Exploring the Asymptotically Tight Boundaries of Query Anonymity in Wireless Sensor Networks

Alireza Mortezaei

June 23, 2014

Contents

List of Figures

List of Tables

Chapter 1

Introduction

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

1.1 Wireless Sensor Networks (WSN)

Wireless Sensor Networks (WSN) are a new breed of distributed systems. The special feature of WSNs is that they are an integrated part of the environment they inhabit and are designed to closely monitor their surroundings. They are a step closer to eliminating the gap between the physical and the virtual world. These networks are easily scalable, cost efficient and can obtain types of data that would be impossible to obtain using traditional approaches, for example, data obtained from hard-to-reach areas. WSNs have a wide range of applications in military, environmental science, health science, crisis management etc. WSNs consist of many sensor nodes called motes. These motes collect data and communicate with one another to provide a real-time data feed. These motes can often self-organize after being deployed in an ad hoc fashion[?].
WSN technology currently is at its infancy stage and there are many aspects

of these systems such as security that still needs addressing. Since the architecture of these networks is drastically different from computer networks, it is difficult to directly employ the existing security approaches to the area of WSNs. The networks are fragile with respect to privacy measures. In the paper *Query privacy in wireless sensor networks*[**?**], several strategies that address the problem of preserving the privacy of clients querying a wireless sensor network owned by untrusted organizations are offered. However, the paper does not fully explore the performance analysis of these strategies and the amount of the performance overhead imposed by these privacy measures is unknown. The goal of our project is to explore this "security versus performance" tradeoff and find exact performance boundaries of these strategies. One of the main steps towards analyzing the performance of such strategies is to simulate them in a network using a simulation tool.

1.2   Problem Statement

In this literature we will explore the asymtotically tight boundaries of communication cost as a function of the privacy provided theough the size of the anonymity set. In this context, privacy can be defined as attackers ability to guess the intended target of a query. Using discrete anonymity sets of size a, the attacker cannot guess the exawith a probability

1.3   Related Work

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use   in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Chapter 2

Discrete Anonymity Sets (DAS) Model of Privacy

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.1 Threat Model

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.2 Network Model

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.2.1 Topological Arrangements

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.2.2 Communication Model

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.2.3 Routing

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space.

The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.3   Cost Model

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

2.4   Analytical Boundaries

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Chapter 3

Experimental Methods

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1 Simulation Framework

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1.1 TinyOS and Tossim

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is

sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1.2   Network Configuration and Setup

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1.3   Packet Format

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1.4   Topology Generation

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to

obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.1.5   Limitations and Considerations

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.2   Simulation Scenarios

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.2.1   Grid Topology

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Network Construction

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Anonymity Set Arrangements

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Worst Case Scenario

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

3.2.2   Random Network

We now generalize our results to a random topology for the WSN. Random topology is the generalized form of WSN network topologies encapsulating any toppology that can be presented by a unit disk graph, a sub-class of geometric graph. We explore worst case and average case scenario under

this generalized from in order to account for all forms of WSN network arrangments which may not necessarily have the potential to be divided into distinct and organized regiones in an intuitive maner. For example, a WSN deployed in an adhoc fashion might require a much finer granuality in their application. Examples of such WSNs are those deployed in military zones in through airborn means for the purpos of monitoring enemy's troops and vehicles movements on the ground.

Networks in this scenario are all homogenious networks and use source routing to guide the packets through the network. Three main characteristics of the random WSN that we will closely observe are n, the size of the network in terms of the number of motes it contains; d, the diameter of the network which the length of the longest shortest path in the network and a the size of the anonymity set.

Network Construction

To construct random WSNs we use the notion of random geometric graph. A random geometric graph is a random undirected graph generated by

To follow this model of network construction and

Anonymity Set Arrangements

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use   in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Worst Case Scenario

In the context of random topologies, the nature of the worst case scenario is closely related to the way annonymity sets are constructed. The first step in the construction of

Chapter 4

Experimental Results

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.1 Grid Topology

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.1.1 Case 1: $a \leq O(n)$

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is

sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.1.2 Case 2: $a > O(n)$

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.2 Random Topology

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.2.1 Case 1: $a \leq O(d)$

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to

obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

4.2.2 Case 2: $a > O(d)$

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing

Chapter 5

Conclusion

LaTeX determines itself how to break up a paragraph into lines, and will occasionally hyphenate long words where this is desirable. However it is sometimes necessary to tell LaTeX not to break at a particular blank space. The special character used for this purpose is . It represents a blank space at which LaTeX is not allowed to break between lines. It is often desirable to use in names where the forenames are represented by initials. Thus to obtain 'W. R. Hamilton' it is best to type W. R. Hamilton. It is also desirable in phrases like 'Example 7' and 'the length l of the rod', obtained by typing