SSUT: A new approach for privacy of source unknown in wireless sensor networks

Geddada Rajakumari, Chinnam Yuvaraju
Dept. Of Cse, Sir Sai Madhavi Institute Of Engineering & Technology, Mallampudi - 533 296, Rajanagaram Mandal, Near Rajahmundry, East Godavari District, Andhra Pradesh, India

Abstract: Sensor Networks which is different compared to other networks which is deployed in unattended area used to sense and monitor the events that are reported to sink. But the locations of events delivered by sensor networks needs to remain unknown. Unauthorized parties revealing source of events by analyzing network traffic.in order to overcome this problem I present new Framework with two effective components.one component is quantitative measure evaluate source unknown in sensor networks. Second one is binary hypothesis testing with nuisance parameters. Finally our proposed technique is effective providing privacy to source in sensor networks.

1. Introduction

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following two ways:

Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required. Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused.

Sensor networks are deployed to sense, monitor, and report events of interest in a wide range of applications including, but are not limited to, military, health care, and animal tracking. In many applications, such monitoring networks consist of energy constrained nodes that are expected to operate over an extended period of time, making energy efficient monitoring an important feature for unattended networks. In such scenarios, nodes are designed to transmit information only when a relevant event is detected (i.e., event-triggered transmission). Consequently, 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. In the example depicted in Figure 1, the locations of the combat vehicle at different time intervals can be revealed to an adversary observing nodes transmissions. There are three parameters that can be associated with an event detected and reported by a sensor node: the description of the event, the time of the event, and the location of the event. When sensor networks are deployed in untrustworthy environments, protecting the privacy of the three parameters that can be attributed to an event-triggered transmission becomes an important security feature in the design of wireless sensor networks.

While transmitting the “description” of a sensed 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 instance, can hide the context of the message from unauthorized observers, but the mere existence of the ciphertext is indicative of information transmission. The source anonymity problem in wireless sensor networks is the problem of studying techniques that provide time and location privacy for events reported by sensor nodes. The source anonymity problem has been drawing increasing research attention recently.

In the existing literature, the source anonymity 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 (e.g., coordinating adversaries spatially distributed over the network). Against global adversaries, routing-based techniques are known to be ineffective in concealing 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.
The first step towards achieving source anonymity for sensor networks in the presence of global adversaries is to refrain from event-triggered transmissions. To do that, nodes are required to transmit fake messages even if there is no detection of events of interest. When a real event occurs, its report can be embedded within the transmissions of fake messages. Thus, given an individual transmission, an observer cannot determine whether it is fake or real with a probability significantly higher than 1/2, assuming messages are encrypted.

In the above approach, there is an implicit assumption of the use of a probabilistic distribution to schedule the transmission of fake messages. However, the arrival distribution of real events is, in general, time-variant and unknown a priori. If nodes report real events as soon as they are detected (independently of the distribution of fake transmissions), given the knowledge of the fake transmission distribution, statistical analysis can be used to identify outliers (real transmissions) with a probability higher than 1/2.

One way to mitigate the above statistical analysis is illustrated. As opposed to transmitting real events as they occur, they can be transmitted instead of the next scheduled fake one. For example, consider programming sensor nodes to deterministically transmit a fake message every minute. If a real event occurs within a minute from the last transmission, its report must be delayed until exactly one minute has elapsed. This approach, however, introduces additional delay before a real event is reported (in the above example, the average delay of transmitting real events is half a minute). When real events have time-sensitive information, such delays might be unacceptable. Reducing the delay of transmitting real events by adopting a more frequent scheduling algorithm is impractical for most sensor network applications since sensor nodes are battery powered and, in many applications, unchargeable. Therefore, a frequent transmission scheduling would drastically reduce the desired lifetime of the sensor network. Practical SSA solutions need to be designed to achieve their objective under two main constraints: minimizing delay and maximizing the lifetime of sensors’ batteries.

2. Related Work

In wireless sensor networks, much of the work in source location privacy assumes a passive, local eavesdropper operating close to the base station. Privacy is maintained in such models through anonymous routing. The location privacy problem was first introduced. The local eavesdropper model was introduced and the authors demonstrated that existing routing methods were insufficient to provide location privacy in this environment. They also proposed a phantom flooding scheme to solve the problem. In Xi et al. proposed a new random walk routing method that reduces energy consumption at the cost of increased delivery time. Path confusion has also been proposed as an anonymity-preserving routing scheme by Hoh and Gruteser. In Ouyang et al. developed a scheme in which cycles are introduced at various points in the route, potentially trapping the adversary in a loop and forcing the adversary to waste extra resources. In Wang et al. proposed a technique to maximize source location privacy by designing routing protocols that distribute message flows to different routes.

Literature Survey

Sensor networks bear a promising future in many important applications such as habitat monitoring, military surveillance, and target tracking. However, sensor networks are also confronted with many security threats such as node compromise, routing disruption and false data injection, because they normally operate in unattended, harsh or hostile environment. Among all these threats, privacy is of special interest to us since it cannot be fully addressed by traditional security mechanisms, such as encryption and authentication. Consider a simple example of event reporting in a sensor network. When a sensor detects an event, it sends a message including event-related information to the base station. After this, the location of the event source has actually been leaked to the attacker (who may be passively monitoring the network), no matter how strong the data encryption key is. Furthermore, an attacker may find out more sensitive information: whether, when and where a particular event occurred, e.g., the appearing of an endangered animal in an asset monitoring sensor network. This can help the attacker in capturing the animal, an unfortunate occurrence.

In it was shown that routing-based techniques, although can provide source anonymity against local adversaries (those monitoring parts of the network), leak source information to global adversaries (those able to monitor the traffic of the entire network). To protect against such adversaries, nodes are programmed to transmit fake messages even if there are no real events to be reported, so that real transmissions can be embedded within the fake ones [1]. Scheduling fake transmissions according to a certain probabilistic distribution, however, gives adversaries the opportunity to distinguish between real and fake transmissions via statistical analysis, if real events are transmitted as they arrive.

3. Existing System

While transmitting the description of a sensed 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 techniques.

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 ineffective in concealing location information in event-triggered transmission
4. 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. 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 generate 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.

6. System Architecture

We analyze existing solutions under the proposed model. By finding a transformation of observed data, we 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.

3. Nuisance Parameters

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.

4. Hypothesis Testing

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).

7. 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.
References


Ms. Rajakumari Geddada is a student of SRI SAI MADHAVI INSTITUTE of Engineering & Technology, Rajahmundry. Presently she is pursuing her M.Tech [Computer Engineering] from this college and she received her B.Tech from Avanthi Institute of Engineering and Technology, affiliated to JNT University, Hyderabad in the year 2005. Her area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. Yuvaraju Chinnam is an associate professor of Sri Sai Madhavi institute of Science and Technology. He received M.Tech (Remote Sensing and GIS) from Centre for Spatial Information Technology, JNTU, Hyderabad in the year 2007 and He received B.Tech (Computer Science and Engineering) from Gudlavalleru Engineering College affiliated to JNTUH in the year 2003. His areas of interests are Computer Networks, Disaster Management, Image Processing, Remote Sensing, Health-GIS.