Toward a Statistical Framework for Source Anonymity in Sensor Networks

Basel Alomair, *Member*, *IEEE*, Andrew Clark, *Student Member*, *IEEE*, Jorge Cuellar, and Radha Poovendran, *Senior Member*, *IEEE*

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.

Index Terms—Wireless sensor networks (WSN), source location, privacy, anonymity, hypothesis testing, nuisance parameters, coding theory

1 Introduction

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 [3], [4], [5]. 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, 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 [6], [7], [8], [9], hiding the timing and spatial information of reported events cannot be achieved via cryptographic means [10], [11]. 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. (Time and location privacy will be used interchangeably with source anonymity throughout the paper.) The source anonymity problem has been drawing increasing research attention recently [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20].

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 [12], [13], [14], [15], [16]. 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

- *B. Alomair is with the Computer Research Institute (CRI), King Abdulaziz City for Science and Technology (KACST), PO Box 6086, Riyadh 11442, Saudi Arabia. E-mail: alomair@uw.edu.*
- *A. Clark and R. Poovendran are with the Network Security Lab (NSL), Department of Electrical Engineering, University of Washington, Campus Box 352500, Seattle, WA 98195-2500. E-mail: {awclark, rp3}@uw.edu.*
- *J. Cuellar is with Corporate Research and Technologies, CT T DE IT1, CERT, Otto-Hahn-Ring 6, 81739 Munich, Germany. E-mail: jorge.cuellar@siemens.com.*

Manuscript received 10 Dec. 2010; revised 3 Sept. 2011; accepted 23 Nov. 2011; published online 13 Dec. 2011.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2010-12-0561. Digital Object Identifier no. 10.1109/TMC.2010.267.

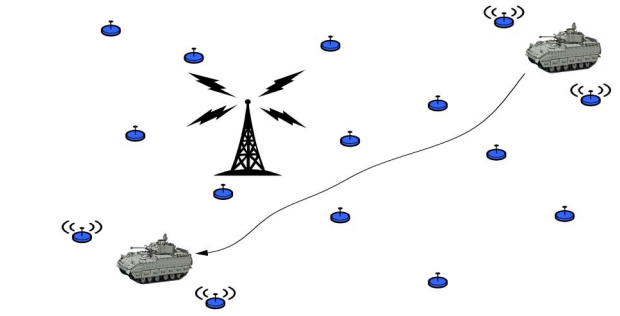

Fig. 1. A sensor network deployed in a battlefield. Only nodes in close proximity to the combat vehicle are broadcasting information, while other nodes are in sleep mode.

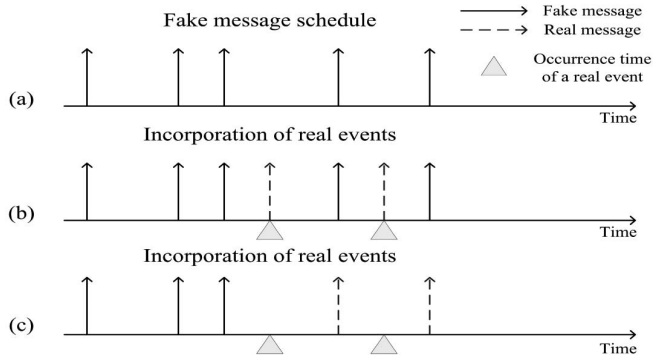

Fig. 2. Different approaches for embedding the report of real events within a series of fake transmissions; (a) shows the prespecified distribution of fake transmissions, (b) illustrates how real events are transmitted as soon as they are detected, (c) illustrates how nodes report real events instead of the next scheduled fake message.

view of the network, it can immediately detect the origin and time of the event-triggered transmission.

The first step toward achieving source anonymity for sensor networks in the presence of global adversaries is to refrain from event-triggered transmissions [10]. To do that, nodes are required to transmit *fake messages* even if there is no detection of events of interest (*real events* will be used to denote events of interest for the rest of the paper). 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 $1/2$, 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.

The Statistical Source Anonymity (SSA) problem in sensor networks is the study of techniques that prevent global adversaries from exposing source location by performing statistical analysis on nodes transmissions [11], [19], [20], [21], [22], [23], [24]. Practical SSA solutions need to be designed to achieve their objective under two main constraints: minimizing delay and maximizing the lifetime of sensors' batteries.

Our Contribution. In this paper, we investigate the problem of statistical source anonymity in wireless sensor networks. The main contributions of this paper can be summarized by the following points.

- We introduce the notion of "interval indistinguishability" and illustrate how the problem of statistical source anonymity can be mapped to the problem of interval indistinguishability.
- We propose a quantitative measure to evaluate statistical source anonymity in sensor networks.
- We map the problem of breaching source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters.
- We demonstrate 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 implies that breaching source anonymity can be converted to finding an appropriate data transformation that removes the nuisance information.
- 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.
- We pose and answer the important research question of why previous studies were unable to detect the possible anonymity breach identified in this paper.
- We discuss, by looking at the problem as a coding problem, a new direction to enhance the anonymity of existing SSA solutions.

Organization. The rest of the paper is organized as follows: In Section 2, we describe our network and adversarial assumptions. In Section 3, we describe the proposed framework. In Section 4, we describe the notion of statistical

goodness of fit tests and study its use in designing SSA solutions. In Section 5, we provide experimental analysis of statistical goodness of fit test-based approaches and quantify their anonymity. In Section 6, we demonstrate the importance of converting the SSA problem into binary codes for uncovering the hidden vulnerabilities missed by previous studies. In Section 8, we extend the source anonymity problem in sensor networks to include the network topology into the anonymity analysis. In Section 9, we discuss related work and conclude the paper in Section 10.

2 Model Assumptions

In this section, we describe the network and adversarial assumption that will be used in this paper.

2.1 Network Model

Communication is assumed to take place in a network of energy constrained sensor nodes. Nodes are deployed to sense events of interest and report them with minimum delay. Consequently, given the location of a certain node, the location of the reported event of interest can be approximated within the node's communication range at the time of transmission. When a node senses an event, it places information about the event in a message and broadcast an encrypted version of the message. To obscure the report of an event of interest, nodes are assumed to broadcast fake messages, even if no event of interest has been detected. Nodes are also assumed to be equipped with a semantically secure encryption algorithm, so that adversaries are unable to distinguish between the reports of events of interest and the fake transmissions by means of cryptographic tests.[1] Furthermore, the network is assumed to be deployed in an unreachable environment and, therefore, the conservation of nodes' energy is a design requirement.

2.2 Adversarial Model

The adversarial model used in this paper is similar to the one considered in [10], [11], in that it is *external*, *passive*, and *global*. An external adversary is an adversary who does not control any of the nodes in the network. As opposed to active adversaries injecting their own traffic or jamming the network, a passive adversary is only capable of observing the network traffic. A global adversary is an adversary who can monitor the traffic of the entire network and can determine the node responsible for the initial transmission reporting an event of interest.

The justification behind this model is twofold. First, it serves as a worst case scenario, when the coverage area of the adversary is time varying and/or unknown. Second, it represents a network of collaborating adversaries that can cover the deployed sensor network.

The adversary is also assumed to know the distribution of fake message transmissions. Furthermore, the adversary is assumed capable of observing nodes transmissions over extended periods of times and performing sophisticated statistical analysis to compare the observed transmission with the known distribution of fake messages. The adversary, however, is not assumed able to break the security of the encryption algorithm and distinguish the report of event of interests via cryptographic tests.

1. In cryptography, semantic security implies that, given a ciphertext, unauthorized users without the knowledge of the decryption key have no means of distinguishing between two plaintexts in which one of them corresponds to the observed ciphertext [25].

3 Proposed Framework for SSA

In this section, we introduce our source anonymity model for wireless sensor networks. Intuitively, anonymity should be measured by the amount of information about the occurrence time and location of reported events an adversary can extract by monitoring the sensor network. The challenge, however, is to come up with an appropriate model that captures all possible sources of information leakage and a proper way of quantifying anonymity in different systems.

3.1 Interval Indistinguishability

Currently, statistical anonymity in sensor networks is modeled by the adversary's ability to distinguish between real and fake transmissions by means of statistical analysis. That is, given a series of transmissions of a certain node, the adversary must be unable to distinguish, with significant confidence, which transmission carries real information and which transmission is fake, regardless of the number of transmissions the adversary may observe.

Consider now an adversary observing a sensor network over multiple *time intervals*. Assume that, during a given time interval, the adversary is able to notice a change in the statistical behavior of transmission times of a certain node in the network. This distinguishable change in the transmission behavior of the node can be indicative of the existence of real activities detected and reported by that node during that interval, even if the adversary was unable to distinguish between individual transmissions.

Consequently, in many applications, modeling source anonymity in sensor networks by the adversary's ability to distinguish between *individual transmissions* is insufficient to guarantee location privacy. It must be the case that an adversary monitoring the network over multiple *time intervals*, in which some intervals contain real event transmissions and the others do not, is unable to determine, with significant confidence, which of the intervals contain the real traffic. Formally, the notion of interval indistinguishability can be defined as follows:

Definition 1 (Interval indistinguishability). *Let I_F denotes a time interval* without *any real event transmission (called the "fake interval" for the rest of the paper), and I_R denotes a time interval* with *real event transmissions (called the "real interval" for the rest of the paper). The two time intervals are said to be statistically indistinguishable if the distributions of intertransmission times during these two intervals cannot be distinguished with significant confidence.*

3.2 Interval versus Event Indistinguishability

This section illustrates the relation between the traditional anonymity notion (i.e., individual event indistinguishability) and the proposed anonymity notion (i.e., interval indistinguishability). First, observe that as the length of intervals decreases or the transmission rate is sparse,

interval indistinguishability approaches event indistinguishability. If each interval consists of a single transmission, interval indistinguishability is equivalent to event indistinguishability.

However, in the more general scenario, in which intervals contain more than a single transmission, interval indistinguishability implies indistinguishability of individual transmissions. To see this, assume a system satisfying interval indistinguishability but does not satisfy individual event indistinguishability. Since real and fake transmissions are distinguishable, given a fake interval and a real interval, the real interval can be identified as the one with the real transmission; a contradiction to the hypothesis that the system satisfies interval indistinguishability. That is, if intervals are indistinguishable, then individual events within them must also be indistinguishable.

In fact, the notion of interval indistinguishability is strictly stronger than the traditional notion individual event indistinguishability. That is, while interval indistinguishability implies individual indistinguishability, the converse is not true in general. This will be shown in Section 5 by demonstrating that there exist schemes that achieve high levels of individual indistinguishability while failing to achieving satisfactory levels of interval indistinguishability.

3.3 Mapping Statistical Source Anonymity to Binary Hypothesis Testing

In binary hypothesis testing, given two hypothesis, H_0 and H_1, 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 inter-transmission times, the goal is to decide whether the interval is fake or real (i.e., consists of fake transmissions only or contains real transmissions).

Given Definition 1 of interval indistinguishability, consider the following game between a challenger, $\mathcal{C}$ (the system designer), and a statistical adversary, $\mathcal{A}$.

Game 1 (Anonymity game).

1. *$\mathcal{C}$ chooses two intervals I_R and I_F, in which I_R is a real interval and I_F is a fake one.*
2. *$\mathcal{C}$ draws a bit $b \in \{0,1\}$ uniformly at random and sets $I_R = I_b$ and $I_F = I_{\bar{b}}$, where $\bar{b}$ denotes the binary complement of b.*
3. *$\mathcal{C}$ gives I_b and $I_{\bar{b}}$ to $\mathcal{A}$.*
4. *$\mathcal{A}$ makes any statistical test of her choice on I_b and $I_{\bar{b}}$ and outputs a bit b'.*
5. *If $b' = b$, $\mathcal{A}$ wins the game.*

Game 1 can be viewed as a standard binary hypothesis testing problem. That is, given two hypotheses (a real interval and a fake interval) and an observed data (an interval of inter-transmission times of a sensor node), the goal of the adversary is to determine to which hypothesis the observed data belong (i.e., whether the observed interval contains real event transmissions).

Remark 1. Although giving the adversary two intervals might seem too strong of an assumption, it is actually a practical one. To see this, note that the adversary can always observe multiple time intervals, two for instance. Then, all that is needed is to analyze these two observed intervals. If they are distinguishable, then it is likely that one of them is a real interval and the other is fake. Moreover, an adversary can discover the distribution of fake intervals by monitoring a node in the absence of real events. Then, all that is needed is to observe different time intervals. The more distinguishable a time interval from the known fake interval, the more likely it is to contain real events. Therefore, Game 1 is suitable to analyze practical systems.

3.4 Quantifying Statistical Source Anonymity

With Definition 1 and Game 1, we aim to find a security measure that can formally quantify the anonymity of different systems. Let σ denote any adversarial strategy for breaching the anonymity of the system. Let $\Pr[b' = b]_\sigma$ denote the adversary's probability of winning Game 1 using strategy σ. We quantify the anonymity of a sensor network against the strategy σ by

$$\Lambda_\sigma := 1 - 2(\Pr[b' = b]_\sigma - 0.5). \tag{1}$$

In the best case scenario, from the challenger's standpoint, the adversary's strategy is a pure random guess; leading to $\Pr[b' = b]_\sigma = 1/2$ and $\Lambda_\sigma = 1$ (absolute anonymity). In the worst case, the adversary will have a strategy with $\Pr[b' = b]_\sigma = 1$ leading to $\Lambda_\sigma = 0$ (no anonymity). Any intelligent strategy will result in a probability of winning the game belonging to the interval $[0.5, 1]$, leading to an anonymity measure in the interval $[0, 1]$ that is monotonically decreasing with the adversary's success probability.

Now, let Σ be the set of all possible adversarial strategies to breach the anonymity of the sensor network. Then, we define the anonymity of the system as:

$$\Lambda := \min_{\sigma \in \Sigma} \Lambda_\sigma, \tag{2}$$

where Λ_σ is as defined in (1).

With the above definition of interval indistinguishability, we introduce the notion of Λ-anonymity in sensor networks.

Definition 2 (Λ-anonymity). *A wireless sensor network is said to be Λ-anonymous if it satisfies two conditions*

1. *the anonymity of the system, as defined in (2), is at least Λ,*
2. *there is no distinguishable transitional behavior between intervals.*

The second condition in Definition 2 ensures that the adversary is unable to infer when an interval starts or when it ends. This is necessary since an adversary with the knowledge that a node is transitioning from one interval to another will infer that either real events have started to arrive or stopped from arriving. In either case, source anonymity can be breached. In Table 1, the terms and notations that will be used throughout the paper are listed.

4 Statistical Goodness of Fit Tests and the SSA Problem

In the literature, statistical source anonymity is shown to be achieved via the use of statistical goodness of fit tests [11],

TABLE 1
A List of Used Terms and Notations

SSA	Statistical Source Anonymity
$\boldsymbol{E_i}$	The random variable representing the type of event reported in the i^{th} transmission (either fake or real)
$\boldsymbol{X_i}$	The random variable representing the inter-transmission time between the i^{th} and the $i+1^{\text{st}}$ transmissions
μ	The desired mean of the $\boldsymbol{X_i}$'s
I_F	A fake interval: an interval consisting of fake events only
I_R	A real interval: an interval containing some real event transmissions
short inter-transmission times	Inter-transmission times that are shorter than the mean of the pre-defined distribution
long inter-transmission times	Inter-transmission times that are longer than the mean of the pre-defined distribution
short-long pattern	A short inter-transmission time followed by a long inter-transmission time

[19], [20], [21], [22], [23], [24]. In this section, we describe the current use of statistical goodness of fit tests in designing anonymous sensor networks.

4.1 SSA Solutions Based on Statistical Goodness of Fit Tests

The statistical goodness of fit of an observed data describes how well the data fits a given statistical model. Measures of goodness of fit typically summarize the discrepancy between observed values and the values expected under the statistical model in question. Such measures can be used, for example, to test for normality of residuals, to test whether two samples are drawn from identical distributions, or to test whether outcome frequencies follow a specified distribution. Examples of well-studied goodness of fit tests include, but are not limited to, the Anderson-Darling (A-D) test [26], the Kolmogorov-Smirnov (K-S) test [27], the Jarque-Bera (J-B) test [28].

The following is a description of how statistical goodness of fit tests have been used to design anonymous sensor networks. Let sensor nodes be designed to transmit independent identically distributed (iid) fake messages according to a prespecified probabilistic distribution, $\mathcal{D}$, with a desired mean, μ. Furthermore, let nodes store a sliding window of times between consecutive transmissions (intertransmission times), say $\boldsymbol{X}_i, \boldsymbol{X}_{i+1}, \ldots, \boldsymbol{X}_{k+i-1}$, where $\boldsymbol{X}_j$ is the random variable representing the time between the jth and the $(j+1)$st transmissions, and k is the length of the sliding window.

Assume that, after the $(k+i)$th transmission, a real event is detected. Ideally, the intertransmission time for reporting the detected event, represented by $\boldsymbol{X}_{k+i}$, should be a random variable drawn from $\mathcal{D}$ independently of all the $\boldsymbol{X}_j$s. To minimize delay, however, consider the following use of a statistical goodness of fit test. Let $\boldsymbol{Y}$ be a random variable drawn from $\mathcal{D}$ and let $\boldsymbol{X}_{k+i} = \boldsymbol{Y} - \epsilon$, where ϵ is defined to be the largest positive number such that the sequence of random variables in the sliding window, $\{\boldsymbol{X}_i, \ldots, \boldsymbol{X}_{k+i}\}$, passes the statistical goodness of fit test for a sequence following the distribution $\mathcal{D}$. That is, an adversary recording the sequence of intertransmission times will observe a sequence that is statistically indistinguishable from an iid sequence of random variables with the prespecified distribution of fake transmissions.

Observe, however, that by continuing in the same fashion of transmitting real event as soon as possible, the mean of the probabilistic distribution will skew away from the desired mean, μ, since nodes always favor shorter times to transmit real events. To adjust the mean, the intertransmission time between the report of the real event and next transmission, $\boldsymbol{X}_{k+i+1}$ in this example, will be purposely delayed. That is, let $\boldsymbol{Y}$ be a random variable drawn from $\mathcal{D}$ and set $\boldsymbol{X}_{k+i+1} = \boldsymbol{Y} + \delta$, where δ is defined to be the largest positive number such that the sequence of random variables in the sliding window, $\{\boldsymbol{X}_{i+1}, \ldots, \boldsymbol{X}_{k+i+1}\}$, passes the statistical goodness of fit test for a sequence following the distribution $\mathcal{D}$. Then, as shown in [11], an adversary observing the sensor node cannot differentiate between real and fake transmissions. Fig. 3 illustrates an instance of this approach.

4.2 Statistical Goodness of Fit under Interval Indistinguishability

As discussed in Section 3.1, when an adversary can distinguish between real and fake intervals, source location can be exposed. In this section, we analyze statistical goodness of fit-based solutions under the proposed model of interval indistinguishability.

As before, let $\boldsymbol{X}_i$ be the random variable representing the time between the ith and the $(i+1)$st transmissions and let the desired mean of these random variables be μ; i.e., $\mathbb{E}[\boldsymbol{X}_i] = \mu$, for all i (since the $\boldsymbol{X}_i$'s are iid). We now examine two intervals, a fake interval and a real one.

4.2.1 Fake Interval (I_F)

Recall that, in the absence of real events, nodes are programmed to transmit iid fake messages according to a pre-specified probability distribution. That is, the $\boldsymbol{X}_i$s in fake

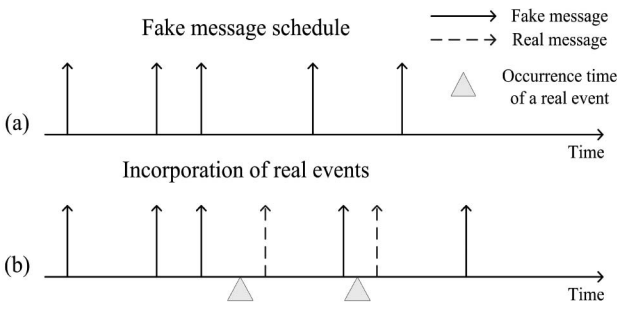

Fig. 3. An illustration of solutions based on statistical goodness of fit tests. Nodes transmit fake messages according to a prespecified probabilistic distribution and maintain a sliding window of intertransmission times. When a real event occurs, it is transmitted as soon as possible under the condition that the samples in the sliding window maintain the designed distribution. The transmission following the real transmission is delayed to maintain the mean of the distribution of intertransmission times in the sliding window.

intervals are iid random variables with mean μ. Therefore, during any fake interval, I_F, for any $\boldsymbol{X}_{i-1}, \boldsymbol{X}_i \in I_F$, one gets

$$\mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu\big] = \mu, \tag{3}$$

by the fact that $\boldsymbol{X}_{i-1}$ and $\boldsymbol{X}_i$ are independent by definition and that $\mathbb{E}[\boldsymbol{X}_j] = \mu$, for all j's.

4.2.2 Real Interval (I_R)

By definition, real intervals will have both fake and real transmissions. Let $\boldsymbol{E}_i$ be the random variable representing the type of the event reported in the ith transmission, i.e., fake or real. Then, $\boldsymbol{E}_i$ can take the values R and F, where R denotes a real event and F denotes a fake one. Since, in the most general scenario, the distribution of interarrival times of real events can be time variant and unknown beforehand, we will assume that $\boldsymbol{E}_i$ can take the values R and F with arbitrary probabilities.

Recall that the time between the transmission of a real event and its preceding fake one is usually shorter than the mean, μ, by design (to reduce delay). Recall further that the time between the transmission of a real event and its successive one is usually longer than μ by design (to adjust the ensemble mean). That is, during any real interval, I_R, for any $\boldsymbol{X}_{i-1}, \boldsymbol{X}_i \in I_R$, one gets

$$\mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu, \boldsymbol{E}_i = R\big] > \mu, \tag{4}$$

and,

$$\mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu, \boldsymbol{E}_i = F\big] = \mu, \tag{5}$$

by design. Combining (4) and (5) one gets

$$\begin{aligned}\mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu\big] &= \mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu, \boldsymbol{E}_i = R\big] \cdot \Pr[\boldsymbol{E}_i = R] \\ &\quad + \mathbb{E}\big[\boldsymbol{X}_i \mid \boldsymbol{X}_{i-1} < \mu, \boldsymbol{E}_i = F\big] \cdot \Pr[\boldsymbol{E}_i = F]\end{aligned} \tag{6}$$

$$> \mu \cdot \Pr[\boldsymbol{E}_i = R] + \mu \cdot \Pr[\boldsymbol{E}_i = F] = \mu. \tag{7}$$

An intertransmission time can be either shorter or longer than μ.[2] For the rest of the paper, we call an intertransmission time that is shorter than μ "short intertransmission time" and an intertransmission time that is longer than μ "long intertransmission time."

Equation (7) implies that short intertransmission times are most likely to be followed by long intertransmission times during real intervals. Therefore, by (3) and (7), short intertransmission times followed by long intertransmission times occur more frequently in real intervals than fake intervals (for the rest of the paper, a short-long pattern will be used to denote a short intertransmission time followed by a long intertransmission time). Fig. 4 illustrates the short-long patterns.

4.3 Questions Arising from Our Analysis

Our analysis in the previous section shows that real and fake intervals in approaches based on statistical goodness of fit tests can be theoretically distinguishable. This raises the following question: *Can the analysis in Section 4.2 be applied in practical scenarios?* If the presented analysis is indeed applicable in practical setups, then the next questions will be: *What is the mathematical explanation for the seemingly contradicting results of Section 4.2 and prior studies acknowledging the effectiveness of statistical goodness of fit tests in designing anonymous systems? That is, how can one explain the fact that the use of statistical goodness of fit is known to be secure in the literature while the analysis of Section 4.2 states otherwise?* The answers to these questions will be the main focus of Sections 5 and 6, respectively. First we provide experimental analysis in an attempt to investigate the first question.

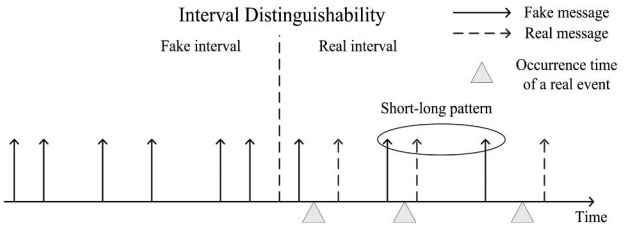

Fig. 4. An illustration of interval distinguishability in the current state-of-the-art solutions based on statistical goodness of fit tests. Real events are transmitted sooner than what is determined by the probabilistic distribution, while the transmission following the real event is later than what is determined by the probabilistic distribution to fix the mean of the predefined distribution.

5 Experimental Analysis of SSA Solutions Based on Statistical Goodness of Fit

The use of statistical goodness of fit tests in designing anonymous sensor networks was pioneered by Shao et al. in [11] and followed by schemes that build on it or acknowledge its effectiveness in providing secure SSA for sensor networks, such as [19], [20], [21], [22], [23], [24]. In this section, we analyze schemes based on statistical goodness of fit tests using the ideas implied by the theoretical analysis of Section 4.2.

5.1 Converting Real-Valued Samples to Binary Codes

Let every intertransmission time that is shorter than the mean μ be represented by the binary digit "0," and every intertransmission time that is longer than the mean μ be represented by the binary digit "1." That is, given a sequence of real-valued intertransmission times $X = \{x_1, \ldots, x_n\}$, the function g is applied to every intertransmission time as follows:

$$g(x_i) = \begin{cases} 1, & \text{if } x_i > \mu \\ 0, & \text{if } x_i \leq \mu \end{cases} \tag{8}$$

for each $i = 1, \ldots, n$. (We use g to denote the indicator function instead of the commonly used notation, I, since I is already used to denote an interval.) Then, the real-valued sequence, X, is transformed into a binary code as follows:

$$f(X) = f\big(\{x_1, \ldots, x_n\}\big) = \{g(x_1), \ldots, g(x_n)\}. \tag{9}$$

Observe that this is the same transformation used implicitly in Section 4.2. That is, short-long patterns will be represented by the ordered sequence "01." Next, we

2. Since intertransmission times are typically drawn from continuous random variables, the probability of an inter-transmission time to be equal to the mean, μ, is zero.

describe the statistical measure that will be used in our experimental analysis of SSA solutions based on statistical goodness of fit tests.

5.2 Correlation Measure for Binary Hypothesis Testing

In this section, we specify the statistical measure that will be used to perform our experimental analysis of SSA approaches based statistical goodness of fit tests. Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ be two sequences of length n. Define the correlation coefficient of the two sequences by

$$\rho(X,Y) = \frac{\left|n\sum_{i=1}^{n} x_i y_i - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)\right|}{\sqrt{\left(n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2\right)\left(n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)}}, \tag{10}$$

where x_i and y_i denote the ith elements of sequences X and Y, respectively. It can be verified that the value of ρ is always in the interval $[0,1]$ [29]. When X and Y are uncorrelated, ρ will be equal to zero. The higher value of ρ, the more the two sequences are correlated.

5.3 Correlation Analysis of SSA Solutions Based on Statistical Goodness of Fit Tests

The interpretation of the analysis of Section 4.2 in terms of the transformation of the previous section is that each bit in a binary code representing a fake interval is independent of the all other bits, while bits in a binary code representing a real interval are correlated. More specifically, a binary code representing a real interval is likely to have more "01" patterns than a binary code representing a fake interval. This suggests to the following approach to distinguish between fake and real intervals. First, generate a "reference" binary code of the form

$$\text{Ref} = \{0,1,0,1,\ldots,0,1\}. \tag{11}$$

Now, let I_0 and I_1 be two time intervals in which one of them contains real event transmissions and the other does not. Let S_0 and S_1 be the two sequences of real-valued inter-transmission times corresponding to I_0 and I_1, respectively. Let $X_0 = f(S_0)$ and $X_1 = f(S_1)$ be the conversion of S_0 and S_1 into their corresponding binary codes according to the transformation of Section 5.1. Correlate X_0 and X_1 with the reference code of (11); the binary code having a higher correlation coefficient with the reference code is the one corresponding to the real interval.

In the context of Game 1, given two intervals I_0 and I_1 in which one is real and the other is fake, the adversary's decision is given by

$$D(I_0,I_1) = \begin{cases} 0, & \text{if } \rho(\text{Ref},\ X_0) > \rho(\text{Ref},\ X_1) \\ \gamma, & \text{if } \rho(\text{Ref},\ X_0) = \rho(\text{Ref},\ X_1) \\ 1, & \text{if} \rho(\text{Ref},\ X_0) < \rho(\text{Ref},\ X_1), \end{cases} \tag{12}$$

where γ denotes any decisional strategy to break a tie. That is, the interval corresponding to the binary code that is more correlated with the reference code is decided to be the real one.

5.3.1 Experimental Parameters and Setup

In this section, We specify our parameters selection and setup our experimental analysis of approaches based on statistical goodness of fit tests.

Intertransmission times between fake transmissions are chosen to be iid exponentials with a rate parameter $\lambda = 20$. Real events arrive according to a Poisson Arrival process with mean $1/20$. The Anderson-Darling goodness of fit test is used to determine the transmission times of real events and the mean recovery algorithm. The two parameters of the A-D test are the significance level of the test and the allowed deviation from the mean which are set to 0.05 and 0.1, respectively.[3]

The experiment was run for 10,000 independent trials. Each trial consists of two intervals, a real one, I_R, and a fake one, I_F. Every trial starts with a "warm-up" period, where 200 iid exponential random variables with rate 20 are drawn to constitute a backlog to be used in the A-D goodness of fit test. Then, real events start arriving and they are transmitted according to the procedure described in Section 4.1 (interested readers may refer to [11] for more detailed algorithms of the transmission mechanism). Each real interval consists of 50 real events. After the 50th real event has been transmitted, the fake interval starts for the same amount of time the real interval lasted.

For each of the 10,000 independent trials, denote by $S_R^{(i)}$ the sequence of intertransmission times of the real interval of the ith trial and, similarly, denote by $S_F^{(i)}$ the sequence of inter-transmission times of the fake interval of the ith trial. The numbers in $S_R^{(i)}$ and $S_F^{(i)}$ will be real valued that are indistinguishable from iid exponential random variables. Let $X_R^{(i)} = f(S_R^{(i)})$ and $X_L^{(i)} = f(S_L^{(i)})$, where f is the function defined in (9), be the binary conversion of the real-valued intertransmission times of the real and fake intervals of the ith trial.

Following the decision rule in (12), we correlate $X_R^{(i)}$ and $X_F^{(i)}$ with the reference sequence Ref for all $i = 1, \ldots, 10{,}000$. Intuitively, the test is said to be successful in distinguishing between real and fake intervals in the ith trial if $\rho(\text{Ref},\ X_R^{(i)}) > \rho(\text{Ref},\ X_F^{(i)})$ and unsuccessful if $\rho(\text{Ref},\ X_R^{(i)}) < \rho(\text{Ref},\ X_F^{(i)})$. When $\rho(\text{Ref},\ X_R^{(i)}) = \rho(\text{Ref},\ X_F^{(i)})$ one of the intervals is chosen to be the real one uniformly at random.

5.3.2 Experimental Results and Anonymity Interpretation

Out of the 10,000 independent trials, the following results were obtained:

- $\rho(\text{Ref},\ X_R^{(i)}) > \rho(\text{Ref},\ X_F^{(i)})$ in 7,301 trials;
- $\rho(\text{Ref},\ X_R^{(i)}) < \rho(\text{Ref},\ X_F^{(i)})$ in 2,695 trials;
- $\rho(\text{Ref},\ X_R^{(i)}) = \rho(\text{Ref},\ X_F^{(i)})$ in four trials.

Now, consider Game 1 for analyzing interval indistinguishability. Given two intervals I_0 and I_1 at which one of them is real and one is fake, let the adversary's strategy for deciding which is which be according to the decision rule in (12). Then, given the simulation results provided above, the adversary's probability of correctly identifying

3. These are the same parameters appeared in [11].

real intervals is 0.730. In other words, the anonymity of the system is at most $\Lambda = 0.539$, significantly far away from the desired $\Lambda \approx 1$ claimed and acknowledged in prior studies such as [11], [19], [20], [21], [22], [23], [24].

6 Explanation for Discrepancies between Our Results and Prior Studies

The results of Section 5 provide an answer to the first question raised in Section 4.3. Namely that the analysis of Section 4.2 can improve the adversary's chances of distinguishing real from fake intervals and, ultimately, breaching the anonymity of the system in practical setups is possible. Now, it remains to investigate the second question raised in Section 4.3. Namely, is there a contradiction between our results and previous studies and, if not, how can we explain such discrepancies mathematically. The keys to answer such questions are "interval indistinguishability" and "nuisance information." We start by a brief background.

6.1 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 [30]. 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 before performing the hypothesis testing [30]. That is, given a data sample $X = (x_1, \ldots, x_n)$ that belongs to one of two possible hypotheses H_0 or H_1, the test is performed on a transformation of the data sample, $f(X)$, rather than the original data itself, X. The transformation function, f, is an application dependent and choosing the right function is a critical step in hypothesis testing with nuisance parameters [30].

6.2 Significance of Interval Indistinguishability and Nuisance Removal

In the literature, the use of statistical goodness of fit to design anonymous sensor networks is known to be secure. The analysis of Section 5, on the other hand, demonstrates that this is not the case. While this might look like a contradiction, there is a mathematical justification for such discrepancy, which can be divided into two points. First, previous studies model statistical source anonymity by the adversary's ability to distinguish between *individual* transmissions. That is, given a sequence of intertransmission times, the adversary is shown to be unable to determine which transmission is fake and which one is real. The interval indistinguishability notion introduced in this paper,[4] on the other hand, assumes that source anonymity can be breached when adversaries can successfully distinguish between real and fake *intervals*.

Observe that no tool in our analysis is introduced to allow the adversary to infer which transmission is real and which one is fake within the real interval itself. That is, if the analysis of Section 5 is repeated with the assumption that anonymity is breached only if the adversary can distinguish between individual fake and real transmissions, the anonymity of the system will be different then the obtained 0.539 (it might very well be close to the desired $\Lambda \approx 1$ since we do not present any mechanism to distinguish between individual transmissions). Therefore, the notion of interval indistinguishability is essential in explaining the discrepancies between our results and prior studies that model SSA by the adversary's ability to distinguish between individual real and fake transmissions.

Interval indistinguishability alone, however, does not explain why our results are different than what is believed in prior work. That is, even though different statistical tools are used to measure anonymity (statistical goodness of fit tests are used to analyze anonymity in previous studies while we use the correlation measure specified in Section 5.2), the difference in the used statistical measure does not explain the discrepancies between our results and prior work.

The conversion of real-valued intertransmission times into binary codes is the main reason for the differences between our anonymity results of Section 5 and prior studies. The conversion to binary codes is a key-enabling tool for the removal of nuisance information precluding successful hypothesis testing. The following experimental analysis demonstrate the significance of the binary code conversion.

6.2.1 Experimental Parameters and Setup

In order to examine the effect of binary code conversion for nuisance removal, the experimental analysis of Section 5 is repeated with the real-valued intertransmission times as opposed to their binary transformation. Ten thousand independent trials are performed. In very trial, a real interval, $S_R^{(i)}$, and a fake interval, $S_F^{(i)}$, are generated with the same parameters of Section 5.3.1. In each trial, the two intervals are correlated with a reference sequence using the formula in (10). However, as opposed to the binary reference code of (11), one real interval, $\mathrm{Ref}_{\mathrm{rv}}$, that serves as a reference sequence of real-valued intertransmission times is generated as a reference sequence.

6.2.2 Experimental Results and Anonymity Interpretation

Out of the 10,000 independent trials, the following results were obtained:

- $\rho(\mathrm{Ref}_{\mathrm{rv}}, S_R^{(i)}) > \rho(\mathrm{Ref}_{\mathrm{rv}}, S_F^{(i)})$ in 5,076 trials;
- $\rho(\mathrm{Ref}_{\mathrm{rv}}, S_R^{(i)}) < \rho(\mathrm{Ref}_{\mathrm{rv}}, S_F^{(i)})$ in 4,924 trials;
- $\rho(\mathrm{Ref}_{\mathrm{rv}}, S_R^{(i)}) = \rho(\mathrm{Ref}_{\mathrm{rv}}, S_F^{(i)})$ in 0 trials.[5]

Under the same adversarial strategy of deciding which interval is real and which is fake given in (12), the system is 0.984-anonymous using real-valued intertransmission times. This result agrees with previous studies in that the sequences corresponding to any trial, whether real or fake, are statistically indistinguishable from iid exponential random variables. On the other hand, when the same system is analyzed using the binary code conversion of intertransmission times it was only 0.539-anonymous. The

4. Recall that, as discussed in Section 3.2, interval indistinguishability implies individual transmission indistinguishability.

5. This is expected since we are dealing with real valued intertransmission times in this case.

importance of this result is that it shows how the actual lengths of intertransmission times can act as nuisance and prevent accurate hypothesis testing.

The results of this section conclude our explanations to the questions posed in Section 4.3. In particular, the results show that there is no contradiction between the results obtained and acknowledged in prior studies and our result of Section 4.2, and that the combination of the interval indistinguishability model and the existence of nuisance information is the mathematical explanation for such seemingly contradicting results.

7 Improving SSA via Induced Correlation in Fake Intervals

Our analysis of SSA solutions based on statistical goodness of fit tests shows that the use of such statistical tools is insufficient to guarantee source anonymity. In particular, not only the real-valued intertransmission times must be indistinguishable from the desired distribution of fake transmissions, but also the binary codes representing the intertransmission times of fake and real intervals must have indistinguishable statistical properties. In what follows, we describe a modification to approaches based on statistical goodness of fit tests to improve their anonymity. The main idea behind the proposed approach is the attempt to induce the same correlation pattern of intertransmission times during real intervals into intertransmission times during fake intervals.

7.1 The Proposed Approach

As can be seen from the analysis in Section 4.2, intertransmission times during fake intervals are iid's, while intertransmission times during real intervals are neither independent nor identically distributed. In theory, the only way to guarantee that a sequence of random variables is statistically indistinguishable from a given iid sequence is to generate it as an iid sequence with the same distribution.

The notion of interval indistinguishability, suggests a different approach for the design of anonymous sensor networks. Observe that Definition 1 of interval indistinguishability does not impose any requirements, such as iid, on the distribution of intertransmission times during fake intervals. Therefore, designing fake intervals with the distribution that is easiest to emulate during real intervals is the most logical solution. This idea opens the door for more solutions as it gives more flexibility for system designers.

To improve anonymity, we suggest introducing the same correlation of intertransmission times during real intervals to intertransmission times during fake intervals. That is, let the transmission procedure consists of two different algorithms: A_R and A_F. In the presence of real events (i.e., in real intervals), algorithm A_R is implemented. In the absence of real events (i.e., in fake intervals), algorithm A_F is implemented. Algorithm A_R is the same as the algorithm described in Section 4.1. In algorithm A_F, 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 A_R, 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. (There is more to be done to decide how nodes switch from algorithm A_R to A_F and vice versa, but since this is not the main focus of this paper, we defer detailed discussion to future investigation that converts the solution to coding problem.)

7.2 Experimental Parameters and Setup

The same experimental analysis of Section 5 is performed with one major difference. To make fake intervals possess the same correlation of real intervals, we implemented the A_F algorithm described above. Dummy events were generated according to iid Gaussian interarrival times with mean 0.05 seconds and a variance of 0.02. (We reemphasize the distinction between fake messages and dummy events: fake messages are the ones transmitted to hide the existence of real transmissions, while dummy events are the ones generated, during fake intervals only, to resemble the existence of real events.) Note that the interarrival distribution of dummy events is purposely different than the interarrival distribution of real events to count for the general case of unknown distribution of real events interarrivals. The A-D test is used in both algorithms, A_R and A_F, to determine the transmission times of real events and dummy events, respectively.

7.3 Experimental Results and Anonymity Interpretations

By running the experiment for 10,000 independent trials, the following observations were recorded.

- $\rho(\text{Ref},\ X_R^{(i)}) > \rho(\text{Ref},\ X_F^{(i)})$ in 5,161 trials;
- $\rho(\text{Ref},\ X_R^{(i)}) < \rho(\text{Ref},\ X_F^{(i)})$ in 4,832 trials;
- $\rho(\text{Ref},\ X_R^{(i)}) = \rho(\text{Ref},\ X_F^{(i)})$ in seven trials.

In terms of the anonymity measure of (1), the system is 0.967-anonymous under the adversarial strategy of (12). Observe the improvement in anonymity against correlation attacks in our modified version (from 0.539 without the use of dummy events to 0.967 when dummy events are used). Table 2 summarizes our experimental results.

7.4 Performance of the Solution

Compared to the original SSA scheme described in Section 4.1, the solution presented in this section induces more computational overhead. That is, while the original scheme described in Section 4.1 requires nodes to perform statistical goodness of fit tests during real intervals only, the solution of this section involves the use of statistical goodness of fit test in both real and fake intervals. Note, however, that the solution of this section does not involve extra communication overhead, only rescheduling of fake transmissions that must be sent anyway. This is an important observation since communication consumes orders of magnitude more energy than computations (depending on hardware, transmitting one bit may consume

TABLE 2
A Quantitative Comparison of the Statistical Goodness of Fit Test-Based Approach of Section 4.1 After the Transformation of Section 5.1 (i.e., without Nuisance), the Statistical Goodness of Fit Test-Based Approach of Section 4.1 without the Transformation of Section 5.1 (i.e., with Nuisance), and Our Improved SSA Solution of Section 7 After the Transformation of Section 5.1 (i.e., without Nuisance)

	$\rho_R > \rho_F$	$\rho_R < \rho_F$	$\rho_R = \rho_F$	Anonymity bound
Statistical goodness of fit based approach (without nuisance)	7,301	2,695	4	0.539
Statistical goodness of fit based approach (with nuisance)	5,076	4,924	0	0.984
Our modified approach (without nuisance)	5,161	4,832	7	0.967

$\rho_R > \rho_F$ denotes larger correlation coefficient in real intervals, $\rho_R < \rho_F$ denotes larger correlation coefficient in fake intervals, while $\rho_R = \rho_F$ denotes equal correlation coefficient in real and fake intervals. The simulation results are obtained from 10,000 independent trials.

up to 2,900 times the energy consumed by performing one instruction) [31].

We emphasize, however, that this solution is merely presented to illustrate how to improve the anonymity of approaches based on statistical goodness of fit tests. The main focus of this work is to come up with a framework that can be used to design and analyze anonymous sensor networks. Using the proposed framework, including the mapping of the problem of statistical source anonymity to coding theory, in order to design more efficient schemes that satisfy the notion of interval indistinguishability is an open research problem.

8 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.

Consider the example of Fig. 5 and assume the adversary's chance of distinguishing between real and fake intervals of each node's transmissions is 55 percent. In such a scenario, according to (1), the anonymity of each node is $\Lambda = 0.9$. The monitored target, however, is moving and node b will start reporting its existence. On average, the adversary will also have a 55 percent chance of breaking the anonymity of node b. Combining the observations from node a and b, the anonymity is reduced to be $\Lambda^2 = 0.81$. Consequently, by the time the target reaches node e, the anonymity is already reduced to 0.59. That is, given the adversary's knowledge of the network topology, the anonymity of a moving target is an exponentially decreasing function of the number of hops reporting its proximity.

In a different direction, consider the case in which multiple nodes are reporting the same event simultaneously, as depicted in Fig. 6. Then, even if the target is stationary, the anonymity is reduced to $\Lambda^6 = 0.53$ (assuming the anonymity of each node is 0.9).

Therefore, unless the anonymity of each node is $\Lambda = 1$, or if there is a multihop anonymous design, global adversaries can substantially increase their advantages of breaking the anonymity of the sensor network by utilizing their knowledge of the network topology and performing multihop analysis.

9 Related Work

The privacy problem in wireless sensor networks comes in different flavors. Proposals dealing with providing sink anonymity in wireless sensor networks have appeared in, e.g., [32], [33], [34], [35], [36]. Network coding-based approaches that protect against traffic analysis have appeared in, e.g., [37], [38], [39]. The privacy problem most

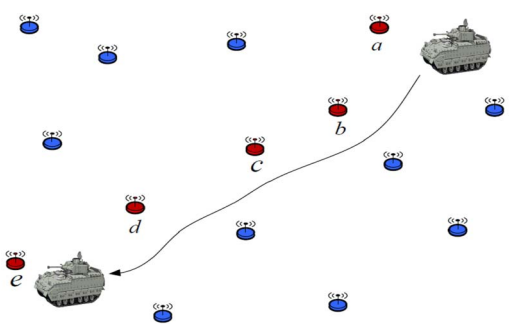

Fig. 5. An example of a sensor networks monitoring a moving target. As the tank moves along its path, nodes a, b,c, d, and e report that the tank is within their sensing range.

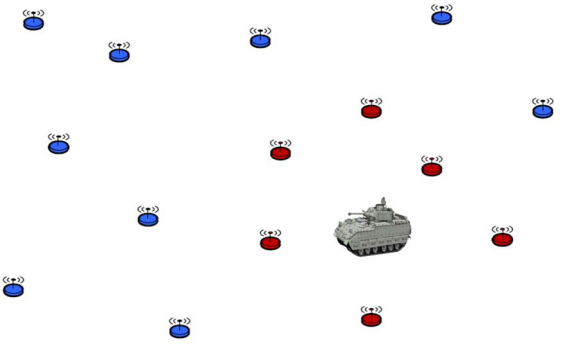

Fig. 6. An example of multiple sensor nodes reporting a stationary event. Six nodes are simultaneously reporting that the tank is within their sensing range.

relevant to this work is the source location privacy in wireless sensor networks. Li et al. presented a state-of-the-art survey on privacy preservation in wireless sensor networks [20].

The source location privacy in sensor networks is part of a broader area, the design of anonymous communication systems. The foundation for this field was laid by Chaum in [40], and since then has become a very active area of research. In particular, topics related to location anonymity have been discussed by Reed et al. in [41], who introduced the idea of preserving anonymity through onion routing, and by Gruteser and Grunwald in [42], 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 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 in [12], [13]. 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 [17], 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 [18]. In [14], 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 [21], Wang et al. proposed a technique to maximize source location privacy by designing routing protocols that distribute message flows to different routes.

However, in the global adversarial model, in which the adversary has access to all transmissions in the network, routing-based schemes are insufficient to provide location privacy [10], [11]. The global adversarial model was first introduced by Mehta et al. in [10]. The authors motivated the problem, analyzed the security of existing routing-based schemes under the new model, and proposed two new schemes. In the first scheme, some sensor nodes act as fake sources by mimicking the behavior of real events. For example, if the network is deployed to track an animal, the fake sources could send fake messages with a distribution resembling that of the animal's movements. This, however, assumes some knowledge of the time distribution of real events. In the second scheme, packets (real and fake) are sent either at constant intervals or according to a predetermined probabilistic schedule. Although this scheme provides perfect location privacy, it also introduces undesirable performance characteristics, in the form of either relatively high delay or relatively high communication and computational overhead. The scheme of [11] was proposed to address this delay/overhead tradeoff.

In [11], Shao et al. introduced the notion of statistically strong source anonymity in which a global adversary with ability to monitor the traffic in the entire network is unable to infer source locations by performing statistical analysis on the observed traffic. In order to realize their notion of statistical anonymity, nodes are programmed to transmit fake events according to prespecified distribution. More specifically, after the transmission of every fake event, the node draws an exponentially distributed random variable $t \sim \mathrm{Exp}(\lambda)$, where λ is the prespecified rate of the exponential distribution. The node then waits for t time units and then transmits another fake event. That is, in the absence of real event transmissions, an adversary monitoring the sensor node will observe intertransmission times that are iid exponentials with mean $\mu = 1/\lambda$.

Upon the occurrence of real events, the goal of a sensor node is to transmit them while maintaining the exponential distribution of the intertransmission times. Obviously, if nodes delay their transmission of real events to the next scheduled fake transmission, no statistical test can be used to distinguish between real and fake events (since intertransmission times are kept exponential iid's with the same rate). The goal in [11], however, is to minimize the latency of reporting real events while maintaining statistical indistinguishability between real and fake transmissions.

To reduce the latency, the authors of [11] proposed the following procedure: let imd_i represent the intertransmission time between the ith and the $(i+1)$st transmissions. Assume a real event has occurred after the transmission of the ith event. Given $\{imd_1, imd_2, \ldots, imd_i\}$, imd_{i+1}, the time after the transmission of the ith event the node must wait before it can transmit the real event, is determined as follows: imd_{i+1} is the smallest positive value such that the sequence $\{imd_1, imd_2, \ldots, imd_i, imd_{i+1}\}$ passes the Anderson-Darling goodness of fit test [43] for a sequence of iid exponentials with mean μ.

Observe, however, that on average $imd_{i+1} < \mu$ since imd_{i+1} is, by definition, the minimum value that passes the test. Therefore, continuing in this fashion will cause the mean of the entire sequence to skew away from desired mean.

To solve the problem of mean deviation described above, the scheme in [11] includes a mean recovery algorithm. The mean recovery algorithm outputs a delay δ and the time between the transmission of a real event and the following event (fake or real) is set to $imd_{i+2} = t + \delta$, where $t \sim \mathrm{Exponential}(\lambda)$. The scheme in [11] is designed so that the sequence $\{imd_1, \ldots, imd_n\}$, where n is the last transmitted message, always passes the A-D goodness of fit test.

To reduce the amount of traffic in the network that is due to the transmission of fake events, techniques based on node proxies and data aggregation have been proposed [19], [44]. In such techniques, the overall communication overhead is reduced by making intermediate nodes act as proxies that filter out fake messages or by aggregating multiple messages in a single transmission. Such approaches make schemes based on generating fake messages more attractive by mitigating the high communication overhead issue.

Shao et al. also consider the problem of an active adversary in [45]. Their adversary also has the ability to perform node compromise attacks, and they develop tools to prevent the adversary from gaining access to event data stored in a node even if the adversary possesses that node's secret keys.

In recent works, Li and Ren [46] proposed a scheme to provide both content confidentiality and source-location privacy through routing to a randomly selected intermediate node (RRIN) and a network mixing ring (NMR), where the RRIN provides local source location privacy and NMR

yields network-level (global) source location privacy. Ouyang et al. [47] proposed four schemes: naive, global, greedy, and probabilistic to protect the source location against global adversaries in. Abbasi et al. [48] proposed a distributed algorithm to mix real event traffic with carefully chosen dummy traffic to hide the real event traffic pattern.

10 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 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.

Acknowledgments

Preliminary versions of this paper appeared in the 40th Annual IEEE/IFIP Conference on Dependable Systems and Networks (DSN 2010) [1] and the 53rd IEEE Global Communications Conference (GlobeCom 2010) [2].

References

[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] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Statistical Framework for Source Anonymity in Sensor Networks," *Proc. IEEE GlobeCom,* 2010.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks,* vol. 38, no. 4, pp. 393-422, 2002.

[4] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," *Proc. IEEE 13th Mediterranean Conf. Control and Automation (MED '05),* pp. 719-724, 2006.

[5] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless Sensor Network Survey," *Computer Networks,* vol. 52, no. 12, pp. 2292-2330, 2008.

[6] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02),* pp. 41-47, 2002.

[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks,* vol. 8, no. 5, pp. 521-534, 2002.

[8] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," *Proc. Eighth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '06),* pp. 46-59, 2006.

[9] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," *Proc. Ninth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '07),* pp. 450-466, 2007.

[10] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," *Proc. IEEE 15th Int'l Conf. Network Protocols (ICNP '07),* pp. 314-323, 2007.

[11] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," *Proc. IEEE INFOCOM,* pp. 466-474, 2008.

[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," *Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS '05),* pp. 599-608, 2005.

[13] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," *Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04),* pp. 88-93, 2004.

[14] Y. Ouyang, Z. Le, G. Chen, J. Ford, F. Makedon, and U. Lowell, "Entrapping Adversaries for Source Protection in Sensor Networks," *Proc. IEEE Seventh Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WOWMOM '06),* pp. 32-41, 2006.

[15] X. Wang, X. Li, Z. Wan, and M. Gu, "CLEAR: A Confidential and Lifetime-Aware Routing Protocol for Wireless Sensor Network," *Proc. IEEE 20th Ann. Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC '09),* pp. 2265-2269, 2009.

[16] Y. Li and J. Ren, "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks," *Proc. IEEE INFOCOM,* pp. 1-9, 2010.

[17] Y. Xi, L. Schwiebert, and W. Shi, "Preserving Source Location Privacy in Monitoring-Based Wireless Sensor Networks," *Proc. IEEE 20th Int'l Parallel & Distributed Processing Symp. (IPDPS '06),* pp. 1-8, 2006.

[18] B. Hoh and M. Gruteser, "Protecting Location Privacy Through Path Confusion," *Proc. IEEE/CreatNet First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05),* pp. 194-205, 2005.

[19] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," *Proc. First ACM Conf. Wireless Network Security (WiSec '08),* pp. 77-88, 2008.

[20] N. Li, N. Zhang, S. Das, and B. Thuraisingham, "Privacy Preservation in Wireless Sensor Networks: A State-of-the-Art Survey," *Elsevier J. Ad Hoc Networks,* vol. 7, no. 8, pp. 1501-1514, 2009.

[21] H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," *Elsevier J. Computer Networks,* vol. 53, no. 9, pp. 1512-1529, 2009.

[22] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. La Porta, "Cross-Layer Enhanced Source Location Privacy in Sensor Networks," *Proc. IEEE Comm. Soc. Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09),* pp. 324-332, 2009.

[23] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query Privacy in Wireless Sensor Networks," *ACM Trans. Sensor Networks,* vol. 6, no. 2, pp. 1-34, 2010.

[24] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks," *IEEE J. Selected Areas in Comm.,* vol. 28, no. 5, pp. 677-691, June 2010.

[25] S. Goldwasser and S. Micali, "Probabilistic Encryption," *J. Computer and System Sciences,* vol. 28, no. 2, pp. 270-299, 1984.

[26] T. Anderson and D. Darling, "Asymptotic Theory of Certain 'Goodness of Fit' Criteria Based on Stochastic Processes," *The Annals of Math. Statistics,* vol. 23, no. 2, pp. 193-212, 1952.

[27] F. Massey Jr., "The Kolmogorov-Smirnov Test for Goodness of Fit," *J. Am. Statistical Assoc.,* vol. 46, no. 253, pp. 68-78, 1951.

[28] C. Jarque and A. Bera, "A Test for Normality of Observations and Regression Residuals," *Int'l Statistical Rev./Revue Internationale de Statistique,* vol. 55, no. 2, pp. 163-172, 1987.

[29] S. Golomb and G. Gong, *Signal Design for Good Correlation.* Cambridge Univ., 2005.

[30] L. Scharf, *Statistical Signal Processing: Detection, Estimation, and Time Series Analysis.* Addison-Wesley, 1991.

[31] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks.* Wiley, 2005.

[32] Q. Gu, X. Chen, Z. Jiang, and J. Wu, "Sink-Anonymity Mobility Control in Wireless Sensor Networks," *Proc. IEEE Fifth Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WiMob '09),* pp. 36-41, 2009.

[33] E. Shakshuki, T. Sheltami, N. Kang, and X. Xing, "Tracking Anonymous Sinks in Wireless Sensor Networks," *Proc. IEEE 23rd Int'l Conf. Advanced Information Networking and Applications (AINA '09)*, pp. 510-516, 2009.
[34] E. Ngai and I. Rodhe, "On Providing Location Privacy for Mobile Sinks in Wireless Sensor Networks," *Proc. 12th ACM Int'l Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '09)*, pp. 116-123, 2009.
[35] E. Ngai, "On Providing Sink Anonymity for Sensor Networks," *Proc. Fifth Int'l Conf. Wireless Comm. and Mobile Computing: Connecting the World Wirelessly (IWCMC '09)*, pp. 269-273, 2009.
[36] Z. Liu and W. Xu, "Zeroing-In on Network Metric Minima for Sink Location Determination," *Proc. Third ACM Conf. Wireless Network Security (WiSec '10)*, pp. 99-104, 2010.
[37] E. Ayday, F. Delgosha, and F. Fekri, "Location-aware Security Services for Wireless Sensor Networks Using Network Coding," *Proc. IEEE INFOCOM*, pp. 1226-1234, 2007.
[38] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient Privacy-Preserving Scheme against Traffic Analysis Attacks in Network Coding," *Proc. IEEE INFOCOM*, pp. 19-25, 2009.
[39] Y. Jiang, Y. Fan, X. Shen, and C. Lin, "A Self-Adaptive Probabilistic Packet Filtering Scheme against Entropy Attacks in Network Coding," *Computer Networks*, vol. 53, no. 18, pp. 3089-3101, 2009.
[40] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Comm. ACM*, vol. 24, no. 2, pp. 84-90, 1981.
[41] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE J. Selected Areas in Comm.*, vol. 16, no. 4, pp. 482-494, May 1998.
[42] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," *Proc. ACM MobiSys*, pp. 31-42, 2003.
[43] M. Stephens, "EDF Statistics for Goodness of Fit and Some Comparisons," *J. Am. Statistical Assoc.*, vol. 69, no. 347, pp. 730-737, 1974.
[44] W. Yang and W. Zhu, "Protecting Source Location Privacy in Wireless Sensor Networks with Data Aggregation," *Proc. Seventh Int'l Conf. Ubiquitous Intelligence and Computing (UIC '10)*, pp. 252-266, 2010.
[45] M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang, "pDCS: Security and Privacy Support for Data-Centric Sensor Networks," *IEEE Trans. Mobile Computing*, vol. 8, no. 8, pp. 1023-1038, Aug. 2009.
[46] Y. Li and J. Ren, "Preserving Source-Location Privacy in Wireless Sensor Networks," *Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09)*, pp. 493-501, 2009.
[47] Y. Ouyang, Z. Le, D. Liu, J. Ford, and F. Makedon, "Source Location Privacy against Laptop-Class Attacks in Sensor Networks," *Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08)*, pp. 1-10, 2008.
[48] A. Abbasi, A. Khonsari, and M. Talebi, "Source Location Anonymity for Sensor Networks," *Proc. IEEE Sixth Conf. Consumer Comm. and Networking Conf. (CCNC '09)*, pp. 588-592, 2009.

Basel Alomair received the bachelor's, master's, and PhD degrees from King Saud University, Riyadh, Saudi Arabia; the University of Wisconsin, Madison; and the University of Washington, Seattle, respectively. He is an assistant research professor in the Computer Research Institute (CRI) at the King Abdulaziz City for Science and Technology (KACST), a member of the Network Security Lab (NSL) at the University of Washington, and a member of the Center of Excellence in Information Assurance (CoEIA) at King Saud University. His PhD dissertation was recognized by the IEEE Technical Committee on Fault-Tolerant Computing (TC-FTC) and the IFIP Working Group on Dependable Computing and Fault Tolerance (WG 10.4) through the 2010 William C. Carter Award. He was also the recipient of the 2011 University of Washington's Electrical Engineering (UWEE) Outstanding Research Award. In 2012, he was awarded the University of Washington's Center for Information Assurance and Cybersecurity (UW CIAC) Distinguished Dissertation Award. His research interests include wireless network security and applied cryptography. He is a member of the IEEE.

Andrew Clark received the BSE degree in electrical engineering and the MS degree in mathematics from the University of Michigan, Ann Arbor, in 2007 and 2008, respectively. He is currently working toward the PhD degree in the Network Security Lab at the University of Washington, Seattle. His research interests include wireless network security, especially design and implementation of security metrics. He is a student member of the IEEE.

Jorge Cuellar is a principal consultant at Siemens AG. He was awarded the DI-ST Award for the best technical achievement for his work on modeling of operating systems and transaction managers. He has coauthored about 30 papers on different topics, including mathematical modeling of performance analysis, learning algorithms, hand-writing recognition, formal specification and verification of distributed system design, and security. He has done technical standardization work related to the development of privacy and security protocols at the IETF, 3GPP, and the Open Mobile Alliance. He has 16 inventions and patents. He has worked on several EU-funded research projects, in particular in AVISPA and AVANTSSAR, both related to the formal modeling and verification of security, and currently on NESSoS, WebSand, and SPACIoS. He has served on many program committees for international conferences, and in particular, he has been the PC cochair of Software Engineering and Formal Methods (SEFM 2004), Formal Methods (FM 2008), and STM 2010, and on the steering committee of ESSoS. He has presented more than 20 invited talks at conferences and seminars, and acts regularly as a reviewer for international conferences and journals. He has been on the editorial board of the *Journal of Science of Computer Programming* (Elsevier) and has been a guest editor for several journals. He is a member of the Industrial Curatory Board of Dagstuhl, Leibniz Center for Informatics, the world's premier venue for informatics. He has held many short term visiting teaching positions at different universities around the world.

Radha Poovendran is a professor and founding director of the Network Security Lab (NSL) in the Electrical Engineering (EE) Department at the University of Washington (UW). He received the NSA Rising Star Award in 1999 and Faculty Early Career Awards including the National Science Foundation CAREER in 2001, ARO YIP in 2002, ONR YIP in 2004, and PECASE in 2005 for his research contributions to multiuser, wireless security. He received the Outstanding Teaching Award and Outstanding Research Advisor Award from UW EE in 2002, the Graduate Mentor Award from the Office of the Chancellor at the University of California, San Diego in 2006, and the Pride@Boeing award in 2009. He coauthored papers recognized with the IEEE PIMRC Best Paper Award in 2007, the IEEE and IFIP William C. Carter Award in 2010, and the AIAA/IEEE Digital Avionics Systems best session paper award in 2010. He coedited a book titled *Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks* and served as a co-guest-editor for an *IEEE Journal on Selected Areas in Computing* special issue on wireless ad hoc networks security. He has cochaired many conferences and workshops, including the first ACM Conference on Wireless Network Security (WiSec) in 2008, the NITRD-NSF National Workshop on High-Confidence Transportation Cyberphysical Systems in 2009, and Trustworthy Aviation Information Systems at AIAA Infotech@Aerospace 2010 and 2011 and IEEE Aerospace 2011. He is a chief editor for the forthcoming *Proceedings of the IEEE* special issue on cyberphysical systems. He was a Kavli fellow of the National Academy of Sciences in 2007 and is a senior member of the IEEE.