Minimizing energy utilization and source anonymity in wireless Sensor Networks
1N.Eswara Reddy 2D.Vijay
1,2Dept. of CSE, Pydah College of Engineering, Patavala, Yanam Road,E.g.dt,AP, India

ABSTRACT:
Monitoring networks consist of energy unnatural nodes that are expected to function over an extended period of time making energy competent monitoring a chief feature for unattended networks. In such situation nodes are designed to transmit information only when a appropriate event is detected i.e. event-triggered transmission. As a result given the location of an event-triggered node the location of a real event reported by the node can be approximated within the node’s sensing range. The places of the combat vehicle at different time intervals can be exposed to an opponent observing nodes transmissions. There are three limitations that can be connected with an event detected and reported by a sensor node as the description of the event, the time of the event and the location of the event. When sensor networks are organized in untrustworthy environments protecting the privacy of the three parameters that can be attributed to an event triggered transmission turn out to be an important security feature in the design of wireless sensor networks.

KEYWORDS: Wireless sensor networks (WSN), source location, privacy, anonymity, hypothesis testing, nuisance parameters, coding theory.

INTRODUCTION:
Encrypting a message before transmission for illustration can conceal the circumstance of the message from unauthorized observers but the simple existence of the cipher text is suggestive of information transmission. Unauthorized observers must be not capable to detect the origin of such events by analyzing the network traffic known as the source anonymity problem. This problem has appeared as an important topic in the security of wireless sensor networks with diversity of techniques based on different adversarial assumptions being proposed. In this work we present a new framework for modelling, analyzing and evaluating anonymity in sensor networks. The innovation of the proposed framework is twofold. First it introduces the notion of interval indistinguishability and provides a quantitative measure to model anonymity in wireless sensor networks. Second it maps source anonymity to the statistical problem of binary suggestion testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model. We show how mapping source vagueness to binary hypothesis testing with nuisance parameters leads to converting the difficulty of exposing private source information into searching for an suitable data transformation that removes or reduce the effect of the nuisance information. By doing so we change the difficulty from analyzing real-value sample points to binary codes which opens the door for coding theory to be integrated into the study of anonymous sensor networks.

RELATED WORK:
The source location isolation in sensor networks is part of a broader area the design of anonymous communication systems. The foundation for this field was laid by Chaum and since then has turn out to be a very active area of research. In particular topics related to location anonymity have been discussed by Reed et al. who bring in the idea of conserve anonymity through onion routing and by Gruteser and Growald who discussed ways to provide anonymity in location-based services such as Global Positioning Systems. In wireless sensor networks much of the work in source location privacy assumes a inactive local eavesdropper operating close to the base station. Privacy is maintained in such models through anonymous routing. The local eavesdropper model was introduced and the authors established that existing routing methods were deficient to provide location privacy in this environment. They also proposed a phantom flooding scheme to solve the problem.

EXISTING METHOD:
While transmitting the description of an intelligence event in a private manner can be achieved via encryption primitives hiding the timing and spatial information of reported events
cannot be achieved via cryptographic means. Encrypting a message before transmission for example can hide the context of the message from unauthorized observers but the mere existence of the cipher text is indicative of information transmission. In the existing literature the source vagueness problem has been addressed under two different types of adversaries’ namely local and global adversaries. A local adversary is defined to be an adversary having limited mobility and partial view of the network traffic. Routing based techniques have been shown to be effective in hiding the locations of reported events against local adversaries. A global adversary is defined to be an adversary with ability to monitor the traffic of the entire network. Against global adversaries routing based techniques are known to be unproductive in hiding location information in event-triggered transmission. This is due to the fact that since a global adversary has full spatial view of the network it can immediately detect the origin and time of the event-triggered transmission.

**DISADVANTAGES:**
The source anonymity problem in wireless sensor networks is the trouble of studying techniques that provide time and location privacy for events reported by sensor nodes. Time and location privacy will be used interchangeably with source anonymity all through the paper. The source anonymity problem has been drawing increasing research concentration recently.

**PROPOSED METHOD:**
We examine the difficulty of statistical source anonymity in wireless sensor networks. We bring in the notion of interval indistinguishability and demonstrate how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability. We propose a quantitative measure to estimate statistical source anonymity in sensor networks. We map the problem of violating source anonymity to the statistical trouble of binary hypothesis testing with nuisance parameters. We exhibit the significance of mapping the problem in hand to a well-studied problem in uncovering hidden vulnerabilities. In particular realizing that the SSA problem can be mapped to the hypothesis testing with nuisance parameters involves that breaching source anonymity can be transformed to finding an suitable data transformation that removes the nuisance information. By finding a transformation of observed data we change the problem from analyzing real-valued examples to binary codes and recognizes a possible anonymity breach in the current solutions for the SSA problem.

**ADVANTAGES:**
Removes or minimize the effect of the nuisance information.

**SENSOR NETWORK ARCHITECTURE:**

**SOURCE ANONYMITY:**
We initiate the concept of interval indistinguishability and demonstrate how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability. We propose a quantitative measure to calculate statistical source anonymity in sensor networks.

**CODING THEORY:**
We analyze existing solutions under the proposed model. By finding a alteration of observed data we adapt the problem from analyzing real-valued samples to binary codes and make out a possible anonymity breach in the current solutions for the SSA problem.

**NUISANCE PARAMETERS:**
In statistical decision theory the term nuisance parameters refers to information that is not essential for hypothesis testing and additionally can rule out a more precise decision making. When performing hypothesis testing of data with nuisance parameters it is needed even necessary in some scenarios to find a suitable transformation of the data that take away or diminish the effect of the nuisance information.

**HYPOTHESIS TESTING:**
In binary hypothesis testing given two hypothesis H0 and H1 and a data trial that fit in to one of the two hypotheses e.g. a bit transmitted through a noisy communication channel and the objective is to make a decision 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 false or real i.e. consists of fake transmissions only or contains real transmissions.

**ALGORITHM USED:**

```plaintext
INPUT: location information L and time information T
OUTPUT: accept the hypothesis $H_0$ or $H_1$

1. if $\mathbf{P}(\mathbf{L}_0) = \mathbf{P}(\mathbf{L}_1)$:
   - compute $T_0(t)$ and $T_1(t)$
   - compute speed $v$ from $\mathbf{L}_0$ and $\mathbf{L}_1$
   - if $v = \mathbf{V}_{\text{ref}}$ then:
     - $w = 0$
   - else:
     - if $v > T_0(t)$ then:
       - Accept the hypothesis $H_0$ and terminate the test
     - else:
       - if $v > T_1(t)$ then:
         - initialize $w$ to 0 and accepts the hypothesis $H_1$
       - end if
     - end if
   - end if

2. if $w = 1$:
   - $\mathbf{P}(\mathbf{L}_0) = \mathbf{P}(\mathbf{L}_1)$
   - $\mathbf{P}(\mathbf{L}_0) = \mathbf{P}(\mathbf{L}_1)$
```

**ERROR RATE OF PROPOSED METHOD:**

![Graph showing error rate for proposed system](image)

**CONCLUSION:**

We afford a statistical framework based on binary hypothesis testing for modelling, analyzing and calculating statistical source anonymity in wireless sensor networks. We introduced the idea of interval indistinguishability to model source location privacy. We showed that the current approaches for designing statistically anonymous systems bring in correlation in real intervals while false 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 escape that was demonstrated in this paper. Finally we proposed a alteration to existing solutions to get better their anonymity against correlation tests. Future extensions to this work include mapping the difficulty of statistical source anonymity to coding theory in order to plan an competent system that convince the concept of interval indistinguishability.

**REFERENCES:**


Mr. N. Eswara Reddy is a student of Pydah College of Engineering, Patavala. Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his B.Tech from Kakinada Institute of Technology, affiliated to JNT University, Kakinada in the year 2011. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. D. Vijay, well known Author and excellent teacher Received M.Tech (CSE) from Pragati Engineering College is working as Assistant Professor, Department of M.Tech Computer science engineering, Pydah College of Engineering. He is an active member of ISTE. He has 3 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences/journals. His area of Interest includes Information security, Computer Networks and other advances in computer Applications.