Contents lists available at ScienceDirect

Ad Hoc Networks

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

Optimal data compression for lifetime maximization in wireless sensor networks operating in stealth mode

Davut Incebacak [a], Ruken Zilan [b], Bulent Tavli [c], Jose M. Barcelo-Ordinas [b,*], Jorge Garcia-Vidal [b]

[a] Middle East Technical University, Ankara 06800, Turkey
[b] Universitat Politecnica de Catalunya-BarcelonaTECH (UPC), Computer Architecture Department, Barcelona 08034, Spain
[c] TOBB University of Economics and Technology, Electrical and Electronics Engineering Department, Ankara 06560, Turkey

ARTICLE INFO

Article history:
Received 4 March 2014
Received in revised form 27 June 2014
Accepted 29 July 2014
Available online 7 August 2014

Keywords:
Wireless sensor networks
Contextual privacy
Data compression
Network lifetime

ABSTRACT

Contextual privacy in Wireless Sensor Networks (WSNs) is concerned with protecting contextual information such as whether, when, and where the data is collected. In this context, hiding the existence of a WSN from adversaries is a desirable feature. One way to mitigate the sensor nodes' detectability is by limiting the transmission power of the nodes (*i.e.*, the network is operating in the stealth mode) so that adversaries cannot detect the existence of the WSN unless they are within the sensing range of the WSN. Position dependent transmission power adjustment enables the network to maintain its level of stealth while allowing nodes farther from the network boundary to use higher transmission power levels. To mitigate the uneven energy dissipation characteristic, nodes that cannot dissipate their energies on communications reduce the amount of data they generate through computation so that the relay nodes convey less data. Dynamic data compression/decompression strategies reduce the amount of data to be communicated, thus, they achieve better energy savings when compared to static compression/decompression of data in which the data is always compressed independently of the power transmission strategy. In this study, we investigate various data compression strategies to maximize the lifetime of WSNs employing contextual privacy measures through a novel mathematical programming framework.

1. Introduction

Wireless Sensor Networks (WSNs) are comprised of a plurality of low cost, limited power, and tiny sensor nodes. In WSN applications such as surveillance, physical measurements are taken by the sensors and reported to the sink node. One of the concerns in the design of a WSN is privacy preservation. Privacy enabling techniques are focussed with two main issues: data-privacy and contextual privacy. *Data-privacy* oriented techniques address the problem of preserving the privacy of the data collected by the sensors. On the other hand, adversaries are also interested in extracting contextual information (*e.g.*, which wireless sensor node has detected the object of interest?). *Contextual Privacy* focus on hiding the identity and location of the nodes, hiding traffic flows, and rendering the task of contextual information extraction more challenging (*i.e.*, defense-in-depth).

Under this scenario, many mechanisms that appear in the literature [1,2], propose the introduction of redundant traffic or extra transmissions. Lowering the transmission power avoids the introduction of these extra transmissions, but still remains the issue of reducing the energy consumption and balancing the load to evenly distribute the energy dissipation. Tavli et al. [3], introduced a Linear

* Corresponding author.
E-mail addresses: idavut@metu.edu.tr (D. Incebacak), rzilan@ac.upc.edu (R. Zilan), btavli@etu.edu.tr (B. Tavli), joseb@ac.upc.edu (J.M. Barcelo-Ordinas), jorge@ac.upc.edu (J. Garcia-Vidal).

http://dx.doi.org/10.1016/j.adhoc.2014.07.019
1570-8705/© 2014 Elsevier B.V. All rights reserved.

Programming (LP) framework for studying the tradeoffs in network lifetime and load balancing in contextual privacy scenarios under uniform sensor node deployments.

Data compression has widely been used to reduce the amount of traffic sent in a WSN, thus, to reduce the energy consumption. Yu et al. [4] proposed the concept of tunable compression that is able to adjust the computational complexity of loss-less data compression based on the energy availability. The concept comes from compression tools such as gzip in which there are ten different levels of compression ratios. Since data compression and decompression in the nodes also dissipate energy, it is important to determine the energy savings achieved by different compression strategies.

There is a clear trade-off in the energy consumed by compressing/decompressing data and the savings obtained by sending less amount of data to next-hop nodes. Lowering the transmission power minimize the domain in which attackers may lie, however, such a contextual privacy preservation approach also renders some links inoperable that can be used to balance the energy dissipation throughout the WSN. Hence, the inter play among data compression/decompression, load balancing, and the extent of the vulnerable domain (*i.e.*, the area where adversaries may lie outside the sensing domain) is explored in this paper.

This paper is a substantially improved and expanded version of an earlier conference paper [5], where we investigated the effects of several data compression strategies on WSN lifetime while providing stealth mode of operation through an LP framework. In fact, the LP framework in [5] is obtained by integrating the LP frameworks presented in [3,6]. Nevertheless, the main contribution of this study is the consideration of more practical aspects of data compression in WSNs providing contextual privacy against adversaries. More precisely stated, this paper extends the concept introduced in [5] by investigating the effects of Optimal Single Level Compression (OSLC) and Limited Compression (LC) strategies through Mixed Integer Programming (MIP) models. Furthermore, we explore the impact of node density and limited transmission range due to contextual privacy scenarios.

The rest of the paper is organized as follows. An overview of the related work is presented in Section 2. We construct and describe the mathematical programming framework in Section 3. Numerical analysis to explore the parameter space and to compare the performances of the proposed strategies are given in Section 4. Conclusions are given in Section 5.

2. Related work

Privacy preservation in the context of WSNs has been surveyed in [1,2]. Li et al. [1] focus their survey on data-oriented and context-oriented privacy while Conti et al. [2] focus their survey on context-oriented privacy techniques, more precisely, on Source Location Privacy (SLP) which is a term to express security measures for hiding the location of the source nodes. The authors classify adversaries having a partial view of the network as local adversaries while those ones having a total view of the network as global adversaries. An example solution against global attackers is the use of Network Coding [7] which have the disadvantage of increasing complexity in the sensing nodes. Most of the solutions proposed defend the network against local adversaries using techniques such as random walk [8], cyclic entrapment [9], delaying the packet [10] or limiting node detectability [3,11]. Some other techniques are able to defend the network against local or global adversaries utilizing implementation dependent approaches (*e.g.*, use of dummy packets [8]).

As discussed earlier, our work can be classified within the limiting node detectability solutions proposed against local adversaries. Another prominent study in this class is by Dutta et al. [11] where it is considered that the attackers measure raw physical properties of messages like angle of arrival or the signal strength of the detected signal. In order to defend against this kind of attackers, they propose anti-localization by silencing in which sensors intelligently predict their own importance as a measure of two conflicting requirements: *localize the adversary* and *hide from the adversary*. Only some sensors will participate in message exchanges reducing the probability that the adversary detects events.

Our work deals with the hypothesis that local attackers want to be undetected while they observe the network. By limiting the transmission power of the nodes, node detectability is restricted to a limited area outside the sensing area. In general, as Cheng et al. [12] show, limiting the transmission power implies the use of non-optimal routing paths with respect using the maximum transmission ranges, impacting, thus, the network lifetime. Tavli et al. [3], analyze the lifetime bounds improving contextual privacy by transmission range control. The authors show that maximizing the network lifetime increases the unobservability area in which the attacker can be placed, while decreasing the transmission range, network lifetime is reduced but the unobservability area is also reduced.

Data compression allows reducing the amount of data to be sent to the sink. In general, compression ratios and time complexity are the metrics used by compression algorithms to evaluate the performance of the mechanisms. Srisooksai et al. [13], survey data compression mechanisms in WSN. The authors classify data compression mechanisms into two broad classes: *distributed data compression* and *local data compression*. Distributed data compression approaches such as Distributed Source modeling (DSM), Distributed Transform Coding (DTC), Distributed Source Coding (DSC) and Compressed Sensing (CS) techniques are, typically, employed in dense sensor deployment cases. In our paper, we consider local data compression techniques that usually exploit temporal correlation of the data and do not depend on the specific WSN topologies. These techniques are classically categorized as lossless and lossy compression schemes. Examples of lossless compression are the well known LZW (Lempel–Ziv–Welch) algorithm and the simple lossless entropy compression (LEC) scheme proposed for WSNs by Marcelloni and Vecchio [14] while an example of lossy compression in WSNs is the Lightweight Temporal Compression (LTC) scheme proposed by Schoellhammer et al. [15].