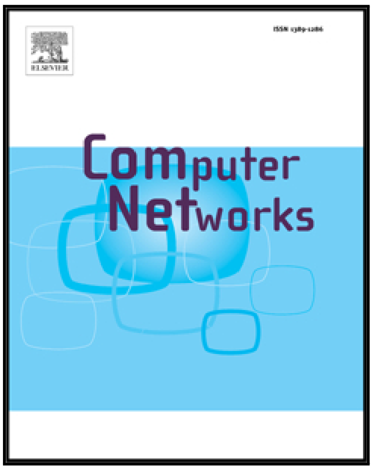

Load-conscious Maximization of Base-station Location Privacy in Wireless Sensor Networks

Nikolaos Baroutis , Mohamed Younis

PII: S1389-1286(17)30265-7
DOI: 10.1016/j.comnet.2017.06.021
Reference: COMPNW 6248

To appear in: *Computer Networks*

Received date: 7 April 2017
Revised date: 6 June 2017
Accepted date: 20 June 2017

Please cite this article as: Nikolaos Baroutis , Mohamed Younis , Load-conscious Maximization of Base-station Location Privacy in Wireless Sensor Networks, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.06.021

Load-conscious Maximization of Base-station Location Privacy in Wireless Sensor Networks

Nikolaos Baroutis and Mohamed Younis
Dept. of Computer Science and Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD 21250
nikbar1, younis@umbc.edu

Abstract – In various applications of Wireless Sensor Networks (WSNs), sensor nodes forward data packets towards an in-situ base-station (BS) over multi-hop routes. The BS not only collects and analyzes the incoming data, but also interfaces the WSN to a higher authority. The unique role of the BS attracts adversary's attention since it can be a single point of failure for the WSN. An adversary that seeks to diminish the network utility can apply traffic analysis techniques in order to uncover the sink of all traffic (i.e., the BS) and target it with denial of service attacks. In this paper, we present a technique for preserving location privacy of the BS. Our technique injects deceptive transmissions aiming to even the traffic density across the network and make the BS undistinguishable. We highlight the trade-off between location privacy and network's performance/lifetime, and show how our technique strikes a balance between conflicting metrics. The simulation results confirm that our proposed traffic analysis countermeasure effectively boosts the location privacy of the BS without a significant impact on the network's performance and lifetime.

Keywords—Location privacy; Anonymity; Traffic analysis techniques; Wireless sensor networks.

1. Introduction

Recent years have witnessed major advances in microelectronics where sensing, processing and communication circuits could be integrated in miniaturized devices, referred to by the technical community as sensor nodes. Deploying these sensor nodes in large numbers and internetworking them through wireless links can provide unprecedented opportunities for a wide variety of military and environmental applications such as combat field reconnaissance, border protection, security surveillance, forest fire detection, etc. [1]. A WSN typically consists of a large population of spatially distributed sensor nodes that cooperatively monitor their surroundings by measuring ambient conditions such as temperature, lightning condition, pressure, humidity, etc., and report their findings to an in-situ BS over wireless links. The BS collects and analyzes the incoming data prior to sharing with remote users [2].

The employed sensor nodes are small-sized battery-operated devices. Since decreasing the transmission range of a sensor node results in energy saving and consequently extends the lifetime of the network, routing of data packets to the BS over multi-hop paths is quite popular in WSNs [1][2]. However, as data packets are forwarded towards the BS their routes merge in the vicinity of BS, and consequently, nodes closer to the BS experience higher transmission rate. Such transmission pattern can expose the whereabouts of the BS as we explain below. Figure 1, shows an example of a WSN where arrows represent the routing topology, antennas represent the sensor nodes, and the computer represents the BS.