Ad Hoc Networks 32 (2015) 53–80

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Increasing base station anonymity using distributed beamforming

Jon R. Ward*, Mohamed Younis

Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, United States

ARTICLE INFO

Article history:
Received 6 June 2014
Received in revised form 8 November 2014
Accepted 2 January 2015
Available online 14 January 2015

Keywords:
Anonymity
Location privacy
Distributed beamforming
Cooperative communication
Traffic analysis
Internet of Things

ABSTRACT

Advances in wireless communication technologies have enabled the networking of devices, which conventionally operated standalone, to form an Internet of Things (IoT). A typical network architecture consists of a set of data sources that report to a base station (BS), e.g., a data aggregation unit, over multi-hop paths. An example of such a network operation model includes surveillance of an unattended area using wireless sensor nodes, and advanced metering within a smart power grid. The unique role of the BS makes it a natural target for an adversary that desires to achieve the most impactful attack possible against an IoT network. Even if a network employs conventional security mechanisms such as encryption and authentication, an adversary may apply traffic analysis techniques to exploit unique traffic patterns within the network and ultimately identify the BS. The first step to successfully protect the BS from attack is to keep the BS's identity, role, and location anonymous. This paper proposes a novel, cross-layer approach that boosts BS anonymity using distributed beamforming. We demonstrate that the characteristics of distributed beamforming make it extremely effective in improving BS anonymity in a wireless network while minimizing the amount of required communication energy overhead. Through analysis and simulation we demonstrate that the proposed approach is both efficient and effective at countering an adversary that employs evidence theory analysis to locate the BS.

1. Introduction

A current trend in industry is to equip many of the conventional data collection and control devices with wireless communication capabilities to enable the networking of these devices and enhance new applications. Such a trend has led to the notion of an Internet of Things (IoT), where a diverse and/or large set of devices collaboratively achieve a task or provide a service [1,2,3]. Some examples of IoT applications include a digital battlefield and the smart grid. The operation model of many IoT applications involves the dissemination of data collected by the various devices over multi-hop paths to a base-station (BS) that processes the data. For example, in smart grid or Advanced Metering Infrastructure (AMI) systems [1,4], utility data are collected in the home using a Home Area Network (HAN) and relayed to the larger Wide Area Network (WAN). As illustrated in Fig. 1, the HAN comprises wireless sensors that monitor utility conditions, trends, and usage data within a home and reports information to a smart meter. Each smart meter then forwards this information to a BS or Data Aggregation Unit (DAU) that serves as the data sink for a neighborhood-sized IoT network [1,2]. The IoT-based smart grid provides utility companies with attractive benefits of improved power supply and demand estimation through trend data and remote control of smart meters for automated reading and configuration.

* Corresponding author.
E-mail addresses: jward3@umbc.edu (J.R. Ward), younis@umbc.edu (M. Younis).

http://dx.doi.org/10.1016/j.adhoc.2015.01.001
1570-8705/© 2015 Elsevier B.V. All rights reserved.

However, the interconnectivity of IoT increases the risk of attack from a nefarious adversary. The BS is a natural focal point for the adversary since a denial of Service (DoS) attack against it would impact the larger network and a man-in-the-middle attack against the BS provides the adversary with the opportunity to collect private user data [5]. The BS not only serves as a data sink, but also provides basic control and management features such as protocol synchronization, a gateway to other networks, and operator failure notifications; an attack against it would cripple the larger network. Therefore, the most successful protection for the BS against a malicious adversary's attack is to remain anonymous in role, identity, and location. Unfortunately, such protection is not provided by frequently published conventional security mechanisms that achieve confidentiality, integrity and authentication and little attention has been paid to the problem of BS anonymity [6].

The majority of research in the field of anonymity to date has focused on routing algorithms that attempt to hide true routes from source to sink [7–9]. Although anonymous routing methods may largely mitigate the threat of an adversary that analyzes routing trends, the adversary may deduce significant information by analyzing link-layer, pair-wise node relationships from which the location and role of the BS can be inferred [10]. Other techniques to increase anonymity have focused on nodes that generate dummy traffic or flood the network such that true routes are obfuscated; however, the overhead in terms of excessively consumed communication energy, increased delay, and decreased throughput may not be tolerable to specific applications. Furthermore, a strategy of employing multiple BSs is not considered a solution since each BS can be individually targeted.

In this paper, we propose a novel, cross-layer technique that leverages distributed beamforming cooperation to increase the BS's anonymity. Distributed beamforming has recently received attention as a method for improving communication range, data rate, energy efficiency, physical-layer (PHY) security [11], and reducing interference in distributed wireless networks [12,13]. In distributed beamforming, nodes with single antennas cooperate and share antennas to form a virtual multi-antenna system. Multiple nodes transmit simultaneously, accounting for wireless channel conditions and precisely controlling the signal phase, such that all signals constructively combine at the destination. For example, under ideal conditions N distributed beamforming transmitters that send identical messages using equal power while incurring equal channel conditions when transmitting to a common destination will achieve a factor of N increase in power at that destination. Although distributed beamforming techniques have not yet been included in commercial standards and products, practical implementations based on software-defined radio (SDR) have overcome many of the design challenges that we discuss throughout this paper [14–16].

Because distributed beamforming is inherently a PHY transmission technique, it provides a powerful approach to boost BS anonymity as either a stand-alone capability or combined with published higher-layer countermeasures. Additionally, an IoT network implementing distributed beamforming enjoys the aforementioned benefits of improved range, data rate, energy efficiency, and decreased interference. Our analysis focuses on employing distributed beamforming as a stand-alone countermeasure for traffic analysis. Specifically, we make the following contributions:

- Develop an attack model that factors in acknowledgement messages to better reflect the adversary's traffic analysis capabilities.
- Develop an energy-aware relay-selection algorithm for diminishing detectability of pair-wise communication links.
- Develop a distributed beamforming protocol to boost anonymity in IoT networks.
- Provide guidelines for employing the proposed protocol in practical IoT settings.
- Validate the performance of the distributed beamforming protocol.

This paper is organized as follows: Section 2 summarizes related work. Section 3 discusses the WSN and adver-

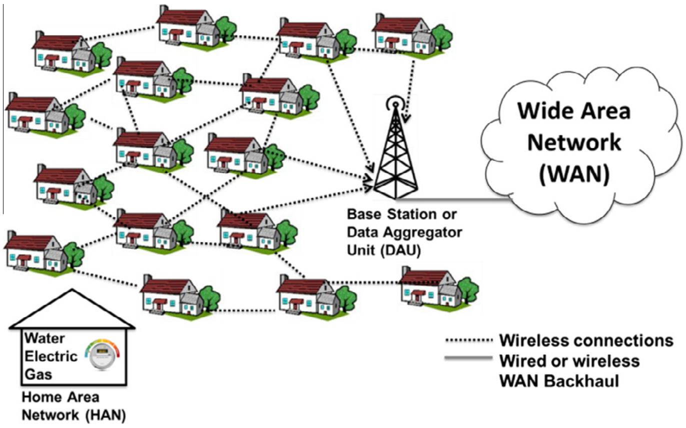

Fig. 1. Example of meter data collection in a smart grid [4].