# Providing Location Obscurity in Wireless Sensor Networks

Rashmi H P
M.Tech, IV SEM CS&E
T.John Institute of Technology
Banglore-560083
email:hprashurohini@gmail.com

Suma R
Assistant Professor
Dept.of CS&E
T.John Institute of Technology
Banglore
,

**Abstract**— Source location anonymity is an attractive and critical security property. Most of prior works assumed a weak adversary model where the adversary sees only local network traffic, but here we consider source anonymity against a global eavesdropper. In certain applications, the locations of events reported by a sensor network need to remain anonymous. That is, When analyzing Network traffic unauthorized observers must be unable to detect the source of such events. The foundations of a formal framework, we propose a new model for analyzing and evaluating anonymity in sensor networks. The novelty of the proposed framework is twofold: first, it introduces the notion of "interval indistinguishability" that is stronger than existing notions; second, it provides a quantitative measure to evaluate anonymity in sensor networks. By analyzing current anonymous designs under the proposed model, show how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information. Finally, we discuss how existing solutions can be modified to improve their anonymity.

***Keywords***— wireless sensor network**,** origin location, movement, binary converstion,real message,fake message,SSA.

## I. INTRODUCTION

The wireless sensor network of spatially distributed autonomus sensors to monitor physical and environmental conditions such as temperature,sound,pressure etc. and to cooperatively pass their data through the network to a main location. In certain application,the location of events reportedby a sensor network.Three parameters that can be associated with an event detected and reported by a sensor node:description of event,time of event,and location of event.privatly transmitting the description of a sensed event can achived via encryption primitives and spatial information of reported events cannot besed achived via cryptographic[10][11].Encrypting a message befoer transmisstion,can hide the context of the message from unauthorized users,but the existence of the cipher text of information transmission.

The source anonymity problem that provide time and location privacy for events reported by sensor nodes and this problem increasing research attention.This problem addressed under two different types of adversaries.first,local adversary is limited mobility and partial view of network traffic.In routing based techniques have to be effective in hiding the location of reported event against local adversaries.second,global adversary is ability to monitor the traffic of the entire network.In routing based technique is ineffective in hiding location information in event triggered transmission.This due to that,Since a global adversary has full view of network,it can immediately detect the source and time of the event-trigered transmission.

This paper proposed to improve anonymity in wireless sensor network.Towards achieving source anonymity in the presence of global adversaries ,nodes to transmit fake messages even no detection of event of interest.When real event occurs,its report can be embedded within the transmissions of fake messages.

The statistical source anonymity (SSA) problem in sensor networks is prevent global adversaries from exposing source location by performing statistical analysis on nodes transmissions.The main objective of our project is minimizing delay and maximizing the lifetime of sensors batteries.

In this paper to proposed framework for modeling,analzing,and evaluating anonymity in sensor network.To introduce the notion of “interval indistiguishability” and illustrate how the problem of source anonymity can be mapped to the problem of interval indítiguishability and propose quantitative measure to evaluate source anonymity in sensor networks. In coding theory, analyze existing solutions under the proposed model. By finding a transformation of observed data, convert the problem from analyzing real-valued samples to binary codes and identify a possible anonymity breach in the current solutions for the SSA problem.

In statistical decision theory, the term “nuisance parameters” refers to information that is not needed for hypothesis testing and, further, can preclude a more accurate decision making . When performing hypothesis testing of data with nuisance parameters, it is desired (even necessary in some scenarios) to find an appropriate transformation of the data that removes or minimizes the effect of the nuisance information.

In binary hypothesis testing, given two hypothesis, H0 and H1, and a data sample that belongs to one of the two hypotheses (e.g., a bit transmitted through a noisy communication channel), the goal is to decide to which hypothesis the data sample belongs. In the statistical strong anonymity problem under interval indistinguishability, given an interval of intertransmission times, the goal is to decide whether the interval is fake or real (i.e., consists of fake transmissions only or contains real transmissions).

## II EXISTING SYSTEM

Existing Wireless sensor networks once sensor nodes have been deployed, there will be minimal manual intervention and monitoring. But, when nodes are deployed in a hostile environment and there is no manual monitoring.

Limitations of existing system:

- It's easy for hackers to hack it as we can not control propagation of waves.
- Comparatively low speed of communication.

## III PROPOSED SYSTEM

To improve anonymity, we suggest introducing the same correlation of inter-transmission times during real intervals to inter-transmission times during fake intervals.

Advantages of proposed system:

- It avoids a lot of wiring.
- Minimizing delay and maximizing lifetime of sensors batteries.

## IV SYSTEM DESIGN

### 4.1 Design Constraints

The project aims to improve source anonymity.we propose the framework for modeling, analyzing, and evaluating source anonymity in sensor network.The novelty of the proposed framework is two fold: ”interval indistinguishable” and maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. Then finaly analzing existing solution to design source anonymity.in sensor network.

### 4.2.Interfaces

Interface refers to a point of interaction between components and is applicable at the level of hardware and software.

#### 4.2.1User Interface

A user interface is the system by which users interact with a machine. The user interface includes hardware (physical) and software (logical) components. User interfaces exist for various systems, and provide a means of input that allow the users to manipulate a system, and output that allow the system to indicate the effects of the users manipulation.

### 4.3 High Level Design

Software Development is generally a stepwise process. Before the process of implementing the software at hand it involves the process of software design. A software design is a description of the structure of the software to be implemented, the data which is part of the system, the interfaces between the components, sometimes, the algorithms used. Designers do not arrive at a finished design immediately but develop the design iteratively through a number of different versions. The design process involves adding formality and detail as the design is developed, with constant backtracking to correct earlier designs.

In many software development projects, software design is an ad hoc process. Starting from the set of requirements, usually in natural language, an informal design is prepared. Coding commences and the design stage is modified as the system is implemented. When the implementation stage is complete, the design has usually changed so much from the initial specification that the original design document becomes an incorrect and incomplete description of the system. There are several advantages of the design phase. Some of them are listed below:

- The design phase helps to understand the user requirements and helps to map the user requirements into implementation phase.
- The iterations in the design phase helps in incorporating as many user requirements as possible in the final software being developed.
- The design phase reduces the cost involved in the development of the software as many changes would be made to the software in the implementation if the design is not clear.

The design process is iterative and requires consideration of various design alternatives at every stage. The objective of the design stage is to produce the overall design of the software. The design stage involves two sub-stages namely:

- High-Level Design
- Detailed-Level Design

In the High-Level Design, the Technical Architect of the project will study the proposed applications functional and non-functional (qualitative) requirements and design overall solution architecture of the application, which can handle those needs. High Level Design means precisely that. A high level design discusses an overall view of how something should work and the top-level components that will comprise the proposed solution.

It should have very little detail on implementation, i.e. no explicit class definitions, and in some cases not even details such as database type (relational or object) and programming language and platform. In this chapter we give an overview of the design of the system and how it is organized and the flow of data through the system. By reading this document the user should have an overall understanding of the problem and its solution. We have also discussed about the problems encountered during the design of the system and justified the use of the design. The Data Flow Diagrams (DFD), given in the later sections of the chapter, shows the flow of data through the system.

## 4.4 Design Considerations

The design process is iterative and requires consideration of various design alternatives at every stage. The design process is constrained by the assumptions made prior to the development of the system. It involves deciding on the type of approach used for the development of each portion of the system with the rationale for the selection of the same. Thus this section describes many of the issues which need to be addressed or resolved before attempting to devise a complete design solution.

### 4.4.1 Assumptions and Dependencies

Several assumptions regarding the hardware required and the working environment of the system influence design decisions. The assumptions have been made after considerable consultation with the end user and are more or less reasonable.

- The system will be implemented on the Windows operating system, using Java. The system should be modified so as to enable its use on the Linux operating system as well.
- The system runs on the Windows Operating System which is Windows XP or above.

### 4.4.2General Constraints

There might be some global limitations or constraints that have a significant impact on the design of the system’s software or an associated impact. Such constraints may be imposed on the following issues related to our project which are as follows:

- There exists a maximum limit on the number of nodes that can be deployed in the network so as to prevent degradation in performance of the proposed algorithm while it is being executed on the system.
- As the number of nodes increases, the complexity of showing different cases for the algorithm becomes difficult. Therefore, we limit ourselves to a fewer number of nodes for demonstration purpose.

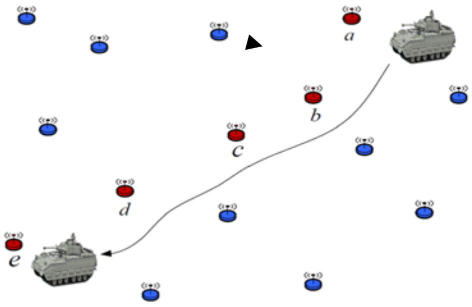
## V SYSTEM ARCHITECTURE

The system is developed using the Top-Down approach. In this method, the system divides the files based on the number of nodes. Each node downloads the files and then requests the missing files from the neighboring nodes.

- The 'JAVA' programming language has been used for development of the application.
- The WINDOWS XP or later versions of windows XP operating system has been used as the platform for development.
- The processes communicate through Sockets.

### 5.1 System Architecture

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system.An architecture description is a formal description and representation of a system,organized in a way that supports reasoning about the structure of the system which comprises system components, the externally visible properties of those components, the relationships between them, and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. The language for architecture description is called the architecture description language (ADL).The main behind this project to improve anonymity in sensor network introducing the same correlation of inter-transmission times during real intervals to inter-transmission times during fake intervals.

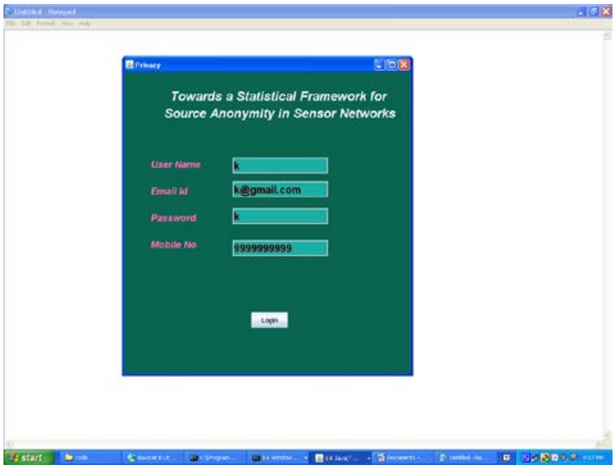


That is, let the transmission procedure consists of two different algorithms: AR and AF . In the presence of real events , algorithm AR is implemented. In the absence of real events , algorithm AF is implemented. In algorithm AF , the nodes generates two sets of events independently of each other: "dummy events" and fake events. Fake events serve the same purpose they serve in algorithm AR, that is, they are used to hide the existence of real transmissions. Since there are no real events in fake intervals, however, dummy events are generated to be handled as if they are real events. That is, dummy events are generated independently of fake messages and, upon their generation, their transmission times are determined according to the used statistical goodness of fit test. The purpose of this procedure is to introduce the same correlation of real intervals into fake intervals. That is, not only the two sequences of intertransmission times will be statistically indistinguishable by means of statistical goodness of fit tests, but also the binary codes representing fake and real intervals will have the same statistical behavior.

.

## VI RESULTS

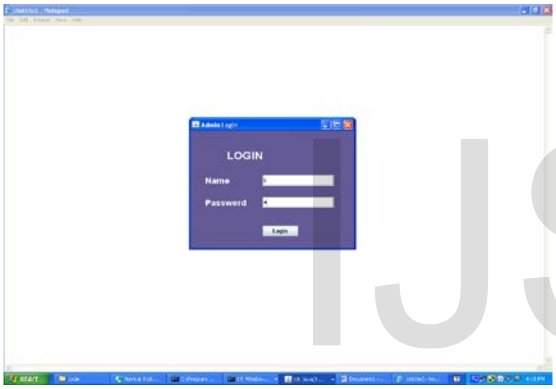
### 6.1 User registration form



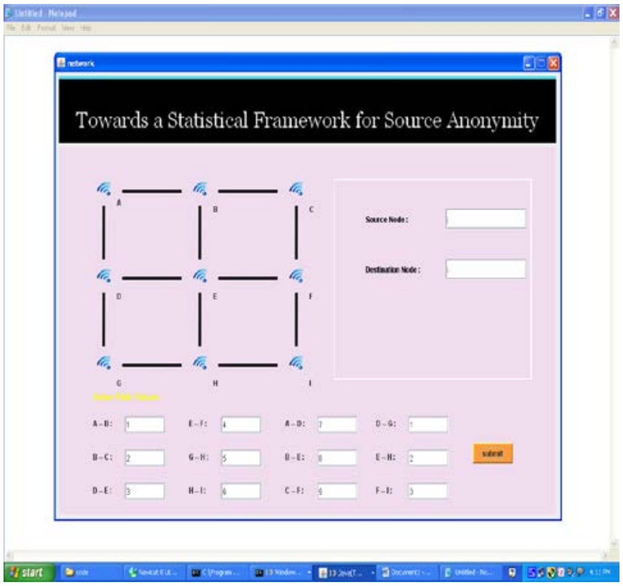
Towards a Statistical Framework for Source Anonymity in Sensor Networks

User Name: k
Email id: k@gmail.com
Password: k
Mobile No: 9999999999

6.2 user login page



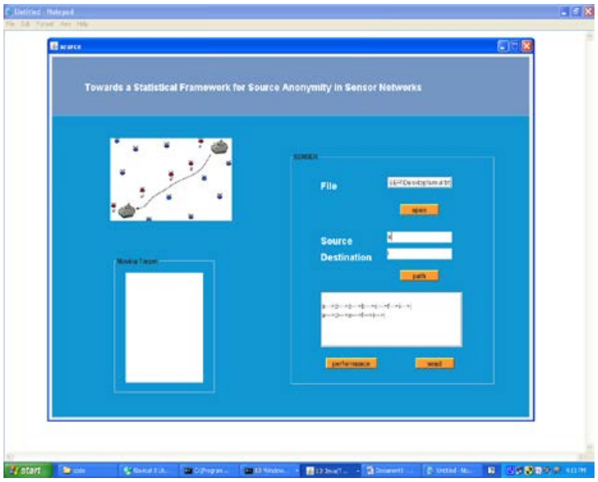
6.3 Main netwok and enter path values



Towards a Statistical Framework for Source Anonymity

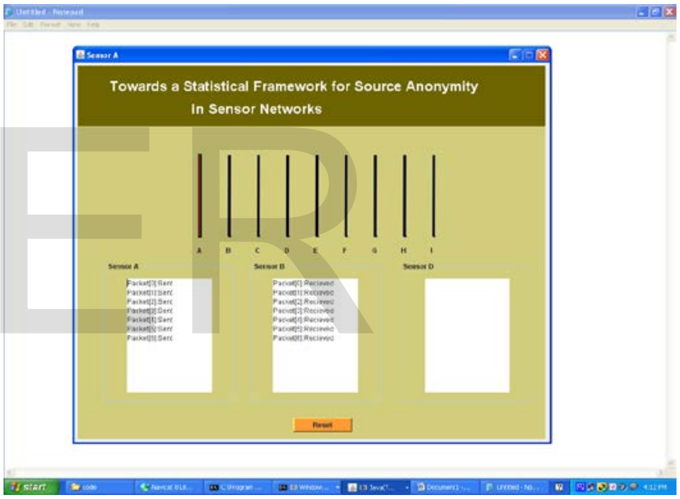
A - B: 1
E - F: 4
A - D: 7
D - G: 1
B - C: 2
G - H: 5
B - E: 8
E - H: 2
D - E: 3
H - I: 6
C - F: 9
F - I: 3

6.4 choose text file and generate fake messagecan send



Towards a Statistical Framework for Source Anonymity in Sensor Networks

6.5 packet moved from node A to node B

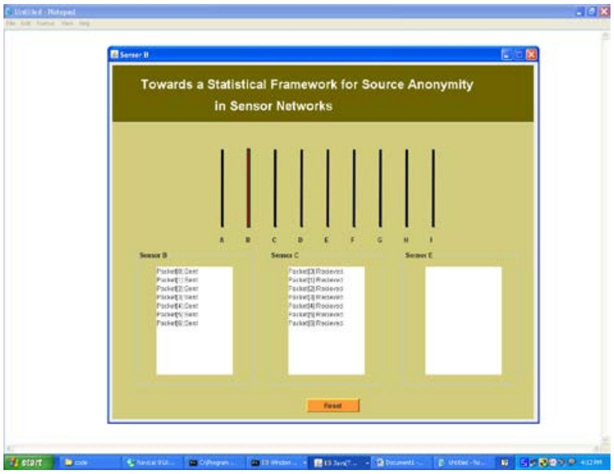


Towards a Statistical Framework for Source Anonymity in Sensor Networks

Sensor A:
Packet[0]:Sent
Packet[1]:Sent
Packet[2]:Sent
Packet[3]:Sent
Packet[4]:Sent
Packet[5]:Sent
Packet[6]:Sent

Sensor B:
Packet[0]:Recieved
Packet[1]:Recieved
Packet[2]:Recieved
Packet[3]:Recieved
Packet[4]:Recieved
Packet[5]:Recieved
Packet[6]:Recieved

6.6 node B to node c

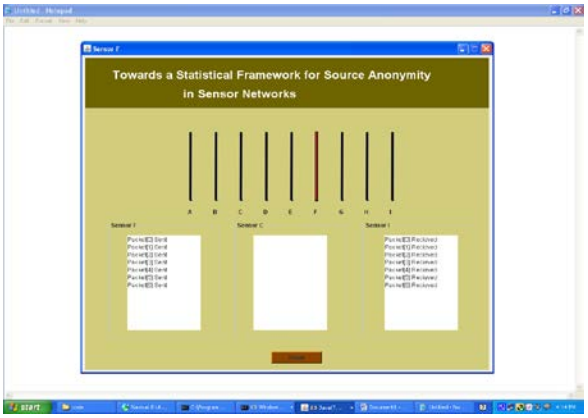


Towards a Statistical Framework for Source Anonymity in Sensor Networks

Sensor B:
Packet[0]:Sent
Packet[1]:Sent
Packet[2]:Sent
Packet[3]:Sent
Packet[4]:Sent
Packet[5]:Sent
Packet[6]:Sent

Sensor C:
Packet[0]:Recieved
Packet[1]:Recieved
Packet[2]:Recieved
Packet[3]:Recieved
Packet[4]:Recieved
Packet[5]:Recieved
Packet[6]:Recieved

### 6.7 Node C to Node F


Untitled - Notepad

Sensor F

Towards a Statistical Framework for Source Anonymity in Sensor Networks

Sensor F

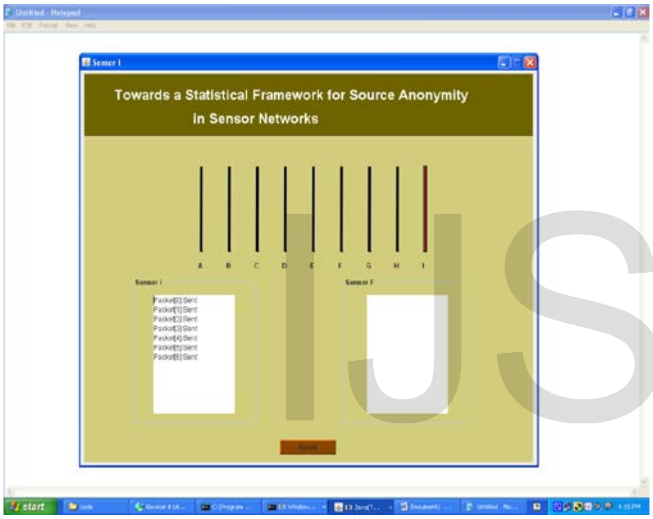
Packet[0] Sent
Packet[1] Sent
Packet[2] Sent
Packet[3] Sent
Packet[4] Sent
Packet[5] Sent
Packet[6] Sent

Sensor C

Sensor I

Packet[0] Received
Packet[1] Received
Packet[2] Received
Packet[3] Received
Packet[4] Received
Packet[5] Received
Packet[6] Received

### 6.8 Node F to Node I


Untitled - Notepad

Sensor I

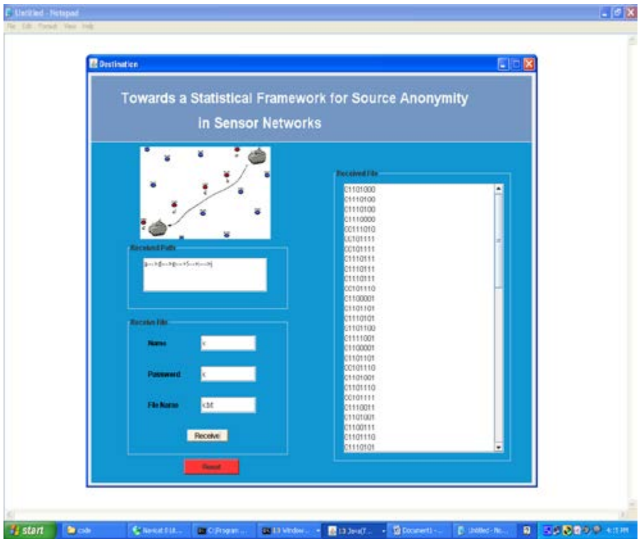
Towards a Statistical Framework for Source Anonymity in Sensor Networks

Sensor I

Packet[0]:Sent
Packet[1]:Sent
Packet[2]:Sent
Packet[3]:Sent
Packet[4]:Sent
Packet[5]:Sent
Packet[6]:Sent

Sensor F

### 6.9 Destination and binary code


Untitled - Notepad

Destination

Towards a Statistical Framework for Source Anonymity in Sensor Networks

Received Path

Receive File

Name: c

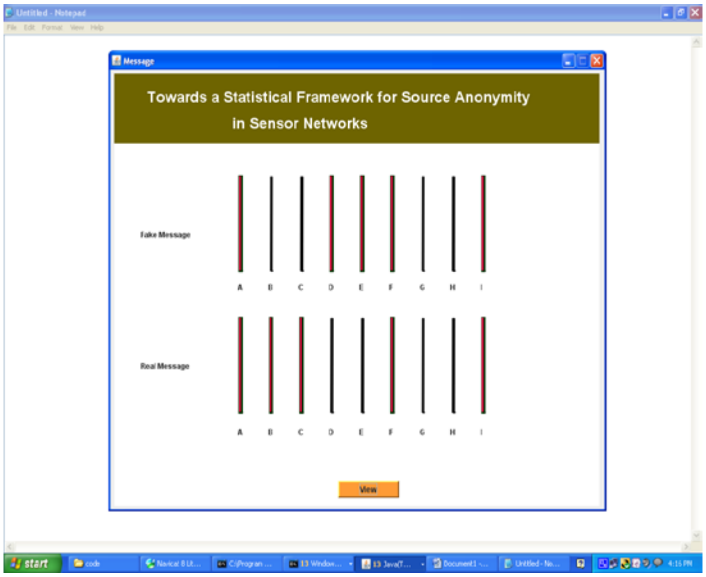
Password: c

File Name: c.txt

Received File

```
01101000
01110100
01110100
01110000
00111010
00101111
00101111
01110111
01110111
01110111
00101110
01100001
01101101
01110101
01101100
01111001
01100001
01101101
00101110
01101001
01101110
00101111
01110011
01101001
01100111
01101110
01110101
```

### 6.10 To view real message and Fake message


Untitled - Notepad

Message

Towards a Statistical Framework for Source Anonymity in Sensor Networks

## VII CONCLUSION

In this paper, we provided a statistical framework based on binary hypothesis testing for modeling, analyzing, and evaluating statistical source anonymity in wireless sensor networks. We introduced the notion of interval indistinguishability to model source location privacy. We showed that the current approaches for designing statistically anonymous systems introduce correlation in real intervals while fake intervals are uncorrelated. By mapping the problem of detecting source information to the statistical problem of binary hypothesis testing with nuisance parameters, we showed why previous studies were unable to detect the source of information leakage that was demonstrated in this paper. Finally, we proposed a modification to existing solutions to improve their anonymity against correlation tests. Future extensions to this work include mapping the problem of statistical source anonymity to coding theory in order to design an efficient system that satisfies the notion of interval indistinguishability.

## VIII REFERENCE

1.Towards a Statistical Framework for Source Anonymity in Sensor Networks Basel Alomair_, Andrew Clark_, Jorge Cuellary, and Radha Poovendran__Network Security Lab (NSL),University of Washington, Seattle, Washington Siemens

Corporate Technology, M¨unchen, Germany Email: falomair,awclark,rp3g@uw.edu, jorge.cuellar@siemens.com.

2.B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, “On Source Anonymity in Wireless Sensor Networks,” in oceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks–DSN’10. IEEE Computer Society, 2010, (Fast Abstract).

3.“Statistical Framework for Source Anonymity in Sensor Networks,” in Proceedings of the 53rd IEEE Global Communications Conference–GLOBECOM’10. IEEE Communications Society, 2010.

4.Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer networks, vol. 38, no. 4, pp. 393–422, 2002.

5.T. Arampatzis, J. Lygeros, and S. Manesis, “A survey of applications of wireless sensors and wireless sensor networks,” in Proceedings of the 13th IEEE Mediterranean Conference on Control and Automation – MED’05. IEEE Control System Society, 2006.