ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Toward a statistical framework for source anonymity in sensor networks

[1]N.ZahiraJahan [2]K.Priyatharshini
[1] Associate Professor, Department Of M.C.A
[2]PG Scholar, Dept of MCA,
Nandha Engineering College, Erode.
Priyatharshini199513@gmail.com

Abstract—In certain applications, the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modeling, analyzing, and evaluating anonymity in sensor networks. The novelty 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 hypothesis testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model. We 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. By doing so, we transform the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be incorporated into the study of anonymous sensor networks. Finally, we discuss how existing solutions can be modified to improve their anonymity.

1. INTRODUCTION

1.1 SENSOR NETWORKS

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 Fig. 1.1, 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.

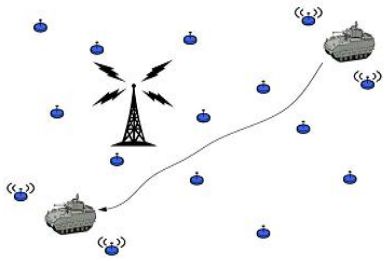

Figure 1.1 A sensor network deployed in a battlefield. Only nodes in close proximity to the combat vehicle are broadcasting information, while other nodes are in sleep mode.

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

.

1.2 SOURCE ANONYMITY PROBLEM

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.

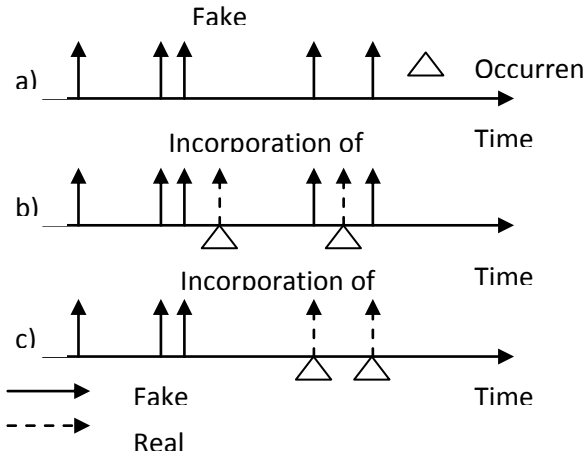

Figure 1.2. Different approaches for embedding the report of real events within a series of fake transmissions; (a) shows the prespecified distribution of fake transmissions, (b) illustrates how real events are transmitted as soon as they are detected, (c) illustrates how nodes report real events instead of the next scheduled fake message.

1.3 PROBABILISTIC DISTRIBUTION

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, as illustrated in Fig. 2b. In other words, transmitting real events as soon as they are detected does not provide source anonymity against statistical adversaries analyzing a series of fake and real transmissions.

One way to mitigate the above statistical analysis is illustrated in Fig. 2c. 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 1 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 will drastically reduce the desired lifetime of the sensor network.

1.4 MAIN CONTRIBUTIONS

The main contributions of this thesis are.

The notion of “interval indistinguishability” is introduced and illustrated how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability.

A quantitative measure is proposed to evaluate statistical source anonymity in sensor networks.

The problem of breaching source anonymity is mapped to the statistical problem of binary hypothesis testing with nuisance parameters. The significance of mapping the problem is demonstrated 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 implies that breaching source anonymity can be converted to finding an appropriate data transformation that removes the nuisance information.

Existing solutions under the proposed model is analysed. By finding a transformation of observed data, the problem is converted from analyzing real-valued samples to binary codes and a possible anonymity breach is identified in the current solutions for the SSA problem.

2.LITERATURE REVIEW

2.1 ON SOURCE ANONYMITY IN WIRELESS SENSOR NETWORKS

In the paper[1], the authors Basel Alomair, Andrew Clark, Jorge Cuellary, and Radha Poovendran were stated that the Preserving source location privacy is becoming one of the most interesting problems in wireless sensor networks. In a variety of real life applications, such as the deployment of sensor nodes in battlefields, the locations of events mon-itored by the network are required to remain anonymous. Given the knowledge of the network topology, however, an adversary can expose the locations of such events by determining the individual nodes reporting them.

When source location privacy is of critical importance, special attention must be paid to the design of the node transmission algorithm so that monitoring sensor nodes does not reveal private source information. One of the ma-jor challenges for the source anonymity problem is that it cannot be solved using traditional cryptographic primitives. Encrypting nodes' transmissions, for instance, can hide the contents of plaintext messages, but the mere existence of ciphertexts is indicative of information transmission.

2.2 STATISTICAL FRAMEWORK FOR SOURCE ANONYMITY IN SENSOR NETWORKS

In this paper [3], the authors Basel Alomair, Andrew Clark, Jorge Cuellary, and Radha Poovendran were stated that investigate the security of anonymous wireless sensor networks. To lay down the foundations of a formal framework, they proposed a new model for analyzing and evaluating anonymity in sensor networks. The novelty of the proposed model 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.

The significance of the proposed model is that it captures a source of information leakage that cannot be captured using existing models. By analyzing current anonymous designs under the proposed model, it expose the source of information leakage that is undetectable by existing models and quantify the anonymity of current designs. Finally, it show how the proposed model can lead to a general and intuitive direction for improving the anonymity of current designs.

In sensor networks, small devices (called sensor nodes) are employed to capture relevant events and report collected data. The type of events nodes are designed to capture and report is an application dependent. Applications where sensor nodes can be utilized range from taking patients' vital signs in controlled indoor environments to collecting tactical military information in hostile war zones.

2.3 SPINS: SECURITY PROTOCOLS FOR SENSOR NETWORKS

In this paper [13], the authors Adrian Perrig, Robert Szewczyk, j.d. Tygar, Victor Wen and David e. culler were stated that wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. They present a suite of security protocols optimized for sensor networks: SPINS.

SPINS has two secure building blocks: SNEP and TESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. TESLA provides authenticated broadcast for severely resource-constrained environments. To implemented the above protocols, and show that they are practical even on minimal hardware: the performance of the protocol suite easily matches the data rate of the network. Additionally, it demonstrated that the suite can be used for building higher level protocols.

3.EFFECT OF NETWORK TOPOLOGY ON SOURCE ANONYMITY

So far, anonymity discussions were restricted to single-hop analysis. However, since the adversary, by assumption, has a global view of the network, the adversary can utilize his/ her knowledge of the network's topology to increase the advantage of exposing secret location information. In this section, we bring the network's topology into the picture to illustrate the importance of increasing the anonymity of each node.

Assume the network is deployed to monitor a moving target. Assume further that a global adversary will have a 55 percent chance of distinguishing between real and fake intervals. In some scenarios, a 0.45 probability of false alarm (the probability that the adversary has concluded a certain interval is real while it is fake) can be

considered high enough to prevent the adversary from taking the risk. Since the adversary has a global view of the network, however, he/she can correlate the analysis to the next hop by monitoring adjacent sensor nodes.

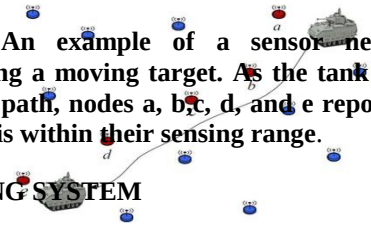

Fig. 5. An example of a sensor networks monitoring a moving target. As the tank moves along its path, nodes a, b, c, d, and e report that the tank is within their sensing range.

EXISTING SYSTEM

The existing system introduces the notion of "interval indistinguishability" and illustrates how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability. It proposes a quantitative measure to evaluate statistical source anonymity in sensor networks.

By introducing real and fake interval concept, the messages are differentiated by the proper observer. The unauthorized observer fails in distinguishing the messages and failed to find the node location.

DRAWBACKS OF EXISTING SYSTEM

Replica attack made by closest nodes cannot be identified. Extra messages need to be communicated between sender and observer nodes .Nodes awakening time is more.

PROPOSED SYSTEM

The proposed system work is motivated from mitigating the limitations of previous schemes. In particular, the new system proposes a reputation-based trust management scheme that is designed to facilitate fast detection and revocation of compromised nodes. The key idea of our scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised. Specifically, it first divides the network into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Sequential Probability Ratio Test (SPRT).

The SPRT decides a zone to be untrustworthy if the zone's trust is continuously maintained at low level or is quite often changed from high level to low level. Once a zone is determined to be untrustworthy, the base station or the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them.In addition, a novel mobile replica detection scheme is proposed based on the Sequential Probability Ratio Test (SPRT). The new system uses the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed.

As a result, a benign mobile sensor node's measured speed will nearly always be less than the system-configured maximum speed as long as it employs a speed measurement system with a low error rate. On the other hand, replica nodes are in two or more places at the same time. This makes it appear as if the replicated node is moving much faster than any of the benign nodes, and thus the replica nodes' measured speeds will often be over the system-configured maximum speed.

ADVANTAGES OF PROPOSED SYSTEM

The main benefit of this zone-based detection approach lies in achieving fast node compromise detection and revocation while saving the large amount of time and effort that would be incurred from using periodic software attestation.
By detecting an entire zone at once, the system can identify the approximate source of bad behavior and react quickly, rather than waiting for a specific node to be identified.

When multiple nodes are compromised in one zone, they can all be detected and revoked at one time. The proposed system validates the effectiveness, efficiency, and robustness of the scheme through analysis and simulation experiments.

The new system finds that the main attack against the SPRT-based scheme is when replica nodes fail to provide signed location and time information for speed measurement.

To overcome this attack, the new system employs a quarantine defense technique to block the noncompliant nodes.

It provides analyses of the number of speed measurements needed to make replica detection decisions, which shows is quite low, and the amount of overhead incurred by running the protocol.

CONCLUSION AND FUTURE WORK

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 demon-strated 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.

REFERENCE

[1] B. ALOMAIR, A. CLARK, J. CUELLAR, AND R. POOVENDRAN, "ON SOURCE ANONYMITY IN WIRELESS SENSOR NETWORKS," PROC. IEEE/IFIP 40TH INT'L CONF. DEPENDABLE SYSTEMS AND NETWORKS (DSN '10), 2010.

[2] K. MEHTA, D. LIU, AND M. WRIGHT, "LOCATION PRIVACY IN SENSOR NETWORKS AGAINST A GLOBAL EAVESDROPPER," IN ICNP 2007. IEEE INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS. , 2007.

[3] B. ALOMAIR, A. CLARK, J. CUELLAR, AND R. POOVENDRAN, "STATISTICAL FRAMEWORK FOR SOURCE ANONYMITY IN SENSOR NETWORKS," PROC. IEEE GLOBECOM, 2010.

[4] P. KAMAT, Y. ZHANG, W. TRAPPE, AND C. OZTURK, "ENHANC-ING SOURCE-LOCATION PRIVACY IN SENSOR NETWORK ROUTING," ICDCS 2005. THE 25TH IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS.

[5] C. OZTURK, Y. ZHANG, AND W. TRAPPE, "SOURCE-LOCATION PRIVACY IN ENERGY-CONSTRAINED SENSOR NETWORK ROUTING," IN PROCEEDINGS OF THE 2ND ACM WORKSHOP ON SECURITY OF AD HOC AND SENSOR NETWORKS, 2004.

[6] Y. XI, L. SCHWIEBERT, AND W. SHI, "PRESERVING SOURCE LOCATION PRIVACY IN MONITORING-BASED WIRELESS SENSOR NET-WORKS," IN IPDPS 2006. THE 20TH INTERNATIONAL PARALLEL AND DISTRIBUTED PROCESSING SYMPOSIUM, 2006.

[7] B. HOH AND M. GRUTESER, "PROTECTING LOCATION PRIVACY THROUGH PATH CONFUSION," IN SECURECOMM 2005. FIRST INTER-NATIONAL CONFERENCE ON SECURITY AND PRIVACY FOR EMERGING AREAS IN COMMUNICATIONS NETWORKS., 2005.

[8] Y. OUYANG, Z. LE, G. CHEN, J. FORD, F. MAKEDON, AND U. LOWELL, "ENTRAPPING ADVERSARIES FOR SOURCE PROTECTION IN SENSOR NETWORKS," IN PROCEEDINGS OF THE 2006 IEEE INTERNATIONAL SYMPOSIUM ON WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS, 2006.