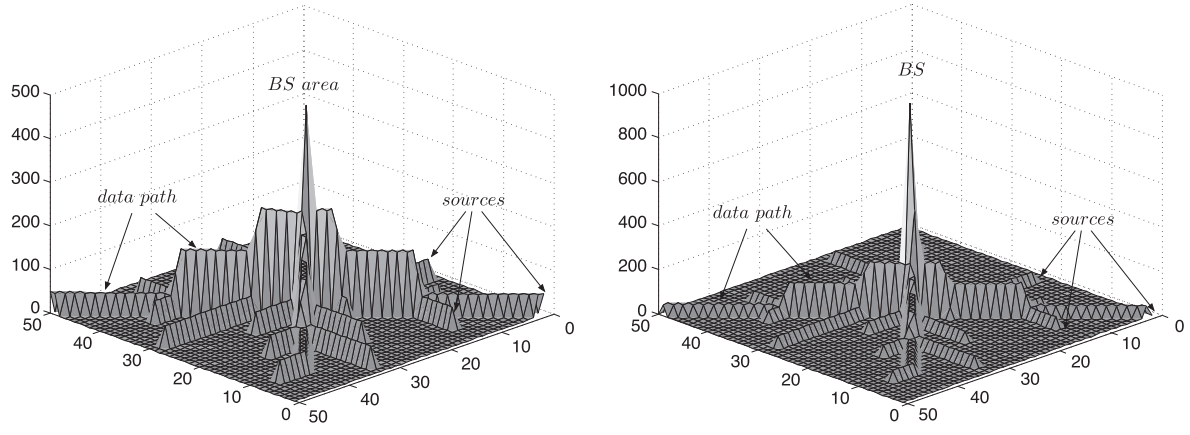
Privacy threats in WSNs can be categorised as content-oriented and context-oriented [19]. Content-oriented privacy focuses on safeguarding the actual data sensed by the nodes [32] and the queries issued to the network [10]. On the other hand, context-oriented privacy refers to the protection of the metadata associated with the measurement and transmission of data. These data include, among other pieces of information [20], the time at which sensitive information is collected and the location of the nodes involved in the communication.

Similarly, there are two main types of location privacy problems affecting sensor networks: source- and receiver-location privacy. The former is concerned with hiding the area where a particular phenomenon is detected while the later is intended to prevent disclosing the location of the base station. For example, in a military scenario, sensor nodes may be deployed to monitor the troops and vehicles belonging to a military force for a better management and control. While moving on the battlefield, the sensors nodes transmit messages which are forwarded to the base station to inform about the units observed and their whereabouts. Even when secure cryptographic algorithms are used to protect the confidentiality and integrity of the communications, the mere presence of messages in the network reveal sensitive information to the enemy: there are troops somewhere in the field. With little effort and not overly sophisticated devices (e.g., a directional antenna) the attacker can deduce more information from the packets he observes and eventually traceback to the original data source. Similarly, the attacker could reach the base station and take control of the network or even render it useless by destroying this critical device. Both source- and receiver-location privacy are important properties but the latter is essential for the integrity and survivability of the network. Besides its importance for the physical protection of the network, the location of the base station is strategically critical because it is most likely housed in a highly-relevant facility. In the aforementioned military scenario, learning the location of the base station gives the attacker an important advantage over the enemy as it is likely housed at military base.

These privacy problems are extensible to any application scenario because they are caused by the singular communication model of WSNs. See in Fig. 1 a typical WSN consisting of 50×50 nodes where 15 nodes are reporting event data using a shortest-path routing protocol. Although this is the most suitable configuration for preserving the limited energy budget of sensor nodes because it minimises the number of nodes involved in the communication process, it also produces very pronounced traffic patterns that reveal the location of both the source nodes and the base station. Ideally, the number of transmissions of each of the nodes should be similar in order to provide an adequate privacy protection level, however this implies a significant energy waste that negatively impacts the lifetime of the network. As a result, a number of techniques [8,14,31] have struggled to randomise the traffic pattern while preserving the limited energy budget of the nodes.

Besides performing traffic analysis attacks, an adversary can exploit the fact that each sensor node stores a routing table to allow the delivery of data to the base station. Normally, the routing tables contain information regarding the distance to or location of the base station. This information can be used by the attacker to effectively reach the base station after inspecting very few routing tables, thus rendering useless the efforts made by the network in deploying anti-traffic analysis mechanisms. Notwithstanding, none of the existing solutions in the literature of receiver-location privacy take this serious threat into consideration. This paper addresses, for the first time, both problems in a single solution, the HISP-NC (Homogenous Injection for Sink Privacy with Node Compromise protection) protocol. On the one hand, HISP-NC data transmission protocol hides the flow of real messages by introducing controlled amounts of fake traffic to locally homogenise the number of packets being forwarded from a sensor node to its neighbours. On the other hand, HISP-NC perturbation scheme modifies the routing tables of the nodes to reduce the risk of node capture attacks while ensuring that data packets eventually reach the base station.

The rest of the paper is organised as follows. Section 2 compares this work with previous location privacy solutions in the area of WSNs. Section 3 describes the network and threat models as well as the main assumptions applicable to the rest of



(a) Number of packets sent (b) Number of packets received

Fig. 1. Single-path routing protocol.