SECURITY AND PRIVACY IN WIRELESS NETWORKING AND MOBILE CROWD SENSING

JING YANG KOH

B. Eng. (Hons.), NTU

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

NUS GRADUATE SCHOOL FOR INTEGRATIVE SCIENCES AND ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2017

Declaration

I hereby declare that the thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Jing Yang Koh

1 August 2017

Acknowledgements

First and foremost, I would like to express my gratitude to my research adviser Professor Lawrence W. C. Wong for his guidance and patience throughout my postgraduate journey. I would also like to extend my deep appreciation to my research co-advisers and mentors Dr Derek Leong and Dr Ido Nevat for teaching me how to conduct good research and for sharing candid tips on writing good research papers.

Next, I would like to thank my collaborator Dr Gareth W. Peters for the fruitful discussions and guidance on my various research problems. I would also like to thank my thesis advisory committee members, Professor Teng Joon Lim and Professor Ee-Chien Chang for their invaluable suggestions and encouraging comments on my research work. I am also grateful to the Agency for Science, Technology and Research (A*STAR), Singapore for funding my postgraduate studies at NUS and at the Institute for Infocomm Research.

I would like to thank my dearest wife Wei Xia and my beloved parents for their continuous encouragement and support throughout my postgraduate journey.

Lastly, I would like to acknowledge all my friends and colleagues at the NUS Graduate School for Integrative Sciences and the Institute for Infocomm Research who directly or indirectly helped me complete this thesis.

Abstract

This thesis addresses three specific security and privacy issues in wireless networking and mobile crowdsensing, each targeting a different security or privacy challenge. Specifically, we study and address (i) the location spoofing attack in time-of-arrival (TOA)-based localization systems, (ii) the traffic analysis attack in wireless networks, and (iii) privacy-awareness in mobile crowd sensing (MCS) applications.

First, we study how to detect location spoofing attacks in TOA-based localization systems and design a generalized likelihood ratio test (GLRT) to detect location spoofing anomalies in the received TOA delay measurements. Second, we study how to provide privacy for a communicating source-destination pair and formulate an efficient optimization problem to select the routing path distribution that minimizes the detection probability of Bayesian maximum-a-posteriori (MAP) inference (a type of traffic analysis method). We then formulate linear programs to minimize the expected detection probability of a MAP adversary, subjected to a privacy budget constraint. We also propose the (k,ϵ)-anonymity privacy constraint for strict privacy guarantees in wireless networks and formulate a mixed-integer linear program to minimize the expected routing cost of the path distribution that satisfies the (k,ϵ)-anonymity privacy constraint. Finally, we study how to improve the utility (in terms of spatial coverage) of privacy-aware mobile crowd sensing applications and propose a Stackelberg game incentive mechanism to select the optimal set of participating mobile users.

Key words: location spoofing, Bayesian traffic analysis, k-anonymity, location privacy, incentive mechanism, privacy-aware.

Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

BAN ..... Body area network

GLRT ..... Generalized likelihood ratio test

GPS ..... Global positioning system

IoT ..... Internet of things

LBS ..... Location-based service

LP ..... Linear program

LRT ..... Likelihood ratio test

MANET ..... Mobile ad hoc network

MAP ..... Maximum-a-posteriori

MCS ..... Mobile crowd sensing

MILP ..... Mixed-integer linear program

MNAR ..... Missing-not-at-random

MSE ..... Mean squared error

MST ..... Minimum spanning tree

NE ..... Nash equilibrium

NLOS ..... Non-line-of-sight

RFID ..... Radio-frequency identification

RSS ..... Received signal strength

ROC ..... Receiver operating characteristic

SCADA ..... Supervisory control and data acquisition

SNR ..... Signal-to-noise

TOA ..... Time-of-arrival

TWR ..... Two-way-ranging

WMN ..... Wireless mesh network

WSN ..... Wireless sensor network

UWB ..... Ultra-wide band

List of Publications

8. **J. Y. Koh**, G. W. Peters, D. Leong, I. Nevat, W.-C. Wong, “Privacy-Aware Stackelberg Incentive Mechanism for Mobile Crowd Sensing,” in preparation for journal publication.

7. **J. Y. Koh**, G. W. Peters, I. Nevat, D. Leong, W.-C. Wong, “Probabilistic Routing in Wireless Networks with Privacy Guarantees," under review, *IEEE Transactions on Signal Processing*, 2017.

6. **J. Y. Koh**, D. Leong, G. W. Peters, I. Nevat, W.-C. Wong, “Optimal Privacy-Preserving Probabilistic Routing for Wireless Networks," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, pp. 1–10, Apr. 2017.

5. **J. Y. Koh**, G. W. Peters, D. Leong, I. Nevat, W.-C. Wong, “Privacy-Aware Incentive Mechanism for Mobile Crowd Sensing," in *Proc. IEEE International Conference on Communications (ICC)*, May 2017.

4. **J. Y. Koh**, I. Nevat, D. Leong, W.-C. Wong, “Geo-spatial Location Spoofing Detection for Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 971–978, Dec. 2016.

3. **J. Y. Koh**, C. M. Teo, D. Leong, W.-C. Wong, “Reliable Privacy-Preserving Communications for Wireless Ah Hoc Networks," in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2015.

2. **J. Y. Koh**, C. M. Teo, W.-C. Wong, “Mitigating Byzantine Attacks in Data Fusion Process for Wireless Sensor Networks using Witnesses," in *Proc. IEEE International Conference on Communication Systems (ICCS)*, Nov. 2014.

1. P. Zhang, **J. Y. Koh**, S. Lin, I. Nevat, “Distributed event detection under Byzantine attack in wireless sensor networks," in *Proc. IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, Apr. 2014.

Chapter 1

Introduction

The research work presented in this thesis revolves around applying mathematical modeling techniques to address security and privacy concerns in wireless networking and mobile crowd sensing. In this chapter, we discuss the key motivations, briefly describe the related work, and highlight the main contributions of the research work done.

Wireless networks are one of today's most used technologies. Its applications include cellular networks [1], Wi-Fi [2], wireless sensor networks (WSN) [3–5], wireless mesh networks (WMN) [6–8], Internet of things (IoT) [9–11], vehicular ad hoc networks (VANET) [12–14], body area networks (BAN) [15], mobile ad hoc networks (MANET) [16–18] and even wireless supervisory control and data acquisition (SCADA) [19] systems. Wireless networks have gained widespread usage as they facilitate convenient access to information, allow user mobility and provide an ease of deployment compared to its wired counterpart. As applications that rely on wireless networks continue to proliferate, so will our reliance on them. Hence, the existing list of security and privacy related vulnerabilities can no longer be ignored. This is particularly true for corporate, healthcare, governmental, and military networks where it is costly to receive falsified or spoofed data or leak private information due to malicious attacks.

While there exist many significant attacks that undermine the reliability of wireless networks, we focus on three specific problems of interest – detecting location spoofing attacks, mitigating traffic analysis attacks, and facilitating privacy-awareness. In a location spoofing attack, an adversary deliberately manipulates information in the localization protocol such that it

appears to be in another location other than its true location. This allows the adversary to gain an unfair advantage over honest network users. The adversary may also masquerade as another network user if it is able to spoof its location information [20]. In the scenario of traffic analysis attacks, it may be possible for an adversary to trace the communications and mobility patterns of individual network users. This results in major privacy concerns, which can deter privacy-concerned users from adopting the vulnerable applications [21]. In addition, the privacy leakages can also cause embarrassment to the system providers and monetary losses for the network users. As for privacy-aware applications (e.g., mobile crowd sensing), the system providers can design an incentive mechanism to incentivize privacy-concerned users to participate in the applications. Since different users may have different privacy preferences [22], a privacy-aware application should accommodate the different user privacy preferences to attract user participation and improve its utility.

To summarize, the main goals of the thesis are to secure the wireless systems against location spoofing attacks, and to address the privacy concerns of the network users. Specifically, the two goals are divided into three topics that address the following research questions:

Topic 1. How to effectively detect location spoofing attacks in TOA-based localization systems?

Topic 2. How to effectively mitigate wireless traffic analysis attacks against a powerful global observer?

Topic 3. How to effectively incentivize mobile smartphone user participation while preserving their location privacy?

Thesis organization: Chapter 2 discusses the work on detecting location spoofing attacks, under Topic 1. Chapter 3 and 4 discuss the work on providing privacy for wireless communications, under Topic 2. Chapter 5 discusses the work on designing a privacy-aware incentive mechanism for mobile crowd sensing applications, under Topic 3. Finally, the summary and future work is presented in Chapter 6.

Next, we give an introduction on the three considered research topics.

1.1 Location Spoofing in Time-of-arrival-based Localization Systems

We consider the *location spoofing detection* problem in a wireless network where the network wants to localize and verify the location of a target node. We assume that the network sink receives some time-of-arrival (TOA) delay measurements from a target node and the location verification system uses a detection test to check if the received delay measurements are spoofed. Many location-based service (LBS) [1, 23] and wireless sensor network (WSN) [3, 24, 25] applications rely on the accurate location information to function correctly.

In a typical range-based TOA-based localization scheme [24, 26, 27], specially deployed *anchors* (or reference nodes) are used to estimate the distance of a target node using the TOA delay measurements. We consider the TOA-based IEEE two-way ranging (TWR) protocol [24, 26–28] where the target node needs to response to the range request packet sent by the anchors. This enables the anchors to estimate their distances from the target by making use of the time-of-arrival/time-of-flight information, which we refer to as the TOA delay measurement.

After collecting some TOA delay measurements, the localization system may use the conventional trilateration (or multilateration) method [17, 24, 26] to estimate the target node's location. However, a malicious target node may spoof the TOA delay measurements received by the anchors to influence its distance estimates, which can lead to an incorrect location estimate. Thus, many location spoofing detection schemes [3, 5, 12–14, 18, 23, 25, 29–31] have been proposed to deal with this threat.

The conventional trilateration method [17, 24, 26] requires at least three or more distance estimates to localize a target node in two-dimension [5, 18, 27]. Otherwise, there may exist ambiguity in the location estimate if there are less than three distance estimates. However, we show that the three or more distance estimates assumption may be relaxed to just two distance estimates. This is possible as prior works simply ignore the existence of inaudible anchors, i.e., the inaudible anchors are completely excluded by the trilateration method.

Our proposed audibility-aware scheme, on the other hand, exploits the implicitly available audibility information to improve the location estimation process. This in turn leads to an improved location spoofing detection rate at essentially no additional cost.

Using the concept of audibility, we develop an *audibility-aware* generalized likelihood ratio test (GLRT) [32] called Enhanced Location Spoofing detection using Audibility (ELSA) to detect location spoofing attacks. The statistical GLRT hypothesis testing technique is a well-recognized approach in the field of statistical signal processing. The GLRT can be used to distinguish between the received TOA delay measurements from an honest and the received measurements from a malicious target. We consider the TOA-based localization system as it is widely used (e.g., in global positioning system (GPS)) and provides the best localization accuracy (e.g., in the range of centimeters for ultra-wide band (UWB) devices [26, 33]) compared to other range-based (e.g., received signal strength (RSS)) and range-free approaches [34]. We consider GPS-denied indoor or urban environments where the GPS measurements are not readily available [27]. We then show that the proposed ELSA significantly outperforms the conventional non-audibility-aware TOA-based approaches in terms of detection rate.

Unlike typical wireless network deployments, the anchors in an IoT environment can be low-cost tags or devices due to their scalability. As such, these limited capability tags do not output any RSS readings. Despite this, our approach is well suited for these scenarios as it derives the implicit audibility information from the received TOA delay measurements. Our approach is also compatible with existing infrastructure-based TOA ranging schemes and does not require additional cryptographic operations or message exchanges between the anchors and the target. To the best of our knowledge, this is the first attempt to incorporate audibility information for location spoofing detection in TOA-based localization systems.

1.2 Traffic Analysis Attacks in Wireless Networks

We consider the *privacy-preserving routing* problem in a wireless network where there exists an adversary who is able to observe all the transmission activities in the entire network.

We assume an adversary that uses a Bayesian traffic analysis method (i.e., the maximum-a-posteriori (MAP) inference method) to identify the communicating source-destination pair.

Wireless networks are vulnerable to *traffic analysis* attacks [35–41] that seek to infer contextual information [40, 42, 43] of the communicating parties (e.g., source-destination identities) from the observed traffic patterns. More worryingly, they are easily executed without raising suspicions in a wireless network as the wireless node transmissions can be passively and stealthy sniffed. Hence, extensive research efforts have been invested in mitigating traffic analysis attacks in wireless networks. A malicious adversary may be interested in learning who is talking to who, at what time intervals, and the duration of the communications in order to infer some other more significant information. For example, an adversary may be interested in determining the period of time a home user is away from home, or determining whether there are unusual activities in a military network, or the adversary may want to track the location and identity of a particular health care patient.

Wireless traffic analysis attacks are different from the conventional cryptographic-based attacks commonly encountered in wired networks. The simple use of cryptography, e.g., encryption alone is insufficient to deter traffic analysis attacks in wireless networks. This is because even if the transmitted information is encrypted, contextual information such as the locations of the source and destination nodes can still be easily inferred from the communication traffic patterns. Typical traffic analysis techniques exploit features such as packet timings [38], packet sizes [44] or packet counts [45] to correlate traffic patterns and compromise user privacy. More advanced traffic analysis techniques include the information theoretic [46] and Bayesian [47] analysis methods, which we focus our attention on.

The most common approaches to mitigate traffic analysis attempts are to: (i) change the physical appearance of each packet at every hop via hop-by-hop encryptions [38, 48, 49], (ii) introduce transmission delays at each transmission hop [36, 50] to decorrelate the communication flows, or (iii) introduce dummy traffic [37, 39, 43, 45, 51–53] to obfuscate the

communication patterns. However, the first two approaches may not be desirable for low-cost or battery-powered wireless networks, e.g., wireless sensor networks as (i) the low-cost nodes may not be able to afford using the computationally expensive encryption operations at each hop, and (ii) introducing delays at each intermediate node may not be effective when there is little traffic in the network.

Therefore, we use the *dummy* traffic approach with probabilistic routing to provide privacy by lowering the adversary's detection rate. Specifically, we consider an adversary that uses the Bayesian maximum-a-posteriori (MAP) inference method and focus on hiding the *source-destination identities* (or *unlinkability* [37, 38, 54]) of each communication. We consider a powerful global adversary that is able to observe node transmissions from the entire network and show that its optimal detection strategy is the MAP estimation method. However, the caveat in using dummy traffic is that it impairs network throughput and other vital network resources. Hence, there is a tradeoff between the amount of additional privacy provided and the amound of additional overhead incurred. To achieve the maximum privacy for a specified overhead constraint, we propose the Optimal Privacy Enhancing Routing Algorithm (OPERA), which uses linear programs (LP) to compute the optimal routing path distribution that minimizes the adversary's detection probability. We show via simulations that our proposed OPERA is significantly better (in terms of lower adversary detection probabilities) than the Uniform and Greedy heuristics, the baseline sink simulation and backbone flooding schemes, and the mutual information minimization scheme.

We also introduce the (k,ϵ)-anonymity property for strict privacy guarantees, which provides a different interpretation of privacy. Next, we formulate a mixed-integer linear program (MILP) to optimize the minimum-cost routing path distributions that achieves the (k,ϵ)-anonymity property. The (k,ϵ)-anonymity property is a "hard" constraint that guarantees privacy for each source-destination pair, i.e., the true source-destination pair is safely hidden among a set of $(k-1)$ or more other distinct source-destination pairs where each pair is just as likely to be the true source-destination pair. Finally, we studied the two different interpretations of privacy (minimizing the adversary's detection rate or achieving (k,ϵ)-anonymity) and

examined their differences under various network topologies. To the best of our knowledge, this is the first work that addresses the privacy-utility tradeoff problem in wireless routing via a statistical decision-making framework that considers a powerful MAP adversary with global observability.

1.3 Incentive Mechanisms for Privacy-aware Mobile Crowd Sensing Applications

We consider the *privacy-aware incentive* problem for mobile crowd sensing (MCS) applications. The mobile crowd sensing platform [55] is an emerging sensing paradigm in the age of Internet of Things (IoT) that replaces the fixed sensing infrastructure (e.g., wireless sensor network (WSN)) and removes its deployment and maintenance costs. The sensing platform can entice the large number of existing mobile smartphone users to contribute sensing data, which are easily obtained via the available sensors built into their smartphones. This allows the sensing platform to estimate some statistics of a spatial event or to conduct spatial regression to predict the sensing data for regions where there are no available data. However, the sensing platform must first design an appropriate incentive mechanism to encourage user participation, e.g., via monetary rewards. More importantly, the sensing platform has to accommodate the individual privacy preferences of privacy-sensitive users.

We consider mobile crowd sensing applications designed for spatial monitoring such as those used for traffic monitoring [56], earthquake detection [57] or noise monitoring [58]. These applications will benefit greatly if the coverage area of their dataset is maximized. Hence, improving the *spatial coverage* of the collected dataset should be one of the main objectives of an incentive mechanism used by spatial monitoring applications. Additionally, current privacy-preserving works such as [22, 59, 60] have attempted to address the user *location privacy* problem in the crowd sensing domain. This is because the privacy issues can easily deter potential users from participating, which in turn reduces the amount of potential data available to the mobile crowd sensing platform.

The location privacy problem has not been fully addressed as existing privacy-preserving schemes that offer location privacy via location or data perturbation are not directly applicable to crowd sensing applications that require specific and true (un-perturbed) location information. For example, it would be unacceptable for a traffic monitoring application if there was a traffic congestion in road X, but due to location or data perturbation, another road Y or a non-congested status was reported respectively. Thus, it is vital for incentive models to address the spatial coverage and location privacy issues concurrently.

An appropriate incentive mechanism to model the hierarchical relationship between the crowdsourcer and the smartphone users is the *Stackelberg (leader-follower) game* model used in [61–63]. In the Stackelberg model, the crowdsourcer (leader) commits a reward strategy that is observed by the smartphone users (followers) who then strategize the amount of data to sell to the crowdsourcer. However, existing Stackelberg incentive models buy data from users independently of their physical locations [64] and do not attempt to improve the spatial coverage of the collected dataset. This limits the utility of the collected dataset, especially for spatial regression purposes.

We propose a privacy-aware Stackelberg incentive model that improves the *spatial coverage* of the collected dataset. Our proposed model is privacy-aware, in that it allows privacy-sensitive users to submit *coarse-grained (or quantized) location* information which could still be useful to the crowdsourcer. We then study the properties of the proposed Stackelberg game analytically and present efficient algorithmic solutions for the privacy-aware incentive problem. Our proposed model does not require a trusted third party for privacy and can protect users against a crowdsourcer who cannot be trusted to anonymize the smartphone users' location information. We show via simulations that our proposed model is superior to two other incentive schemes that maximize a different coverage metric.

Chapter 2

Detecting Location Spoofing in Time-of-arrival-based Localization Systems

We consider the *location spoofing detection* problem in a wireless network where the network sink receives some time-of-arrival (TOA) delay measurements from a target node and uses a detection test to check if the received delay measurements are spoofed. This problem is challenging because the network may only have a small sample of delay measurements to work with. Hence, some works like [13] and [25] make special assumptions such as the existence of hidden anchors to improve the detection rate of the location verification system. Different from these works, we exploit the implicitly available audibility information and formulate a statistical generalized likelihood ratio test (GLRT) to detect the location spoofing attacks. By doing so, we do not require any changes to existing localization systems.

2.1 Introduction to Location Spoofing

In the considered TOA-based localization systems [25, 66, 67], the trilateration (or multilateration) technique [17, 24] is commonly used to fuse three or more range-based measurements to localize a target node. The range-based measurements are collected by specially deployed anchors (or reference nodes). A location spoofing adversary can easily mislead the localization system by manipulating the range-based measurements. In the considered TOA-based localization system, the received range-based measurements are the delay (or time of flight)

The material in this chapter was presented in part in [65].

duration for a wireless packet to travel from the target node to the anchor. Hence, the adversarial target node can introduce an additional delay before sending a TOA ranging packet to trick the anchor into believing that the target node is located further away (from its true location). This may cause its estimated location to be different from its actual location.

2.1.1 Contributions

To the best of our knowledge, this is the first attempt to model and incorporate audibility information to improve location spoofing detection using a statistical approach based on the *missing-not-at-random (MNAR)* [68] concept (explained in Section 2.3).

The key contributions of this work can be summarized as follows:

- We introduce the notion of *audibility* and develop a audibility-aware framework to improve the location estimate of a target node.
- We design an algorithm called Enhanced Location Spoofing Detection Using Audibility (ELSA), which uses an audibility-aware GLRT to detect location spoofing attacks, and prove that it has better detection performance than the conventional non-audibility-aware GLRT.
- We verify the efficacy of ELSA compared to the conventional non-audibility-aware GLRT using both extensive simulations and a real-world experimental dataset.

2.1.2 Notation

We use the following notation in this chapter. Uppercase letters denote random variables and the corresponding lowercase letters their realizations, and bold letters represent vectors. With a slight abuse of notation, we use lowercase $p(x)$ to represent both the probability density function (pdf) and probability mass function (pmf), and uppercase P("event") to represent the probability of an event. The normal pdf is represented by $\mathcal{N}(x;\mu,\sigma^2) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, and the standard normal cumulative distribution function (cdf) by $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}}\, dt$. Lastly,

we use $\mathbb{1}(\cdot)$ to denote the indicator function which equals one if its argument $(\cdot)$ is true, and zero otherwise.

The table of notation used in this chapter can be found in Table 2.1.

Table 2.1: Notation.

$\mathbf{x}_i$	location of the i^{th} anchor.
Θ	location of a target node.
t_i	delay measurement received by anchor i.
W_i	received time delay error where $W_i \sim \mathcal{N}(0, \sigma^2_W)$.
P_i	mean received power of target's signal at anchor i.
ϵ_i	received power error where $\epsilon_i \sim \mathcal{N}(0, \sigma^2_\epsilon)$.
r_i	indicator value that depends on the whether the anchor i receives a delay measurement from the target node [see 2.4].
v_p	signal propagation speed.
η	threshold for the proposed GLRT.

To improve the presentation of the chapter, we present all the lengthy proofs (that occupy more than a page) in Section 2.8.

2.2 Related Work

Location verification schemes have mainly rely on either the TOA or RSS range-based approaches to estimate and verify the location of a target node. In range-based approaches, deterministic geometrical boundaries are often used to decide whether to accept or reject location claim of a target node. For example, Vora *et al.* [69] adopted a geometric approach to detect location spoofing attacks. The authors defined two boundaries for determining acceptance (circular zone) and rejection (polygonal zone) of location claims. All target nodes are assumed to be audible within a circular acceptance zone. However, such deterministic methods do not account for the variance of the naturally occurring observation noise in the received measurements and can introduce false alarms when the observation noise is large.

Several works have relied on cryptographic security protocols and message exchanges to detect location spoofing attacks. For example, the work in [1] proposed a framework for using special witness nodes to validate the location of targets via a cryptographic asserted

location proof protocol. The protocol allows the witness nodes to verify their distances to the target, hence preventing any location spoofing. Next, the work in [18] proposed a similar but distributed cooperative witnesses protocol to verify a target's location through a series of message exchanges. Likewise, the work in [3] proposed a verification method to check if the target lies within a claimed region and whether the claimed location exceeds a reasonable bound. Distance bounding protocols (e.g., [31, 70]) have also been proposed to verify that a target is located within a geometric region from the anchors. This is achieved by a sequence of message exchanges, each containing a random nonce used to bound the distance between the target and the anchors. It is assumed that the target node is in the audible range of the anchors in order to receive the random nonces. However, these works do not statistically model the received TOA measurements, which can introduce false alarms due to the naturally occurring observation noise.

To further improve the location spoofing detection rate, the work in [13] assumed the existence of anonymous beacons to allow the localization system to verify a target's location. Capkun *et al.* [25] further assumed hidden and mobile anchors (i.e., the anchors' locations are not known to the adversary) to verify the location of target nodes via a simple challenge-response protocol. Interestingly, Basilico *et al.* [5] modeled the location verification problem as a game-theoretic non-cooperative two-player game between the anchors and the malicious target to compute the best location to place the anchors.

Different from the above works, the works in [12, 14, 23, 67] use the likelihood ratio test (LRT) approach to verify the target's location in RSS-based localization systems. The authors showed that the LRT approach results in the optimal decision rule for the location verification problem. We adopt the a similar LRT framework for our TOA-based location verification problem and also tackle the additional challenge of having the anchors localize the target themselves in contrast to the prior works, which assume that the LRT test has knowledge of the target's location. Furthermore, we exploit the audibility information in our detection test to improve the location spoofing detection rate.

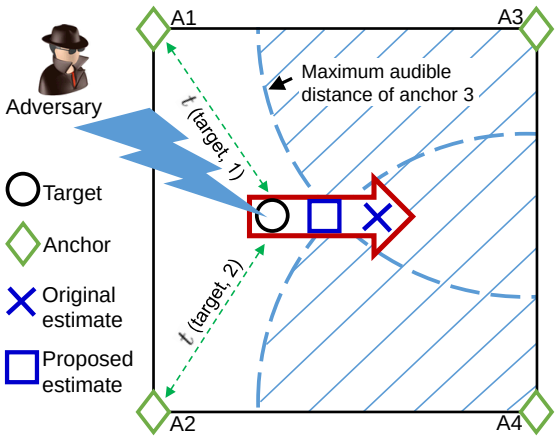


Figure 2.1: Illustration of a location spoofing attack.

2.3 Motivating Example For Proposed Audibility Framework

Before going into the details, we first illustrate with an example of the location spoofing attack and how audibility can be exploited to detect the attacks. Shown in Fig. 2.1 is a room with four anchors (A1, A2, A3, A4), each in the four corners. Suppose that a malicious target node at the left side of the room (denoted by the circle) is in the audible range of two anchors A1 and A2. The target node aims to spoof its location such that it appears (to the location verification system) at the other side of the room (marked with a cross).

If the target is controlled by an adversary, it can add additional delays to increase its TOA delay measurement [4, 5, 17, 29, 31, 70, 71], and hence increase the estimated distance from itself to the two anchors A1 and A2. Otherwise, an external adversary may also selectively jam the wireless channel [72–74] to introduce additional delays to the TOA delay measurements. Note that in actual scenarios, the location estimate may be a small region of equally likely points (see Fig. 2.3) instead of an exact location point as shown in Fig. 2.1 but the concept remains the same. The adversary model is explained in greater detail in Section 2.4.4.

Using the conventional non-audibility-aware approaches, the location verification system will not be able to detect the location spoofing attack as there are insufficient contradictory information to raise suspicions. However, using the additional implicitly available audibility information as input, it is now unlikely that the target is located at the cross since it is not

in the range of the two anchors A3 and A4 at the right side of the room. With the audibility information considered, we are able to detect the location spoofing attack. This is the main idea behind our proposed audibility-aware framework.

We also statistically model the received TOA and RSS measurements, which generalizes the geometric-based location spoofing detection approach [69] by accounting for the naturally occurring observation noise via a Gaussian noise term [see (2.1)] $W_i \sim \mathcal{N}(0, \sigma_W^2)$. The conventional geometric-based approach is therefore a special case of our model where $W_i \sim \mathcal{N}(0,0)$. Therefore, our stochastic model provides a better representation of the real-world wireless conditions by quantifying the probability of being audible and we also account for the naturally occurring observation noise.

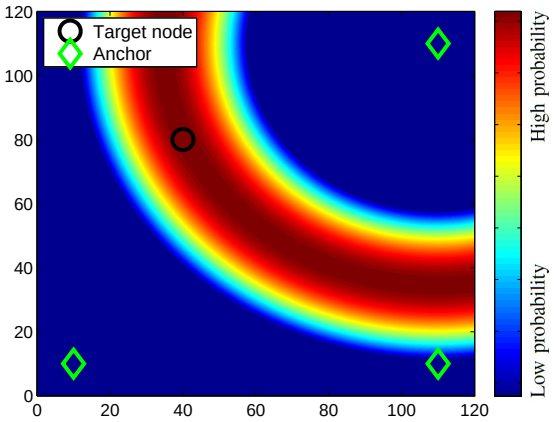
Next, we give an example of how audibility aids in location estimation.

2.3.1 Example: How Audibility Aids in Estimation

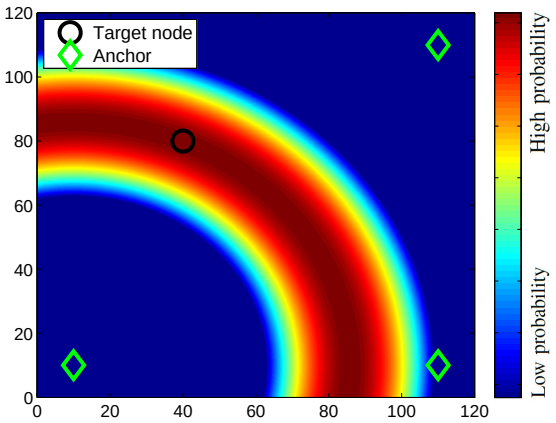
Using the conventional trilateration technique [17, 24, 26] (without utilizing audibility information), we need distance estimates from at least three different non-collinear anchors to localize a target node. Otherwise, there may exist ambiguity when there are only two delay estimates. This can be explained with the aid of Figs. 2.2 and 2.3.

Fig. 2.2 shows the likelihood heatmap of the target's location (under the MAP estimation approach in (2.10)) when information from a single anchor is used. The regions with higher probabilities for the target's location are represented by red. Note that the bottom-right anchor does not receive any delay measurement (not audible) from the target. With only distance estimates from two anchors, the target node may be equally likely to be at two separate regions as seen from the likelihood heat map shown in Fig. 2.3a.

The ambiguity in the location estimate can be significantly reduced when we incorporate the audibility information (see Fig. 2.3b). The bottom-right region that has high probability is now unlikely since there exists a nearby bottom-right anchor that does not receive any delay



(a) TOA likelihood surface using information from the top-right anchor.

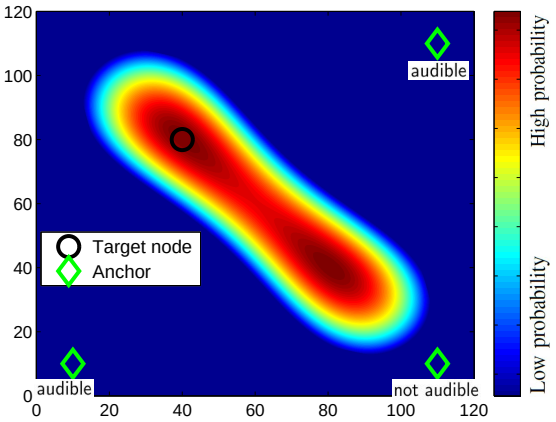


(b) TOA likelihood surface using information from the bottom-left anchor.

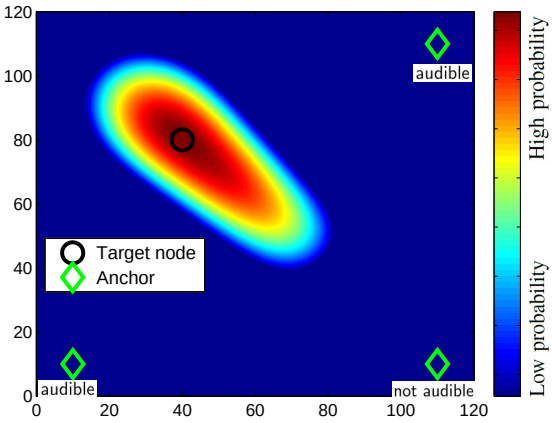
Figure 2.2: Log-likelihood heat map for the location of a target using information from a single anchor.

measurement (not audible). Hence, by taking advantage of the "missing delay measurements" or the inaudibility information, we are able to relax the fundamental three distance estimates assumption of the trilateration technique without using any additional hardware or message exchanges. This leads to an improved accuracy of the TOA localization algorithm at no extra cost since the audibility information is implicitly available to the anchors.

The audibility information can be exploited because the missing delay measurements are *missing not at random (MNAR)* as termed by Rubin in his seminal work in [68] where he developed a statistical framework to account for missing data. To put it differently, the missing measurements are due to the inaudibility of the target. Hence, even the missing delay



(a) Conventional TOA likelihood surface.



(b) TOA likelihood surface with audibility information.

Figure 2.3: Log-likelihood heat map for the location of a target with three anchors (of which two are audible).

measurements can provide additional information on the target's location.

2.4 System Model

In this section, we formally define audibility and describe our connectivity, network, and adversary models. We also provide a brief intoduction on the TOA-based two-way ranging (TWR) distance estimation protocol in Section 2.4.2. Recall that our goal is to design a location spoofing detection test for localization systems using the TWR protocol.

2.4.1 Connectivity Model

We now define audibility and the assumed power loss model.

In order for two nodes A and B to communicate with each other, the transmitted signals should be audible to the other party, i.e., A should be audible to B and vice versa. This is modeled as the widely used power loss model [75] given in Definition 2.1.

Definition 2.1 (Power loss model)**.** *The received signal power by a node A located at $\Theta_A = \begin{bmatrix} x^{(A)} & y^{(A)} \end{bmatrix}$ from a signal sent by node B which is located at $\Theta_B = \begin{bmatrix} x^{(B)} & y^{(B)} \end{bmatrix}$ is given by*

$$P_R = P_T - 10\alpha \log \frac{d(A,B)}{d_0} + \epsilon,$$

where P_T is the transmitted power by node B, α is the path-loss exponent, $d(A,B) := \sqrt{\left(x^{(A)} - x^{(B)}\right)^2 + \left(y^{(A)} - y^{(B)}\right)^2}$ is the Euclidean distance between nodes A and B, d_0 is a reference distance and $\epsilon \overset{i.i.d.}{\sim} \mathcal{N}\left(0, \sigma_\epsilon^2\right)$ represents the shadowing effect.

If node B is able to receive signals transmitted by node A, then the former is said to be to be audible. More formally, we define audibility in Definition 2.2.

Definition 2.2 (Audibility)**.** *Node B is said to be audible to node A if*

$$P_R = P_T - 10\alpha \log \frac{d(A,B)}{d_0} + \epsilon \geq \lambda,$$

where λ is a pre-defined threshold representing the receiver's sensitivity.

2.4.2 Preliminaries: Two-Way Ranging Distance Estimation Protocol

The TWR protocol is a time-of-arrival (TOA)/time-of-flight (TOF) range-based method specified in the IEEE 802.15.4a standard [76]. It is a popular distance estimation method especially in small low-cost UWB devices. The TWR protocol allows two devices to estimate their distances from each other via the TOA delay measurements without needing any time synchronization. Suppose that one device is the anchor while the other device is the target node.

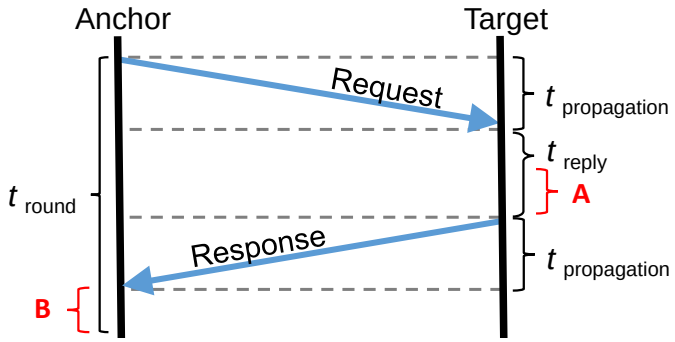


Figure 2.4: Message exchange of the TWR distance estimation protocol [76].

In the two-way ranging (TWR) protocol (see Fig. 2.4), the anchor first sends a range request packet to the target. The target then waits for some known time period t_{reply} before sending a response packet back to the anchor. The value of t_{reply} is assumed to be known to both devices. Assuming that there are no measurement errors, the anchor is able to obtain the round trip time of the two packets t_{round} by subtracting the time it first sent a request packet from the time it received the response packet. Since packet round trip time

$$t_{\text{round}} = 2 \times t_{\text{propagation}} + t_{\text{reply}},$$

the value of the packet propagation delay can be determined using $t_{\text{propagation}} = \frac{t_{\text{round}} - t_{\text{reply}}}{2}$. Subsequently, the distance between the target and the anchor can be computed as follows:

$$d(\text{target}, \text{anchor}) = t_{\text{propagation}} \times v_p,$$

where v_p is the signal propagation speed. No time synchronization between the two devices is required in the TWR protocol as the anchor uses its local clock information to infer distance. This advantage enables the protocol to be used even with low cost RFID tags where time synchronization is not possible [77]. With sufficient range-based distance estimates, we are able to localize a target using the trilateration or multilateration techniques [17, 24].

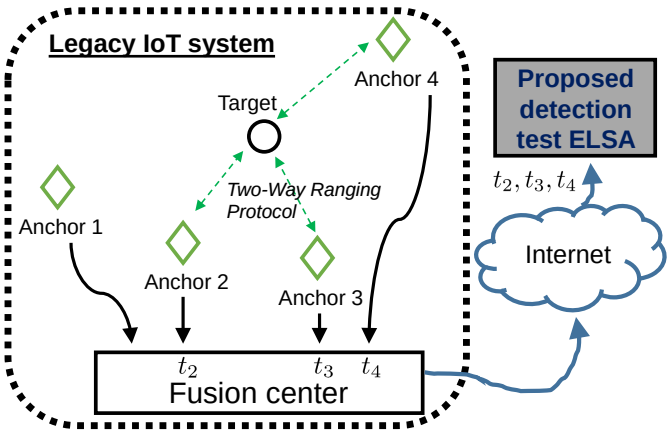


Figure 2.5: System model with a target, multiple anchors, and a fusion center.

2.4.3 Network Model

We consider a scenario where a fusion center (or the network sink) receives some TOA delay measurements from its anchors (also known as reference nodes) and fuses the measurements to verify a target node's location (see Fig. 2.5). The proposed detection test can either be implemented at the fusion center or implemented at a backend server.

We make the following assumptions:

1. Assume a wireless network with n static anchors where the location of the i^{th} anchor is denoted by

$$\mathbf{x}_i = [x_i \; y_i],$$

where its 2D coordinates $\{x_i, y_i\} \in \mathbb{R}$ for $\{i = 1, \ldots, n\}$.

2. The location of the unlocalized target node is denoted by

$$\Theta = [x_\theta \; y_\theta],$$

where its 2D coordinates $\{x_\theta, y_\theta\} \in \mathbb{R}$. Depending on the deployment scenario, we assume that there is a prior $p(\Theta)$ for the target node. A uniform prior can be assigned if the target is equally likely to exist anywhere in the considered region.

3. We consider a scenario where the TWR protocol [76] is used. Each anchor i in the communication range of the target node will receive a delay measurement [24] which can be represented by:

$$t_i = \frac{d(\Theta, \mathbf{x}_i)}{v_p} + W_i, \tag{2.1}$$

where $d(\mathbf{x}_i, \mathbf{x}_j)$ is the Euclidean distance between two locations $\mathbf{x}_i, \mathbf{x}_j$ and is given by

$$d(\mathbf{x}_i, \mathbf{x}_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \tag{2.2}$$

v_p is the signal propagation speed and $W_i \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0, \sigma_W^2)$ is the time delay error.

4. We assume that each anchor i in the communication range of the target node will receive a signal with a mean received power P_i (or received signal strength (RSS)) that is equal or higher than the minimum signal receiving threshold λ. We use the widely accepted log-normal propagation model [24] to estimate the received power of the signal:

$$P_i(\text{dBm}) = P_t(\text{dBm}) - 10\alpha \log \frac{d(\Theta, \mathbf{x}_i)}{d_0} + \epsilon_i \geq \lambda, \tag{2.3}$$

where P_t is the received power from the transmitter at a reference distance d_0 (typically 1 meter), α is the path loss exponent, and $\epsilon_i \overset{\text{i.i.d.}}{\sim} \mathcal{N}(0, \sigma_\epsilon^2)$ is the received power error.

5. If an anchor i does not receive any signal from the target node, we assume that the received signal has a received power P_i that is less than the minimum signal receiving threshold λ, i.e., $P_i < \lambda$.

6. We let r_i be an indicator variable that depends on the whether the anchor i receives a delay measurement from the target node [see 2.3]:

$$r_i = \begin{cases} 1 & \text{if } P_i \geq \lambda, \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

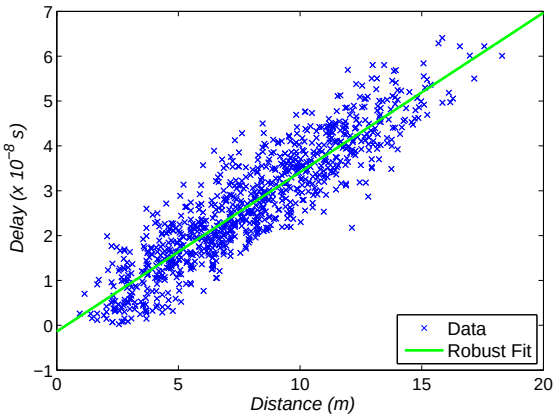


Figure 2.6: TOA delay measurements (from real-world dataset [78]) as a function of distance between two nodes.

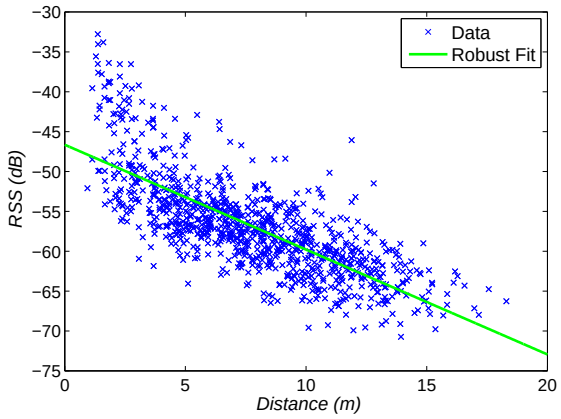


Figure 2.7: RSS measurements (from real-world dataset [78]) as a function of distance between two nodes.

Empirical Support for Chosen TOA and RSS Models

Our chosen TOA and RSS models in (2.1) and (2.3) respectively are supported by the experimental measurements obtained from a real-world dataset [78]. The TOA and RSS measurements are plotted in Figs. 2.6 and 2.7. As seen from the figures, the zero mean Gaussian noise and linearity assumptions are reasonable and provide good representation of the actual experimental data. A Kolmogorov-Smirov (KS) test was also used in [78] to conclude that the Gaussian assumption is valid under a 0.05 significance level.

2.4.4 Adversary Model

We consider both the internal and external adversaries whose main goal is to significantly perturb a target's perceived location by the fusion center $\widehat{\Theta}$ from its true location Θ by *manipulating the response time of the target, thus affecting the TOA delay measurements* received by the anchors as discussed in our motivating example in Section 2.3. Recall from Section 2.4.3 that the delay measurement received at the i^{th} anchor in a non-adversarial environment is given by:

$$t_i = \frac{d(\Theta, \mathbf{x}_i)}{v_p} + W_i.$$

A malicious target can spoof its location by adding a delay δ_i before replying a TWR request message such that the received delay measurement becomes:

$$t_i = \frac{d(\Theta, \mathbf{x}_i)}{v_p} + W_i + \delta_i, \tag{2.5}$$

where we assume $\delta_i \overset{\text{i.i.d.}}{\sim} \mathcal{N}(\mu_\delta, \sigma_\delta^2)$.

The malicious target can insert the delay at point A (as shown in Fig. 2.4) in the TWR protocol while a malicious anchor may insert the delay at point B. The malicious target may fool the anchors by appearing to be closer or further from them. This scenario is accounted by the i.i.d. Gaussian noise model in (2.5). A positive adversarial delay will fool an anchor into believing that the target is further away from its actual position while a negative adversarial delay will make the target appear nearer to the anchor than it really is. The Gaussian model is used for analytical convenience and it accounts for both the adversarial distance enlargement and distance reduction attacks [79].

Since the distance estimate computed by an anchor i is equivalent to:

$$\widehat{d}(\Theta, \mathbf{x}_i) = t_i v_p = \left(\frac{d(\Theta, \mathbf{x}_i)}{v_p} + W_i + \delta_i \right) v_p, \tag{2.6}$$

where $v_p \gg 0$, depending on the carrier frequency, a small value of delay δ_i (e.g., 10^{-9} s) is

sufficient to result in a large difference in the estimated distance (approximately 12.5cm, in the case of 2.4 GHz radio waves). An *external* adversary (who cannot compromise nodes) may also increase the delay measurement by some δ_i, which may not necessarily be non-negative by attacking the PHY layer [70].

2.5 ELSA: Enhanced Location Spoofing Detection Using Audibility

We present the location spoofing detection algorithm called Enhanced Location Spoofing Detection Using Audibility (ELSA), which uses both the TOA delay measurements and the implicitly available audibility information to verify that a target is not spoofing its delay measurements.

The proposed ELSA can be implemented at the fusion center, independent of the protocols used between the anchors and targets (see Fig. 2.5) for data communications, authentication, network registration, etc. The fusion center receives the TOA delay measurements from the anchors directly or via a network sink and does not require any changes to existing legacy IoT systems. This allows compatibility with existing TWR systems. Therefore, the proposed detection test is flexible enough to be used in both scenarios with low power, low-computational power IoT devices and scenarios with high computational-power IoT devices.

2.5.1 Problem Formulation: Optimal Detection Test

One approach to verify that the received TOA delay measurements were not spoofed is to construct a binary hypothesis test to compare the likelihood of the received measurements. The well-known likelihood ratio test (LRT) which is a generalization of the optimal test (justified by the Neyman-Pearson lemma [32, 80]) can be used to detect location spoofing attacks under the two hypotheses:

$$\begin{aligned} &\mathcal{H}_0 : \text{no location spoofing} \\ &\mathcal{H}_1 : \text{location spoofing attempt.} \end{aligned} \tag{2.7}$$

The LRT is commonly used for signal detection and estimation when the signal is corrupted by white Gaussian noise. It can also be applied to our location spoofing detection test. The LRT can be formulated as:

$$\Lambda(\mathbf{t},\mathbf{r}) \triangleq \frac{p(\mathbf{t},\mathbf{r}|\mathcal{H}_1)}{p(\mathbf{t},\mathbf{r}|\mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \tag{2.8}$$

where the bold letters $\mathbf{t}$ and $\mathbf{r}$ represents a vector of n observations $\mathbf{t} = [t_1, \ldots, t_n]$ and $\mathbf{r} = [r_1, \ldots, r_n]$ respectively, and η is a chosen threshold.

Under the Neyman-Pearson lemma [32, 80], the LRT is the most powerful test at each significance level α (false alarm) for a threshold η where $p(\Lambda(\mathbf{t},\mathbf{r}) > \eta|\mathcal{H}_0) = \alpha$. The functions $p(\mathbf{t},\mathbf{r}|\mathcal{H}_0)$ and $p(\mathbf{t},\mathbf{r}|\mathcal{H}_1)$ represent the likelihood functions for the null hypothesis $\mathcal{H}_0$ and alternative hypothesis $\mathcal{H}_1$ respectively.

The LRT for the conventional non-audibility-aware approach excludes the audibility terms: $\Lambda(\mathbf{t}) \triangleq \frac{p(\mathbf{t}|\mathcal{H}_1)}{p(\mathbf{t}|\mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta$.

The likelihood functions of the audibility-aware LRT can be decomposed into:

$$\begin{aligned} p(\mathbf{t},\mathbf{r}|\mathcal{H}_j) &= \int p(\mathbf{t},\mathbf{r}|\Theta,\mathcal{H}_j)\, p(\Theta|\mathcal{H}_j)\, d\Theta \\ &= \int p(\mathbf{t}|\mathbf{r},\Theta,\mathcal{H}_j)\, p(\mathbf{r}|\Theta,\mathcal{H}_j)\, p(\Theta|\mathcal{H}_j)\, d\Theta. \end{aligned}$$

However, a closed-form solution to the above integral is intractable due to the non-linear relationship in $p(\mathbf{t},\mathbf{r}|\Theta,\mathcal{H}_j)$. Hence, we replace the unknown parameters Θ with the maximum-a-posteriori (MAP) estimate $\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}$. If we treat Θ as an unknown random variable, the resulting test will be the generalized likelihood ratio test (GLRT) [32, 80]) given by:

$$\Lambda(\mathbf{t},\mathbf{r}) \triangleq \frac{p(\mathbf{t},\mathbf{r}|\mathcal{H}_1,\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})}{p(\mathbf{t},\mathbf{r}|\mathcal{H}_0,\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \tag{2.9}$$

where we approximate $p(\mathbf{t},\mathbf{r}|\mathcal{H}_j)$ with the MAP estimate $\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}$.

Next, we first derive the MAP estimator for $\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}$ required in (2.9). Subsequently, we substitute

the expression for the MAP estimator into the likelihood function $p(\mathbf{t},\mathbf{r}|\mathcal{H}_j,\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j})$ and derive the likelihood function under the null and alternative hypotheses. With the expressions for the two likelihood functions, we are able to derive the GLRT test statistic used in our proposed ELSA Algorithm (see Algorithm 2.1).

2.5.2 Derivation of MAP Estimate

Assuming that we have prior knowledge of Θ, the MAP estimate [81] for the target's location is given by:

$$\begin{aligned}
\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j} &= \arg\max_{\Theta} p(\Theta|\mathbf{t},\mathbf{r},\mathcal{H}_j) \\
&= \arg\max_{\Theta} p(\mathbf{t},\mathbf{r}|\Theta,\mathcal{H}_j)\,p(\Theta|\mathcal{H}_j) \\
&= \arg\max_{\Theta} p(\mathbf{t}|\mathbf{r},\Theta,\mathcal{H}_j)\,p(\mathbf{r}|\Theta,\mathcal{H}_j)\,p(\Theta|\mathcal{H}_j) \\
&= \arg\max_{\Theta} \prod_{i=1}^{n} \Big[p(t_i|r_i,\Theta,\mathcal{H}_j)\mathbb{1}(r_i=1) + \mathbb{1}(r_i=0) \Big] p(r_i|\Theta,\mathcal{H}_j)\,p(\Theta|\mathcal{H}_j) \\
&= \arg\max_{\Theta} \sum_{i=1}^{n} \Big[\log p(t_i|r_i,\Theta,\mathcal{H}_j)\mathbb{1}(r_i=1) + \log p(r_i|\Theta,\mathcal{H}_j) \Big] + \log p(\Theta|\mathcal{H}_j) \\
&= \arg\max_{\Theta} \sum_{i=1}^{n} \log \mathcal{N}(t_i; \frac{d(\Theta,\mathbf{x}_i)}{v_p} + \delta_i, \sigma_W^2)\mathbb{1}(r_i=1) \\
&\quad + \sum_{i=1}^{n} \log P(r_i=1|\Theta,\mathcal{H}_j)\mathbb{1}(r_i=1) + P(r_i=0|\Theta,\mathcal{H}_j)\mathbb{1}(r_i=0) + \log p(\Theta|\mathcal{H}_j). \qquad (2.10)
\end{aligned}$$

The indicator function $\mathbb{1}(\cdot)$ ensures that the product term is non-zero when no delay measurements are received. We took the log of the likelihood function since it can potentially speed up the computation time as small likelihood values may cause numerical issues for the solver. Since the log is a monotonically increasing function, the point that maximizes the log-likelihood function will also maximum the likelihood function. If no prior knowledge of Θ is available, then a uniform prior may be used instead.

The probability of an anchor i receiving a signal with a RSS value that is greater or equal to the

minimum signal receiving threshold λ is given by:

$$\begin{aligned} P(r_i = 1|\Theta) &= \int_{\lambda}^{\infty} \mathcal{N}(r_i; P_t - 10\alpha \log \frac{d(\Theta, \mathbf{x}_i)}{d_0}, \sigma_\epsilon^2)\, dr_i \\ &= 1 - \Phi\left(\frac{\lambda - P_t + 10\alpha \log \frac{d(\Theta,\mathbf{x}_i)}{d_0}}{\sigma_\epsilon} \right). \end{aligned} \tag{2.11}$$

On the other hand, the probability of an anchor i not receiving a delay measurement is given by:

$$\begin{aligned} P(r_i = 0|\Theta) &= \int_{-\infty}^{\lambda} \mathcal{N}(r_i; P_t - 10\alpha \log \frac{d(\Theta, \mathbf{x}_i)}{d_0}, \sigma_\epsilon^2)\, dr_i \\ &= \Phi\left(\frac{\lambda - P_t + 10\alpha \log \frac{d(\Theta,\mathbf{x}_i)}{d_0}}{\sigma_\epsilon} \right). \end{aligned} \tag{2.12}$$

2.5.3 Derivation of Likelihood Function

With the MAP estimate derived, we now proceed to derive the likelihood function required by the GLRT. The generalized likelihood function can be expressed as:

$$\begin{aligned} & p(\mathbf{t}, \mathbf{r}|\mathcal{H}_j, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}) = p(\mathbf{t}|\mathbf{r}, \mathcal{H}_j, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}) p(\mathbf{r}|\mathcal{H}_j, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}) \\ &= \prod_{i=1}^{n} \left[\mathcal{N}(t_i; \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}, \mathbf{x}_i)}{v_p}, \sigma_W^2) \mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0) \right] \\ &\quad \times \prod_{i=1}^{n} \left[p(r_i = 1|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}) \mathbb{1}(r_i = 1) + p(r_i = 0|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}) \mathbb{1}(r_i = 0) \right] \\ &= \prod_{i=1}^{n} \left[\mathcal{N}(t_i; \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}, \mathbf{x}_i)}{v_p}, \sigma_W^2) \mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0) \right] \\ &\quad \times \prod_{i=1}^{n} \left[1 - \Phi\left(\frac{\lambda - P_t + 10\alpha \log \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}, \mathbf{x}_i)}{d_0}}{\sigma_\epsilon} \right) \right] \mathbb{1}(r_i = 1) + \Phi\left(\frac{\lambda - P_t + 10\alpha \log \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_j}, \mathbf{x}_i)}{d_0}}{\sigma_\epsilon} \right) \mathbb{1}(r_i = 0). \end{aligned} \tag{2.13}$$

With the likelihood function derived, we proceed to derive the test statistic for our GLRT.

2.5.4 Derivation of GLRT Test Statistic

Under the null hypothesis $\mathcal{H}_0$, the likelihood function is simply:

$$p(\mathbf{t},\mathbf{r}|\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}}) = p(\mathbf{t}|\mathbf{r},\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}})\,p(\mathbf{r}|\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}}), \tag{2.14}$$

where

$$p(\mathbf{t}|\mathbf{r},\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}}) = \left[\prod_{i=1}^{n}\mathcal{N}(t_i;\frac{d(\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}},\mathbf{x}_i)}{v_p},\sigma_W^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\right], \tag{2.15}$$

and

$$p(\mathbf{r}|\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}}) = \prod_{i=1}^{n}\left[P(r_i=1|\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}})\mathbb{1}(r_i=1)+P(r_i=0|\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}})\mathbb{1}(r_i=0)\right]. \tag{2.16}$$

Under the alternative hypothesis $\mathcal{H}_1$, the likelihood function is simply:

$$p(\mathbf{t},\mathbf{r}|\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}}) = p(\mathbf{t}|\mathbf{r},\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}})\,p(\mathbf{r}|\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}}), \tag{2.17}$$

where

$$p(\mathbf{t}|\mathbf{r},\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}}) = \prod_{i=1}^{n}\left[\mathcal{N}(t_i;\frac{d(\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}},\mathbf{x}_i)}{v_p}+\mu_\delta,\sigma_W^2+\sigma_\delta^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\right], \tag{2.18}$$

and

$$p(\mathbf{r}|\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}}) = \prod_{i=1}^{n}\left[P(r_i=1|\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}})\mathbb{1}(r_i=1)+P(r_i=0|\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}})\mathbb{1}(r_i=0)\right]. \tag{2.19}$$

We substitute (2.14) and (2.17) into (2.9) to obtain the test statistic:

$$\Lambda(\mathbf{t},\mathbf{r}) = \frac{p(\mathbf{t}|\mathbf{r},\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}})\,p(\mathbf{r}|\mathcal{H}_1,\widehat{\Theta}^{\mathcal{H}_1}_{\text{MAP}})}{p(\mathbf{t}|\mathbf{r},\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}})\,p(\mathbf{r}|\mathcal{H}_0,\widehat{\Theta}^{\mathcal{H}_0}_{\text{MAP}})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta. \tag{2.20}$$

Using the test statistic in (2.20), we propose the following Algorithm 2.1 for the proposed ELSA.

Algorithm 2.1: ELSA algorithm for detecting location spoofing.

ELSA($t_{1,\dots,n}, x_{1,\dots,n}, \eta, v_p, d_0, P_t, \lambda, \mu_\delta, \alpha, \sigma_W^2, \sigma_\epsilon^2, \sigma_\delta^2$) :

Input : Delay measurements received from a target $t_{1,\dots,n}$, positions of the anchors $x_{1,\dots,n}$, threshold η, and the system parameters.

Output : Binary result of the GLRT test.

Compute MAP estimate for $\mathcal{H}_0$ (no location spoofing), $\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}$ via (2.10) (with $\delta_i = 0$).

Compute MAP estimate for $\mathcal{H}_1$ (location spoofing attempt), $\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}$ via (2.10) (with $\delta_i \neq 0$).

Compute likelihood probabilities for the two MAP estimates, $p(\mathbf{t},\mathbf{r}|\mathcal{H}_0, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})$ and $p(\mathbf{t},\mathbf{r}|\mathcal{H}_1, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})$ via (2.14) and (2.17) respectively.

Compute the decision rule $\Lambda(\mathbf{t},\mathbf{r}) = \frac{p(\mathbf{t},\mathbf{r}|\mathcal{H}_1, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})}{p(\mathbf{t},\mathbf{r}|\mathcal{H}_0, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})}$ via (2.20).

Reject $\mathcal{H}_0$ (no location spoofing) if $\Lambda(\mathbf{t},\mathbf{r}) > \eta$. Otherwise, we assume $\mathcal{H}_1$ (location spoofing).

Finally, we prove using the following theorem that ELSA provides better detection rates than the conventional non-audibility-aware GLRT for the same false alarm rate tradeoff.

Theorem 2.1. *For a fixed false alarm rate, the proposed audibility-aware GLRT will have a detection rate P_d^{A} that is higher than the conventional GLRT P_d^{NA} which does not take into account audibility. i.e.,*

$$P_d^{\text{A}} \geq P_d^{\text{NA}}.$$

Proof. See Section 2.8.4. □

2.6 Simulation Results and Discussion

In this section, we evaluated the performance of our proposed detection test ELSA against the conventional non-audibility-aware GLRT (labeled as 'original' in the figures), which does not take into account audibility (similar to the work in [67]) in terms of the location spoofing detection performance. Both synthetic data and data from a real-world dataset (available in [82]) were used in our evaluation. The MATLAB code used to obtain the simulation results can be found in [83]. Unless otherwise stated, the parameters in Table 2.2 were used in our simulations.

Table 2.2: Simulation Parameters.

Parameter	Value (equivalent distance)
TOA noise σ_W	10^{-8} s (3 m)
RSS noise σ_ϵ	$\sqrt{10}$ dBm
Adversary's delay mean μ_δ	4×10^{-8} s (12 m)
Adversary's delay s.d. σ_δ	4×10^{-8} s (12 m)
*Only positive adversary delays $\lvert\delta_i\rvert$ were used.	see (2.5)
Path loss exponent α	3.2
Transmit power P_t at $d_0 = 1$ m	-40 dBm
Signal receiving threshold λ	-102 dBm

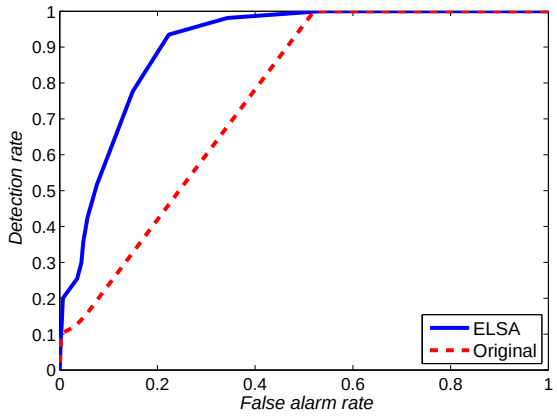


Figure 2.8: ROC curves for three anchors (of which two are audible).

2.6.1 Results from Synthetic Data

We compared the detection performance of the proposed ELSA against the detection performance of the conventional non-audibility-aware GLRT using simulations. We consider the scenario where there exist three anchors at the corners of a 100 m × 100 m area as shown in Fig. 2.3 and the target is selected uniformly at random inside this area (hence, $p(\Theta) = \frac{1}{100} \times \frac{1}{100}$).

We used a grid search with a one meter granularity to search for the optimal target location using the MAP approach (see (2.10)). A finer granularity would improve the accuracy of the schemes, but the improvement will not be significant in our case. Under an adversarial environment, the received delay measurements are adjusted accordingly as discussed in our threat model in Section 2.4.4.

Performance metric: We use the receiver operating characteristic (ROC) curve to compare the detection and false alarm performance of ELSA, against the conventional non-audibility-aware GLRT. For a given decision rule η, the detection rate is given by $P(\Lambda(\mathbf{t},\mathbf{r}) > \eta|\mathcal{H}_1)$, and the false alarm rate is given by $P(\Lambda(\mathbf{t},\mathbf{r}) > \eta|\mathcal{H}_0)$. The ROC curve is obtained by plotting the detection rate of the detection test against the false alarm rate at various η thresholds. The ROC curve allows us to study the tradeoff between the detection rate and the false alarm rate of the two GLRT tests. It is commonly used in the signal detection field to assess the performance of binary classifiers such as our proposed ELSA. For a fixed false alarm rate, we consider the detection test that has a higher detection rate to be the superior one.

ROC Curve Performance

In Fig. 2.8, we plot the ROC curves for scenarios when an adversary adds a positive delay to the delay measurements received by the anchors and the target is on the range of exactly two audible anchors (same anchor locations as Figs. 2.2 and 2.3). The ROC curve for ELSA indicates a significantly better detection performance which demonstrates the superiority of our approach. Despite a slight model mismatch, an adversary that only adds positive delays does not significantly degrade the detection rate of ELSA. The detection performance of the conventional approach however, is lower than ELSA's as it is difficult to detect the attack without making use of additional information from the third anchor. Despite not receiving any observations from the third anchor, this piece of valuable information itself is exploited by ELSA whereas the conventional approach simply ignores this. As it is unlikely that the adversary is able to reduce the propagation delay of a radio wave signal, we only used a positive adversary delay (considered by most works in the literature [5, 17, 31]) in our comparisons.

ROC Curve Performance under Different Conditions

Next, we evaluate the performance of the GLRT tests for different $\mu_\delta, \sigma_\epsilon, \sigma_W$ parameters and randomize the target locations for each iteration. The chosen signal receiving threshold λ includes different inaudible scenarios depending on the target location. In Fig. 2.9, we plot

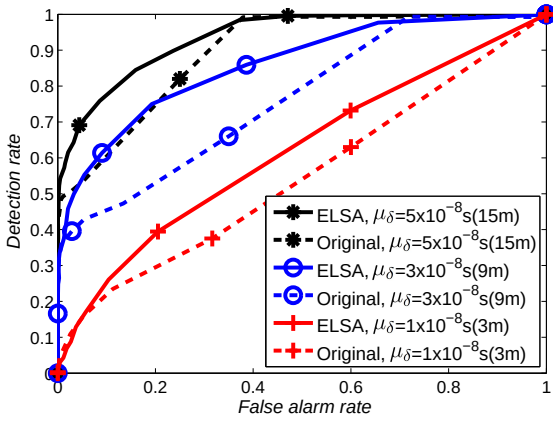


Figure 2.9: ROC curves for different attack mean μ_δ with three anchors.

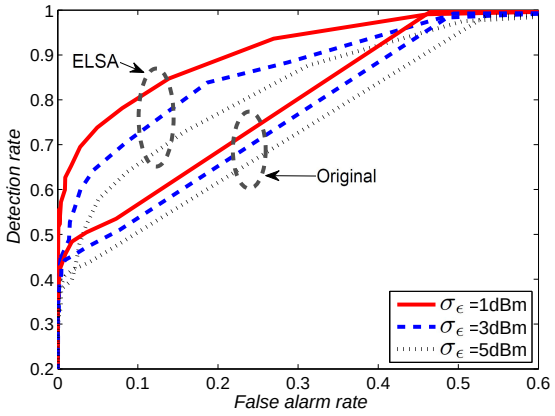


Figure 2.10: ROC curves for different RSS noise variance σ_ϵ^2 with three anchors.

the ROC curves for different adversary delay mean μ_δ values. A higher μ_δ value will perturb the delay measurements further and increase the spoofed distance of the target at the expense of increased detection rate by the GLRT. Similar to Fig. 2.8, the detection performance of the conventional GLRT is worse than ELSA's. As we increase μ_δ to more than 5×10^{-8} s (15 m approximately - take the delay and multiply it with v_p), the detection rate for ELSA goes nearer to 100% and thus we do not plot further.

The impact of obstacles and multipaths can affect the detection performance of the proposed test by increasing the TOA observation noise variances [78]. Similarly, the RSS variances will also increase due to the shadowing and multipath. In Figs. 2.10 and 2.11, we vary the RSS noise variance σ_ϵ^2 and TOA noise variance σ_W^2 respectively to verify that the proposed ELSA can still

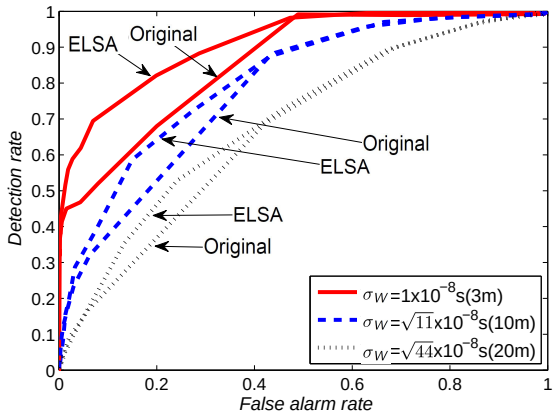


Figure 2.11: ROC curves for different TOA noise variance σ_W^2 with three anchors.

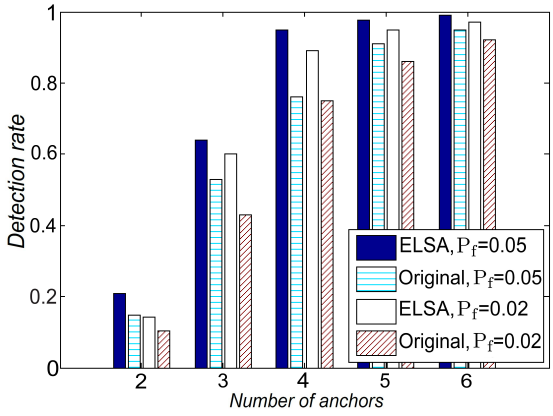


Figure 2.12: Detection rates for different number of anchors (synthetic data) with fixed false alarm rates $P_f = 0.02$ and $P_f = 0.05$.

function correctly under large noise variances. In Fig. 2.10, we vary the RSS noise variance σ_ϵ^2 and verify that the proposed ELSA can still function correctly under large noise variances. Note that the performance of the conventional non-audibility-aware GLRT is largely unaffected by the RSS noise variance since it does not make use of the RSS information. However, the performance of ELSA depends on the quality of the received RSS readings, which affects the audibility information.

In Fig. 2.11, we vary the TOA noise variance σ_W^2. The detection rates for both tests drops as σ_W^2 increases because the adversary's delay is covered by in the TOA observation noise. Hence, the impact of the attack also drops when the σ_W^2 is high. Next, we increase the number of deployed anchors and plot the detection performance in Fig. 2.12 for fixed false alarm rates.

We placed an anchor at each corner of the 100 m × 100 m area and another two anchors in the middle. Similarly, the detection rate of the conventional approach is less than the proposed ELSA's as it does not account for audibility. However, the detection performance for both tests will improve with diminishing returns as the number of anchors increases.

In the event where a malicious node colludes with another node to create a fake audibility condition, the malicious node may either appear to be closer or further to some anchors. However, our existing threat model, which accounts for an i.i.d. adversarial delay will be able to detect the location spoofing attempt due to the inconsistency in the TOA delay measurements and RSS readings. For jamming scenarios, an adversary may be able to fool the detection test into having a false alarm but he is still unable to successfully spoof his location which is the main goal of the location spoofing detection test. However, with the emergence of the Ultra Wide Band (UWB) technology, the threat of jamming attacks have been reduced. An UWB IoT chip marker (e.g., [84]) have even claimed that their devices are immune to multipath interference.

2.6.2 Results from Real-World Dataset

We adopt a real sensor network TOA and RSS measurements dataset used in Patwari *et al.*'s works [78, 85] to validate our proposed audibility framework. The considered network consisted of 44 sensor nodes distributed in an office area in Motorola Labs' Florida Communications Research Lab, in Plantation, FL. Both TOA and RSS measurements were recorded between each sensor node and a high signal-to-noise ratio (SNR) was maintained throughout the experiment to ensure the reliability of the recorded data. Additional implementation details can be found in the Patwari *et al.*'s paper [78] and the dataset is available from the author's website [82].

We selected the minimum signal receiving threshold λ such that there are inaudible scenarios and evaluated the performance of ELSA and the conventional approach under various scenarios. We used three of the anchors (node numbers 10, 35, 44) as used by the original authors

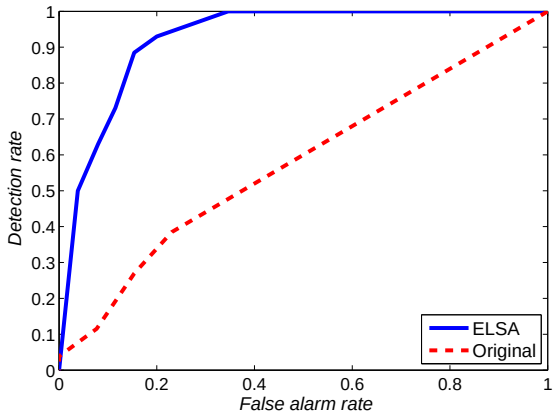


Figure 2.13: ROC curves with $\lambda = -61$ dBm and 41 different target locations (real-world dataset) and three anchors.

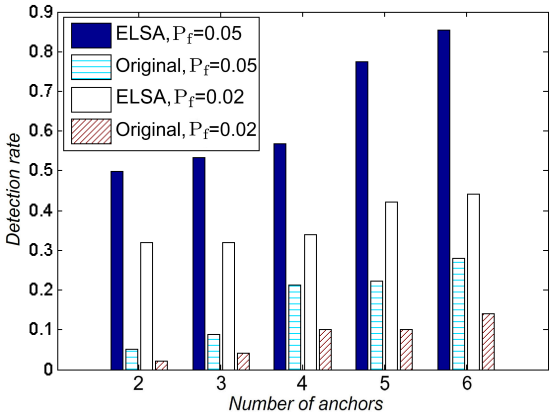


Figure 2.14: Detection rates for different number of anchors (real-world dataset) with $\lambda = -61$ dBm for false alarm rates $P_f = 0.02$ and $P_f = 0.05$.

and an adversary mean of $\mu_\delta = 1.5 \times 10^{-8}$ s (4.5 m approximately). The anchors are located at the corners of the testbed.

ROC Curve Performance:

In Fig. 2.13, we plot the ROC curves for $\lambda = -61$ dBm. The chosen scenario includes a good mix of different numbers of audible anchors and highlights the superiority of ELSA compared to the conventional GLRT. For a fixed false alarm rate, ELSA has a significantly higher detection rate. The ROC curve for the conventional GLRT however, is closer to the diagonal line (not drawn) at low false alarm rates which indicates its poorer detection rate trade-off. A higher μ_δ

parameter will lead to a steeper ROC curve for both schemes with the proposed scheme still being superior. In Fig. 2.14, we vary the number of deployed anchors and plot the detection rates of the tests for a fixed false alarm rate. Note that the relative detection improvements of ELSA is significantly better that the relative detection improvements taken from the synthetic results in Fig. 2.12. This could be due to the limited target locations and their clustered distribution in the dataset whereas in our simulation, we uniformly picked the location of each target in each iteration.

2.7 Conclusion and Future Work

In this chapter, we introduced a new audibility-based framework for detecting location spoofing attacks in TOA-based localization systems. We showed an example of how the conventional TOA-based detection method may not be able to detect location spoofing attacks especially during inaudible scenarios and developed an audibility-aware detection test called ELSA to overcome the problem. The proposed ELSA is able to overcome inaudible scenarios and improve its detection rate by exploiting the implicitly available audibility information. In addition, we have also demonstrated that ELSA has a better detection performance compared to the conventional non-audibility-aware GLRT using experimental results from both synthetic data and a real-world dataset. ELSA also accommodates usage of low-cost IoT devices and lessens the need to deploy a dense network of anchors. This makes ELSA attractive and practical compared to existing protocols that require multiple message exchanges and even hidden anchors.

A future research direction would be to investigate other deployment environment-specific TOA, RSS-based statistical models to further improve ELSA's detection performance. It would also be interesting to design a detection test that accounts for an adversarial target node using directional antennas.

2.8 Proofs

2.8.1 GLRT Test Statistic without Audibility Considerations

Consider the case where only l out of the n deployed anchors receive a delay measurement from the target. Under the null hypothesis $\mathcal{H}_0$, the likelihood function is simply

$$p(\mathbf{t}|\mathcal{H}_0, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}) = \prod_{i=1}^{l} \mathcal{N}(t_i; \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}, \mathbf{x}_i)}{v_p}, \sigma_W^2). \tag{2.21}$$

Under the alternative hypothesis $\mathcal{H}_1$, the likelihood function is given by

$$p(\mathbf{t}|\mathcal{H}_1, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}) = \prod_{i=1}^{n} \mathcal{N}(t_i; \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}, \mathbf{x}_i)}{v_p} + \mu_\delta, \sigma_W^2 + \sigma_\delta^2). \tag{2.22}$$

We obtain the test statistic

$$\begin{aligned}
\Lambda(\mathbf{t}) &= \frac{p(\mathbf{t}|\mathcal{H}_1, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})}{p(\mathbf{t}|\mathcal{H}_0, \widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})} \\
&= \frac{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)} \exp\{-\frac{1}{2(\sigma_W^2+\sigma_\delta^2)}(t_i - \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}, \mathbf{x}_i)}{v_p})^2\}}{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi}\sigma_W} \exp\{-\frac{1}{2\sigma_W^2}(t_i - \frac{d(\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}, \mathbf{x}_i)}{v_p})^2\}} \\
&\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta.
\end{aligned} \tag{2.23}$$

2.8.2 Derivation of Detection and False Alarm Probabilities without Audibility Considerations

We denote the distance-related term as

$$\psi_i = \frac{d(\Theta, \mathbf{x}_i)}{v_p}. \tag{2.24}$$

We obtain the test statistic which does not take into account audibility as follows (see Section 2.8.1):

$$\begin{aligned}&\Lambda(\mathbf{t})\\&= \frac{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)} \exp\{-\frac{1}{2(\sigma_W^2+\sigma_\delta^2)}(t_i-\psi_i-\mu_\delta)^2\}}{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi}\sigma_W} \exp\{-\frac{1}{2\sigma_W^2}(t_i-\psi_i)^2\}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta.\end{aligned} \tag{2.25}$$

Taking the logarithm on both sides, we obtain (2.26).

$$\begin{aligned}\Lambda(\mathbf{t}) &= \sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} - \sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}\sigma_W} + \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2}\\
&= \ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} + \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2}\\
&= \ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} + \sum_{i=1}^{l} \frac{(\sigma_W^2+\sigma_\delta^2)(t_i^2+\psi_i^2-2t_i\psi_i) - \sigma_W^2(t_i^2+\mu_\delta^2+\psi_i^2-2\psi_i t_i-2t_i\mu_\delta+2\psi_i\mu_\delta)}{2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)}\\
&= \ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} + \sum_{i=1}^{l} \frac{\sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i + \sigma_\delta^2\psi_i^2 - 2\psi_i\mu_\delta\sigma_W^2 - \mu_\delta^2\sigma_W^2}{2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta\end{aligned}$$

Next, we shift some terms over to the RHS,

$$\begin{aligned}&\sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\ln\left(\frac{\eta(\sigma_W+\sigma_\delta)}{\sigma_W}\right) + \sum_{i=1}^{l} 2\psi_i\mu_\delta\sigma_W^2 + \mu_\delta^2\sigma_W^2 - \sigma_\delta^2\psi_i^2\\
&\sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma.\end{aligned} \tag{2.26}$$

Now, let $Z = \sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i$ and γ be the threshold. The detection probability for the non-audibility-aware GLRT is given by

$$P_{d|\psi}^{\mathrm{NA}} = P(z>\gamma|\mathcal{H}_1,\psi) = \int_\gamma^\infty p(z|\mathcal{H}_1,\psi)dz, \tag{2.27}$$

and the false alarm probability is given by

$$P_{f|\psi}^{\mathrm{A}} = P(z>\gamma|\mathcal{H}_0,\psi) = \int_\gamma^\infty p(z|\mathcal{H}_0,\psi)dz. \tag{2.28}$$

2.8.3 Derivation of Detection and False Alarm Probabilities with Audibility Considerations

From the test statistic derived in (2.20), we obtain:

$$\begin{aligned}
&\Lambda(\mathbf{t},\mathbf{r}) \\
&= \Bigg(\prod_{i=1}^{n} \mathcal{N}(t_i;\psi_i+\mu_\delta,\sigma_W^2+\sigma_\delta^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0) \\
&\quad \times \prod_{i=1}^{n} \Big[P(r_i=1|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})\mathbb{1}(r_i=1) \\
&\qquad + P(r_i=0|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1})\mathbb{1}(r_i=0) \Big] \Bigg) \\
&\Big/ \Bigg(\prod_{i=1}^{n} \mathcal{N}(t_i;\psi_i,\sigma_W^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0) \\
&\quad \times \prod_{i=1}^{n} \Big[P(r_i=1|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})\mathbb{1}(r_i=1) \\
&\qquad + P(r_i=0|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0})\mathbb{1}(r_i=0) \Big] \Bigg) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta.
\end{aligned} \tag{2.29}$$

We further let $\psi_i' = \frac{d(\Theta,\mathbf{x}_i)}{d_0}$ and $\mu' = \frac{\mu_\delta}{d_0}$ to obtain the following audibility related equations under $\mathcal{H}_0$:

$$\begin{aligned}
P(r_i=0|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}) &= \Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right), \\
P(r_i=1|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_0}) &= 1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right).
\end{aligned} \tag{2.30}$$

Under $\mathcal{H}_1$, the adversary adds additional delays to the delay measurements such that the estimated distance to an anchor will be enlarged if the anchor receives a measurement and decreased if there is an inaudible scenario. The latter is due to the fact that the estimated target location will tend to be closer towards the inaudible anchors as illustrated in Fig. 2.1. As such, we obtain:

$$\begin{aligned}
P(r_i=0|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}) &= \Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right), \\
P(r_i=1|\widehat{\Theta}_{\text{MAP}}^{\mathcal{H}_1}) &= 1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right).
\end{aligned} \tag{2.31}$$

Substituting the above audibility terms into (2.29) and taking logarithm on both sides, the test statistic becomes

$$\begin{aligned}
\Lambda(\mathbf{t},\mathbf{r}) &= \sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} \\
&+ \sum_{i=1}^{l} \ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right) \\
&+ \sum_{i=l+1}^{n} \ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right) \\
&- \left[\sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}\sigma_W} - \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2}\right. \\
&+ \sum_{i=1}^{l} \ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right) \\
&\left.+ \sum_{i=l+1}^{n} \ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right] \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta.
\end{aligned} \tag{2.32}$$

Next, we simplify and rearrange the terms to get

$$\begin{aligned}
&\Lambda(\mathbf{t},\mathbf{r}) \\
&= \ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} + \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2} \\
&+ \left[\sum_{i=1}^{l} \ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right)\right. \\
&+ \sum_{i=l+1}^{n} \ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right) \\
&- \sum_{i=1}^{l} \ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right) \\
&\left.- \sum_{i=l+1}^{n} \ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right] \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta.
\end{aligned} \tag{2.33}$$

Finally, we obtain

$$\begin{aligned}
\Lambda(\mathbf{t},\mathbf{r}) &= \ln\frac{\sigma_W}{(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l}\frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} + \sum_{i=1}^{l}\frac{(t_i-\psi_i)^2}{2\sigma_W^2} \\
&\quad + \sum_{i=1}^{n}\Xi_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} 2\sigma_W^2\ln\eta, \\
&\sum_{i=1}^{l}\sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i + 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\Xi_i \\
&\quad \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\ln\left(\frac{\eta(\sigma_W+\sigma_\delta)}{\sigma_W}\right) \\
&\quad + \sum_{i=1}^{l} 2\psi_i\mu_\delta\sigma_W^2 + \mu_\delta^2\sigma_W^2 - \sigma_\delta^2\psi_i^2, \\
&\sum_{i=1}^{l}\sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i + 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\Xi_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma.
\end{aligned} \tag{2.34}$$

where Ξ_i is some function of the audibility terms (fourth term of (2.33) in [.] brackets) and is independent of the delay measurements $\mathbf{t}$. Using the same $Z = \sum_{i=1}^{l}\sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i$ and γ as the previous Section 2.8.2, and let $\Xi = 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\Xi_i$, the detection probability for the audibility-aware GLRT is given by

$$\begin{aligned}
P_{d|\psi}^{\mathrm{A}} &= P(z+\Xi>\gamma|\mathcal{H}_1,\psi) \\
&= \int_\gamma^\infty p(z+\Xi|\mathcal{H}_1,\psi)dz,
\end{aligned} \tag{2.35}$$

and the false alarm probability is given by

$$\begin{aligned}
P_{f|\psi}^{\mathrm{A}} &= P(z>\gamma|\mathcal{H}_0,\psi) \\
&= \int_\gamma^\infty p(z|\mathcal{H}_0,\psi)dz,
\end{aligned} \tag{2.36}$$

as $\Xi = 0$ under $\mathcal{H}_0$ due to the audibility terms being canceled out by each other when $\mu_\delta = 0$.

2.8.4 Proof of Theorem 2.1

We let the distance related terms $\psi_i = \frac{d(\Theta,\mathbf{x}_i)}{v_p}$, $\psi_i' = \frac{d(\Theta,\mathbf{x}_i)}{d_0}$, and $\mu' = \frac{\mu_\delta}{d_0}$. It can be shown that the detection and false alarm rates for the conventional GLRT without audibility considerations

are given by

$$P_{d|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} p(z|\mathcal{H}_1,\psi)dz \text{ and } P_{f|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} p(z|\mathcal{H}_0,\psi)dz,$$

respectively (see Section 2.8.2), where γ is a threshold, and l is the number of received delay measurements. On the other hand, the detection and false alarm rates for the proposed audibility-aware GLRT are given by

$$P_{d|\psi}^{\mathrm{A}} = \int_{\gamma}^{\infty} p(z+\Xi|\mathcal{H}_1,\psi)dz \text{ and } P_{f|\psi}^{\mathrm{A}} = \int_{\gamma}^{\infty} p(z|\mathcal{H}_0,\psi)dz,$$

respectively (see Section 2.8.3) where the term Ξ (from (2.34)) consists of the audibility-related probabilities. Note that the false alarm rates for both cases are the same:

$$P_{f|\psi}^{\mathrm{A}} = P_{f|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} p(z|\mathcal{H}_0,\psi)dz.$$

Hence, it can be seen that for a fixed false alarm rate $P_{f|\psi}$, the detection rates

$$P_{d|\psi}^{\mathrm{A}} \geq P_{d|\psi}^{\mathrm{NA}},$$

if $\Xi \leq 0$ holds since the complementary cdf function in both $P_{d|\psi}^{\mathrm{A}}$ and $P_{d|\psi}^{\mathrm{NA}}$ is a non-increasing function.

Suppose that $\Xi \leq 0$ and $\mu_\delta > 0$ (which is true in our model). From (2.34), the Ξ term can be expressed as (2.37).

$$\begin{aligned}\Xi =& 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\left[\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right)+\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)\right.\\ &\left.-\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right)-\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right].\end{aligned} \tag{2.37}$$

Next, we simplify the equation to obtain:

$$\Xi = \sum_{i=1}^{l} \ln \frac{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)}{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} + \sum_{i=l+1}^{n} \ln \frac{\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)}{\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} \leq 0. \tag{2.38}$$

Since $\mu_\delta > 0$, then $\mu' = \frac{\mu_\delta}{d_0} > 0$ as $d_0 > 0$. Because the logarithm function is strictly increasing for positive inputs, we have

$$\Phi\left(\log((\psi_i' - \mu')^+)\right) < \Phi\left(\log(\psi_i')\right) < \Phi\left(\log(\psi_i' + \mu')\right).$$

Note that $(\psi_i' - \mu')^+$ is strictly positive as it is not possible to receive a negative delay. Similarly, this implies that

$$\frac{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)}{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} < 1,$$

and

$$\frac{\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)}{\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} < 1.$$

Since the natural logarithmic function always has a negative value when the inputs are less than 1 and Ξ consists of the summation of negative terms, hence, the statement $\Xi \leq 0$ must be true and $P_{d|\psi}^{\mathrm{A}} \geq P_{d|\psi}^{\mathrm{NA}}$.

Subsequently, we can marginalize $P_{d|\psi_i}$ over all possible ψ_i values to obtain

$$P_d = \int P_{d|\psi_i} \times p(\psi_i)\, d\psi_i.$$

Therefore, for a fixed P_f, the following inequalities hold:

$$P_d^{\mathrm{A}} \geq P_d^{\mathrm{NA}},$$

since their equivalent representations,

$$\begin{aligned}&\int_{\psi}\int_{\gamma}^{\infty} p(z+\Xi|\mathcal{H}_1,\psi)\,p(\psi_i)\;dz d\psi_i \\ &\geq \int_{\psi}\int_{\gamma}^{\infty} p(z|\mathcal{H}_1,\psi)\,p(\psi_i) dz d\psi_i,\end{aligned}$$

where the following has already been proven to be true:

$$\int_{\gamma}^{\infty} p(z+\Xi|\mathcal{H}_1,\psi) dz \geq \int_{\gamma}^{\infty} p(z|\mathcal{H}_1,\psi) dz.$$

Hence, we complete the proof. □

Chapter 3

Mitigating Traffic Analysis Attacks in Wireless Networks

We consider the *privacy-preserving routing* problem in a wireless network where a Bayesian maximum-a-posteriori (MAP) adversary is able to observe all the transmission activities in the entire network. We focus on protecting the privacy of the source-destination identities (see Definition 3.2) by designing a *probabilistic privacy-preserving* routing protocol to minimize *the probability of an adversary correctly guessing the source-destination identities*. In addition, the routing scheme should consider the adversary's observation model $p(\boldsymbol{y}|\boldsymbol{x})$ while computing a (routing) path distribution $p(\boldsymbol{x}|w)$ that serves the source-destination pair w. The set of transmission paths $\mathcal{X}$ is related to the set of observed node transmissions $\mathcal{Y}$ via the adversary's observation model $p(\boldsymbol{y}|\boldsymbol{x})$. Ideally, knowledge of $\boldsymbol{y}$ should not immediately reveal w, e.g., there should be a many-to-one mapping from w to $\boldsymbol{y}$.

The privacy-preserving routing problem has typically been addressed in the literature using heuristic methods [43, 52, 87]. While the heuristic solutions may be easy to compute, their provided privacy level may not be optimal for every network topology. Hence, we propose an optimization approach to compute the optimal routing path distribution for the privacy-preserving routing problem.

The material in this chapter was presented in part in [65, 86].

3.1 Introduction to Traffic Analysis

We first describe the characteristics of a privacy compromising adversary (with respect to wireless networks) before elaborating on the traffic analysis techniques available to the adversary. Generally, a traffic analysis adversary can be characterized by the following properties [36, 40, 43]:

- *Global or local observability.* A global observability adversary is one that can observe all the transmission activities in the entire network. This can be achieved if the adversary is able to deploy his own network of sniffers to observe the network traffic or has a few sniffers with high-gain antennas. The local observability adversary on the other hand, can only observe the transmission activities in localized parts of the network. However, some authors [51, 52] have assumed that the local adversary is mobile and can trace each transmission packet hop-by-hop to its source or destination node.

- *The active or passive adversary.* An active adversary is one that may actively alter the network transmission traffic, e.g., inject, modify, or drop packets or by violating the implemented communication protocols of the compromised nodes. A passive adversary on the other hand, simply passively eavesdrops the transmitted packets without disrupting the network traffic. Since the passive adversary simply (silently) monitors the network traffic, it is not possible to detect such an adversary other than placing physical security guards or surveillance cameras to visually scan the entire network for suspicious sniffing devices.

- *The internal or external adversary.* An internal adversary is one that has the ability to compromise nodes in the network. By doing so, the internal adversary is able to view encrypted information (including the internally stored encryption keys), send probe messages to compromise privacy, participate in voting activities, and has access to all routing and network related information. An external adversary on the other hand, does not have access to any encrypted data but is still able to replay transmitted packets or

selectively drop acknowledgment packets. All adversaries are able to view the packet header information if it is unencrypted.

After sniffing the transmission traffic patterns in the network, the adversary may use the following traffic analysis techniques commonly considered in the literature to compromise privacy:

- *Content correlation.* The adversary is able to acquire information about the source or destination node from the packet headers and payload if no encryption is applied. Even if the packets are encrypted, they are still distinguishable from the other packets if the encrypted contents do not change while in transit. Such attacks can be easily prevented via hop-by-hop encryptions [88], which changes the physical appearance of the transmitted packet (in terms of bytes) at every hop.

- *Size correlation.* The adversary is able to easily identify and distinguish between individual packets if they are of different packet sizes. A simple countermeasure would be to pad each transmitted packet into a common size [38, 44, 88].

- *Time correlation.* The adversary correlates the packet transmission times of each node and traces the packets hop-by-hop from its source to its destination. The intuition here is that under normal scenarios, each intermediate forwarder will forward a packet towards its destination without adding additional delay or packet mixing. Privacy can be enhanced when each forwarder node adds a random delay before transmitting the packet [36, 38] or route the packets to fake destinations [35]. The time correlation attack is simple to conduct and effective in compromising privacy. Hence, it is the most considered attack in prior works and widely studied in many Internet anonymity protocols [88].

- *Rate monitoring.* The adversary counts the number of packet transmissions executed by each node in a region for a period of time. If the nodes are communicating to a common destination node, e.g., the sink node, then the latter should be located in a region of

higher packet transmissions, commonly referred to as a hotspot. One approach to mitigate this attack is to introduce dummy traffic to create fake hotspots and fool the adversary [35, 36].

- *Statistical and information theoretic analysis.* Other than the above-mentioned attacks, other application specific statistical and information theoretic traffic analysis techniques [16, 36, 44, 89, 90] have also been used in the literature. Most of these attacks make use of the timing-based information and can be considered as advanced time correlation or simply flow correlation attacks.

- *Bayesian analysis.* The Bayesian inference techniques such as the one applied in [47] exploits prior knowledge of the communication patterns and provides the adversary with a posterior distribution on the communicating pairs. The adversary can then proceed to estimate the most likely communicating pair. One approach to mitigate the Bayesian analysis is to manipulate the likelihood function such that the posterior distribution is uniformly distributed.

3.1.1 Contributions

To the best of our knowledge, this is the first work that addresses the privacy-utility tradeoff problem in wireless routing via a statistical decision-making framework that considers a powerful MAP adversary with global observability.

The key contributions of this work can be summarized as follows:

- We propose Optimal Privacy Enhancing Routing Algorithm (OPERA), which uses a statistical decision-making framework to optimize the privacy-utility trade-off for routing in wireless networks against a global and informed adversary using the Bayesian MAP estimation strategy. We then formulate linear programs to efficiently compute the optimal privacy-preserving paths under the lossless and lossy adversarial models, given a privacy budget.

- We study the choice of our objective function (minimizing the adversary's detection probability) and how it differs from minimizing mutual information or using the Uniform and Greedy heuristics.

- We propose a low-complexity approximation method to compute the optimal privacy-preserving paths under the lossy adversarial model.

- We demonstrate via simulations that privacy does not necessarily depend on the number of receivers as the communication patterns are more important. We also evaluated the proposed OPERA in several different network topologies, including two real-world testbeds.

3.1.2 Notation

The table of notation used in this chapter can be found in Table 3.1.

Table 3.1: Notation.

$\mathcal{G}$	connected hypergraph representing the network.
$\mathcal{V}$	set of nodes in the network.
$\mathcal{H}$	set of all (directed) hyperarcs in the network.
$h = (s, \mathcal{R})$	hyperarc which represents a source-receivers pair where $s \in \mathcal{V}$ is the source node and $\mathcal{R} \subseteq \mathcal{V}$ is a non-empty set of receiver nodes adjacent to s.
$w \triangleq (u, v)$	source-destination pair where $u \in \mathcal{V}$, $v \in \mathcal{V}$ are the source and destination nodes respectively.
$\boldsymbol{x} = (h_1, h_2, \ldots)$	actual transmission path.
$\boldsymbol{y}$	observed path where $\boldsymbol{y}$ is a subvector of $\boldsymbol{x}$.
$\mathcal{X}$	set of all possible paths $\boldsymbol{x}$ in the network.
$\mathcal{X}^w$	set of all possible paths $\boldsymbol{x}$ that serve w.
c_h	cost (e.g., transmission cost) for using hyperarc h.
α	probability of not observing a given transmission $h \in \boldsymbol{x}$.

3.2 Related Work

Traditional anonymity enhancing techniques like onion routing [49] and mix-net [48] allow users to communicate anonymously over the wired Internet network. These techniques

mostly rely on packet encryption and randomized routing from the source to the destination to hide sensitive information (e.g., the identities of the communicating parties) from eavesdropping adversaries. The onion routing offers privacy protection from an adversary with only local observability while the mix-net provides privacy even against adversaries with global observability via special mix nodes. However, the onion routing technique is more prevalent due to its lower latency which makes it practical. While the local observability assumption is valid in the large-scale Internet, it may not hold for the relatively smaller wireless networks, i.e., wireless networks are more vulnerable to traffic analysis from a global adversary. Due to the wireless broadcast medium, it is possible for an adversary to passively eavesdrop on all transmissions from a wireless node without being detected.

To address the privacy concerns, the field of *location privacy* emerged with the first location privacy problem (specifically the source-location privacy problem) for wireless networks being studied by Ozturk *et al.* [51]. The authors used the dummy packet approach to provide privacy and proposed several flooding-based routing techniques, including the randomized phantom flooding routing to prevent an adversary with local observability from tracing a transmitted packet to its source node. Since the flooding-based solution incurs excessive network resources, several other works [91, 92] have built on the randomized routing strategy and improved the effectiveness and efficiency of the privacy-preserving routes. As there exists a vast literature in the source-location privacy field, we refer the reader to the survey on source-location privacy in [40].

Subsequently, Jian *et al.* [52] proposed a routing protocol to provide receiver-location privacy against timing-based packet tracing attacks. The proposed protocol used multipath routing to decorrelate the incoming and outgoing traffic at each forwarder node. However, the authors considered an adversary with local observability and thus, the protocol is not secure against a stronger global observability adversary that can observe transmissions in the entire network. Mehta *et al.* [43] considered the global adversary and proposed the periodic collection and source simulation (dummy sources) techniques for source location privacy and the backbone flooding and sink simulation (dummy sinks) techniques for receiver location privacy. A loose

approximation for the lower bound on the communication overhead needed for achieving a given level of location privacy was also provided. However, the proposed solution is still heuristic in nature and may not provide the optimal level of privacy for the amount of additional overhead incurred.

The work in [87] further considered internal adversaries who can compromise and view the routing tables of the forwarder nodes and designed a routing protocol based on randomized routing and dummy packet transmissions. Similarly, the work in [45] proposed a dummy packet routing scheme where the destination node randomly forwards some of its received packets to a randomly selected neighbor node located M hops away.

Limitations of current heuristic algorithms: It is evident that the existing privacy-preserving schemes do not come for free and there exists a trade-off between the amount of privacy provided and the transmission overheads incurred. Although the above schemes have mainly relied on additional dummy traffic (or/and random delays) to mitigate traffic analysis attempts, there is no rigorous quantification of the adversary's detection probability, its optimal attacking strategy, and the overheads incurred by the privacy-preserving scheme. Hence, it would be interesting to quantify the loss of utility (or overheads) incurred by the privacy-preserving scheme and weigh it against the additional amount of privacy provided.

The work in [93] designed an optimal route selection strategy that maximizes the sender anonymity for the Internet and formulated an optimization problem to determine a path length distribution that maximizes the anonymity degree (a function of Shannon's entropy) of a system. Different from [93], we formulate a statistical decision-making framework and use a more direct (non-information-theoretic) privacy metric for our objective function.

3.3 System Model

In this section, we first describe our network and adversary model before formally defining our privacy metric in Definition 3.2.

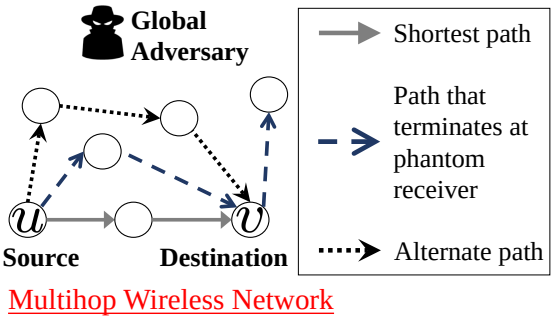


Figure 3.1: Illustration of the path distribution available to a source node u.

3.3.1 Network Model

We consider the scenario where a source node u wants to send packets to a single destination node v in a static wireless network. The source node uses a source routing protocol (e.g., dynamic source routing) and specifies a routing path from itself to the destination (see Definition 3.1). Due to the wireless broadcast nature of the network, when a node transmits, all its one-hop neighbors are able to receive the transmission.

An illustration of the path distribution available to a source node u is shown in Fig. 3.1. Suppose there exist three possible routing paths from the source node u to the destination node v. The source has to select a path distribution over the three possible paths to its destination such that it minimizes the average detection probability of a global adversary who is able to observe the all node transmissions from the entire network.

Next, we introduce the graph notations used in the chapter:

- Let the wireless network be modeled as a connected hypergraph $\mathcal{G} = (\mathcal{V}, \mathcal{H})$ where $\mathcal{V}$ is the set of nodes and $\mathcal{H}$ is the set of (directed) hyperarcs. A hyperarc $h = (s, \mathcal{R})$ represents a source-receivers pair where $s \in \mathcal{V}$ is the source node and $\mathcal{R} \subseteq \mathcal{V}$ is a non-empty set of receiver nodes adjacent to s. The hyperarc h is used as it models the scenario where a packet transmitted by a source node can be received by multiple receiver nodes.

- Let $w \triangleq (u, v)$ represent the source-destination pair, where $u \in \mathcal{V}$ is the source node and $v \in \mathcal{V}$ is the destination node.

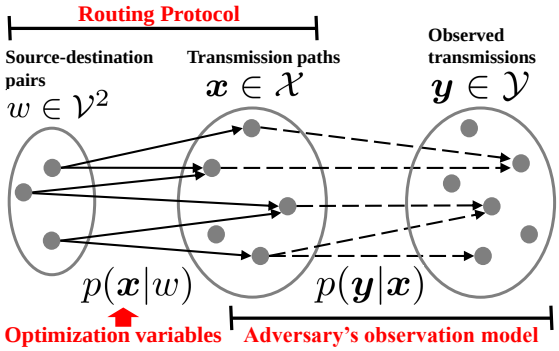


Figure 3.2: Illustration of a probabilistic routing scheme that maps a source-destination pair $w \in \mathcal{V}^2$ to a set of transmission paths $\boldsymbol{x} \in \mathcal{X}$.

- Let $\boldsymbol{x} = (h_1, h_2, \ldots)$ be the actual transmission path comprising the distinct hyperarcs h_i and the source node of h_{i+1} must be a receiver node of h_i.
- Let $\boldsymbol{y}$ be the observed path where $\boldsymbol{y}$ is a subvector of $\boldsymbol{x}$. An observer may not necessarily observe all the hyperarc transmissions in $\boldsymbol{x}$ as some of them may be erased (i.e., lossy observations). The ordering of the observed transmissions, however, remains unchanged.
- Let $\mathcal{X}$ represent the set of all possible paths $\boldsymbol{x}$ in the network and let $\mathcal{X}^w$ be the set of all paths $\boldsymbol{x} = (h_1, h_2, \ldots)$ that serve the source-destination pair $w = (u, v)$, i.e., $h_1 = (u, \mathcal{R})$ and there exists an $h = (s, \mathcal{R}) \in \boldsymbol{x}$ such that $v \in \mathcal{R}$. Let $\mathcal{Y}$ represent the set of all possible observations $\boldsymbol{y}$.
- Let $c_h \geq 0$ represent the cost (e.g., transmission or latency cost) for using the hyperarc h.

Definition 3.1 (Routing Protocol)**.** *Given a network graph $\mathcal{G}$, a probabilistic source-routing protocol selects a path $\boldsymbol{x} \in \mathcal{X}^w$ according to a path distribution $p(\boldsymbol{x}|w)$ for a given source-destination pair $w \in \mathcal{V}^2$.*

3.3.2 Adversary Model

We consider an *external, passive, global* and *informed* [36] adversary that observes a (possibly lossy) sequence of transmissions $\boldsymbol{y}$ from an actual transmission path $\boldsymbol{x}$. Using a Bayesian

traffic analysis technique, the adversary aims to *detect the identity of the source-destination pair w for each observation* $\boldsymbol{y}$, i.e., he aims to identify which node is talking to which node based on his possibly imperfect observations.

We first state the adversary's observation model and its assumed capabilities before studying its optimal detection strategy.

Adversary's Observations

We assume the adversary has *global observability*, i.e., it is potentially able to observe all node transmissions from the entire network. However, we consider the following two observation models for the adversary:

- *Lossy observations.* In practice, the adversary may have lossy observations due to the lossy nature of the wireless channel or some blind spots in his network. Hence, the adversary may only observe a subvector $\boldsymbol{y}$ from the actual transmission path $\boldsymbol{x}$. We assume that the observation distribution $p(\boldsymbol{y}|\boldsymbol{x})$ for observing $\boldsymbol{y}$ given that $\boldsymbol{x}$ was transmitted is known.

  For simplicity, we let $\alpha \in [0, 0.5]$ be the probability of not observing a given transmission $h \in \boldsymbol{x}$ ("erasure probability") and observation of each transmission is independent. This allows the probability $p(\boldsymbol{y}|\boldsymbol{x})$ to be computed using a sequence of $\|\boldsymbol{x}\|_0$ independent Bernoulli trials with parameter of success $(1-\alpha)$, i.e., $p(\boldsymbol{y}|\boldsymbol{x}) = (1-\alpha)^{\|\boldsymbol{y}\|_0}\alpha^{(\|\boldsymbol{x}\|_0 - \|\boldsymbol{y}\|_0)}$, where $\|.\|_0$ represent the L0-norm, which counts the number of non-zero elements in a vector.

- *Lossless observations.* The lossless observations model is a special case of the lossy observations model in which the adversary perfectly observes a sequence of transmissions $\boldsymbol{y}$ which coincides with the actual transmission path $\boldsymbol{x}$, i.e., $\boldsymbol{y} = \boldsymbol{x}$.

Adversary's Capabilities

We assume that the adversary is *informed*, in that it has complete knowledge of the network graph $\mathcal{G}$, prior probabilities $p(w)$, observation distribution $p(\boldsymbol{y}|\boldsymbol{x})$, and path distribution $p(\boldsymbol{x}|w)$. We assume that the actual node transmissions are lossless and only the adversary's observations may be lossy.

We assume that the adversary is *external*, in that it does not have access to the individual nodes in the network, and the contents of the communications, including the packet headers, are protected by encryption and do not leak any information on w. We further assume that the adversary is *passive*, in that it does not manipulate the network traffic by dropping or injecting packets.

The adversary can identify w from each observed $\boldsymbol{y}$ by enumerating the entire set of possible observations for each source-destination pair and apply the MAP inference method explained in the following section.

Adversary's Optimal Detection of Source-Destination Pair w

Suppose that w is the true source-destination pair and the adversary observes the path $\boldsymbol{y}$. A successful detection occurs when the adversary's estimate of the source-destination pair $\widehat{w}(\boldsymbol{y})$ matches w.

Although there exist heuristic-based techniques to estimate $\widehat{w}$ (for example, given that N nodes have received the transmission, a naive heuristic may assign each node that received the transmission with equal probability $\frac{1}{N}$ of being the destination node), the optimal approach to maximize the expected detection probability of the adversary is the Bayesian maximum-a-posteriori (MAP) estimator [81] given by $\widehat{w}_{\text{MAP}} = \underset{w\in\mathcal{V}^2}{\arg\max}\, p(w|\boldsymbol{y})$, where the posterior probability is computed using Bayes' rule: $p(w|\boldsymbol{y}) = \frac{p(w,\boldsymbol{y})}{p(\boldsymbol{y})} = \frac{p(\boldsymbol{y}|w)p(w)}{\sum_{w'\in\mathcal{V}^2} p(\boldsymbol{y}|w')p(w')}$.

The MAP estimator is known to be an optimal estimator optimal under the linear-error and squared-error loss functions. It allows the adversary to exploit the prior knowledge of $p(w)$,

observation distribution $p(\boldsymbol{y}|\boldsymbol{x})$ and the path distribution $p(\boldsymbol{x}|w)$ to maximize his expected detection rate. Note that the source's identity is implicitly known if the adversary has lossless observations since the source is always the first node that transmits. However, the destination's identity may be hidden if there are multiple receivers for the transmission.

For a given observation $\boldsymbol{y}$, the probability of correctly guessing w under the MAP approach is given by $P(W = \widehat{w}_{\text{MAP}}|\boldsymbol{y}) = \max_{w \in \mathcal{V}^2} p(w|\boldsymbol{y})$. Thus, the (expected) detection probability for all observations $\boldsymbol{y} \in \mathcal{Y}$ is given by:

$$\begin{aligned} P_{\text{detect}} &= \sum_{\boldsymbol{y} \in \mathcal{Y}} p(\text{“detect”}|\boldsymbol{y})\, p(\boldsymbol{y}) \\ &= \sum_{\boldsymbol{y} \in \mathcal{Y}} \max_{w \in \mathcal{V}^2} p(w|\boldsymbol{y})\, p(\boldsymbol{y}) \\ &= \sum_{\boldsymbol{y} \in \mathcal{Y}} \max_{w \in \mathcal{V}^2} p(w, \boldsymbol{y}). \end{aligned} \tag{3.1}$$

Suppose the observations are lossy. Let $p(\boldsymbol{y}|\boldsymbol{x})$ be the probability of observing $\boldsymbol{y}$ given that $\boldsymbol{x}$ was actually transmitted. From (3.1), the detection probability of the lossy observations adversary is:

$$\begin{aligned} P_{\text{detect}}^{\text{lossy}} &= \sum_{\boldsymbol{y} \in \mathcal{Y}} \max_{w \in \mathcal{V}^2} \sum_{\boldsymbol{x} \in \mathcal{X}} p(w, \boldsymbol{y}, \boldsymbol{x}) \\ &= \sum_{\boldsymbol{y} \in \mathcal{Y}} \max_{w \in \mathcal{V}^2} \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{y}, \boldsymbol{x}|w)\, p(w) \\ &= \sum_{\boldsymbol{y} \in \mathcal{Y}} \max_{w \in \mathcal{V}^2} \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x}) p(\boldsymbol{x}|w)\, p(w). \end{aligned} \tag{3.2}$$

Suppose that the observations are lossless, i.e., $p(\boldsymbol{y}|\boldsymbol{x}) = 1$ if $\boldsymbol{y} = \boldsymbol{x}$, and $p(\boldsymbol{y}|\boldsymbol{x}) = 0$ otherwise. From (3.1), the detection probability of the lossless observations adversary is:

$$\begin{aligned} P_{\text{detect}}^{\text{lossless}} &= \sum_{\boldsymbol{x} \in \mathcal{X}} \max_{w \in \mathcal{V}^2} p(w, \boldsymbol{x}) \\ &= \sum_{\boldsymbol{x} \in \mathcal{X}} \max_{w \in \mathcal{V}^2} p(\boldsymbol{x}|w)\, p(w). \end{aligned} \tag{3.3}$$

We quantify the adversary's detection probability P_{detect} in Definition 3.2.

Definition 3.2 (Detection Probability of Adversary)**.** *The detection probability of the adversary is given by* $P_{detect} = \sum_{\boldsymbol{y}\in\mathcal{Y}} \max_{w\in\mathcal{V}^2} p(w,\boldsymbol{y})$ *[see* (3.1)*]. A lower* P_{detect} *corresponds to a higher level of privacy and vice versa.*

Next, we present a motivating example for the chosen probabilistic routing approach before formulating the optimization problem to minimize P_{detect} for maximum privacy.

3.4 Motivating Example: Probabilistic Routing for Enhanced Privacy

The idea of using probabilistic (or randomized) routing for location privacy was first proposed in [51] by Ozturk *et al.*. The authors used a single parameter denoted by P_{forward} to decide if a forwarder node that receives a packet transmission should forward the packet to its neighbors (under the probabilistic flooding scheme). Subsequent dummy traffic schemes have also relied on similar parameters to probabilistically route packets through dummy paths. For example, Deng *et al.* [35] used a parameter P_r to decide the probability that a node forwards a dummy packet to its parent node while Jian *et al.* [52] used the parameter P_f to decide the probability that a node forwards a dummy packet to a decoy node away from the true destination node.

The privacy parameters indirectly determine the path distribution $p(\boldsymbol{x}|w)$ and a larger parameter value generally translates to more privacy at the expense of more dummy traffic being genrated. Hence, many authors studied the privacy-utility tradeoffs of their proposed schemes via simulations. Despite this, the amount of privacy provided by the probabilistic paths may not be optimal for a given privacy budget.

Therefore, instead of using a fixed parameter, e.g., P_{forward} to determine the path distribution $p(\boldsymbol{x}|w)$, we let $p(\boldsymbol{x}|w)$ be the *optimization decision variables* in our optimization problem. Next, we use a simple example to illustrate the selection of the optimal path distribution $p(\boldsymbol{x}|w)$ and how it compares to the Uniform heuristic (explained in Section 3.7.2).

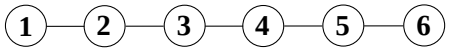


Figure 3.3: Illustration of 6-node line network.

3.4.1 Basic Idea: Optimizing the Routing Paths

For the purpose of illustration, we consider a small 6-node undirected line network as shown in Fig. 3.3. We list the optimized path distribution $p(\boldsymbol{x}|w)$ given a source node $u = 3$ and destinations $v \in \{1,2,4,5,6\}$ for the proposed OPERA and the Uniform heuristic (explained in Section 3.7.2) in Table 3.2. For ease of reading, we only list the source node of each hyperarc h_i in the transmission paths $\boldsymbol{x}$ and $\boldsymbol{y}$ in the table.

It is clear from the table that for the same amount of dummy traffic incurred as the Unifrom heuristic results in a 10% increase in P_{detect} (which gives lower privacy) compared to the proposed OPERA. This is because the Uniform heuristic does not attempt to achieve the lowest possible posterior probability $p(w|\boldsymbol{y})$ for each observation $\boldsymbol{y}$. For example, the path $\boldsymbol{x} = (3,4)$ is never used in the proposed OPERA solution but it has a maximum posterior probability of $p(u = 3, v = 5|\boldsymbol{y} = (3,4)) = 0.5$ when $w = (3,5)$ in the Uniform heuristic. Hence, we have shown that the Uniform heuristic does not maximize the amount of privacy achieved for the same amount of dummy traffic incurred.

The difference in the adversary's detection probability P_{detect} is more significant in a larger network and is investigated in our simulation section. Therefore, we focus on designing an efficient optimization formulation to select the optimal path distribution $p(\boldsymbol{x}|w)$ that minimizes P_{detect} for a given privacy budget.

3.4.2 Example: Optimal Detection for Adversary

We now study the optimal detection strategy of the source-destination pair w given an observation $\boldsymbol{y}$. Consider the same 6-node network as used in Section 3.4.1. Given that the adversary knows the probabilities $p(w)$, $p(\boldsymbol{y}|\boldsymbol{x})$, and $p(\boldsymbol{x}|w)$, it can compute the posterior probabilities $p(w|\boldsymbol{y})$ using Bayes' rule and obtain the values in Table 3.2. For ease of reading, we only list

Table 3.2: Possible (lossless) observations $\boldsymbol{y}$ for $u = 3$ and their corresponding path distribution $P(X = \boldsymbol{x}|W = w)$, and posterior probability $P(W = w|Y = \boldsymbol{y})$ for the two approaches: (i) minimize P_{detect}, and (ii) Uniform heuristic, in a 6-node line network with $\eta = 0.5$.

Source-dest. pair $w = (u, v)$	Prior prob. $P(W = w)$	Path $\boldsymbol{x} = \boldsymbol{y}$ (i.e., lossless model)	Path distr. (Opt. vars.) $P(X = \boldsymbol{x}\|W = w)$	Posterior prob. $P(W = w\|Y = \boldsymbol{y})$	Path distr. (Opt. vars.) $P(X = \boldsymbol{x}\|W = w)$	Posterior prob. $P(W = w\|Y = \boldsymbol{y})$
			(i) Minimize P_{detect} (OPERA)		(ii) Uniform heuristic	
(3,1)	1/4	(3,2)	1	0.4	1	0.667
(3,2)	1/4	(3)	1/4	0.5	1/4	0.5
(3,2)	1/4	(3,2)	3/4	0.3	1/4	0.167
(3,2)	1/4	(3,4)	0	-	1/4	0.25
(3,2)	1/4	(3,4,5)	0	-	1/4	0.125
(3,4)	1/4	(3)	1/4	0.5	1/4	0.5
(3,4)	1/4	(3,2)	3/4	0.3	1/4	0.167
(3,4)	1/4	(3,4)	0	-	1/4	0.25
(3,4)	1/4	(3,4,5)	0	-	1/4	0.125
(3,5)	1/4	(3,4)	0	-	1/2	0.5
(3,5)	1/4	(3,4,5)	1	0.5	1/2	0.25
(3,6)	1/4	(3,4,5)	1	0.5	1	0.5
Adversary's detection probability P_{detect}			45%		55%	

the source node of each hyperarc h_i in the transmission paths $\boldsymbol{x}$ and $\boldsymbol{y}$ in the table.

To illustrate how the MAP estimation in (3.1) works, we examine the observation $\boldsymbol{y} = (3,2)$ under the $(\boldsymbol{x} = \boldsymbol{y})$ column. Suppose that the Uniform heuristic (explained in Section 3.7.2) is used. When the adversary observes (3,2), it can refer to the Table 3.2 (rows 1, 3, and 7) and examine the posterior probabilities: $p(u = 3, v = 1|\boldsymbol{y} = (3,2)) = \frac{2}{3}$, $p(u = 3, v = 2|\boldsymbol{y} = (3,2)) = \frac{1}{6}$, and $p(u = 3, v = 4|\boldsymbol{y} = (3,2)) = \frac{1}{6}$. The probabilities can be interpreted as follows - with $\frac{2}{3}$, $\frac{1}{6}$, and $\frac{1}{6}$ probabilities, the destination node is 1, 2 and 4 respectively.

Our MAP adversary always picks node 1 as the destination each time he observes $\boldsymbol{y} = (3,2)$. The rationale being that he will guess correctly with a higher probability of $\frac{2}{3}$ (the *maximum posterior probability*) on average compared to other arbitrary approaches. Intuitively, node 1 is the most likely destination node in the posterior setting.

3.5 Optimizing the Privacy-Utility Tradeoff

We present the Optimal Privacy Enhancing Routing Algorithm (OPERA), which solves the following problem statement: *compute the optimal path distribution* $p(\boldsymbol{x}|w)$ *that minimizes*

privacy leakage given some user-defined privacy budget η. We first explain our objective — minimizing the adversary's detection probability P_{detect}, followed by the cost of using each path $\boldsymbol{x}$, the utility and other network constraints in our optimization problem and finally, the optimization formulation.

3.5.1 Privacy Metric for the Paths

Our optimization objective is to *minimize the adversary's detection probability P_{detect} (see Definition 3.2) for better privacy*, i.e., we minimize

$$\sum_{\boldsymbol{y}\in\mathcal{Y}} \max_{w\in\mathcal{V}^2} \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x})\, p(\boldsymbol{x}|w)\, p(w).$$

3.5.2 Cost of Using Privacy-Preserving Paths

For a given source-destination pair w, we define the cost of using a privacy-preserving path $\boldsymbol{x} \in \mathcal{X}^w$ to be the cost difference between the path $\boldsymbol{x}$ and the minimum-cost path serving w, given by $\sum_{h\in\boldsymbol{x}} c_h - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h$. Suppose each path $\boldsymbol{x}$ is transmitted accordingly to a path distribution $p(\boldsymbol{x}|w)$, and c_h represents the transmission cost. The expected amount of transmission cost incurred by a source-destination pair w is given by $\Big[\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) \sum_{h\in\boldsymbol{x}} c_h\Big] - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h$.

With this, we define the cost of the privacy-preserving scheme for a given network topology to be given by the *expected amount of additional transmission cost incurred by the network*:

$$\begin{aligned}
&\mathbb{E}_{w\in\mathcal{V}^2}\left[\mathbb{E}_{\boldsymbol{x}\in\mathcal{X}}\Big[\sum_{h\in\boldsymbol{x}} c_h\Big] - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h\right] \\
&= \sum_{w\in\mathcal{V}^2} p(w)\left[\Big[\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) \sum_{h\in\boldsymbol{x}} c_h\Big] - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h\right].
\end{aligned} \tag{3.4}$$

Note that the cost c_h can also be used to measure latency.

3.5.3 Optimization Formulation

We first provide a general optimization formulation for the lossy (incomplete observation) adversarial model and examine in Section 3.6 the lossless observations adversarial model, which is a special case of this general problem. To correctly specify our problem, our formulation must specify the (i) privacy budget η, (ii) valid probabilities, and (iii) valid routing paths. Consider the following constraints:

(i) Privacy budget for each source node u: The value in (3.4) should be less than or equal to the budget budget η.

$$\sum_{v\in\mathcal{V}} p(w)\left[\Big[\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w)\sum_{h\in\boldsymbol{x}} c_h\Big] - \min_{\boldsymbol{x}'\in\mathcal{X}^w}\sum_{h\in\boldsymbol{x}'} c_h\right] \leq \eta, \quad \forall u\in\mathcal{V}. \tag{3.5}$$

Recall that $w=(u,v)$ and in (3.5), we fix the source u while varying the destination v in the outer summation term.

(ii) Sum of probabilities over support and non-negativity of probabilities: The summation of the path distribution $p(\boldsymbol{x}|w)$ over its entire support $\mathcal{X}$ must equal one.

$$\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) = 1, \qquad \forall w\in\mathcal{V}^2. \tag{3.6}$$

A valid probability has to be non-zero.

$$0 \leq p(\boldsymbol{x}|w) \leq 1, \qquad \forall \boldsymbol{x}\in\mathcal{X}, w\in\mathcal{V}^2. \tag{3.7}$$

(iii) Valid transmissions: The source node u, by definition must be the first node to transmit while the destination node v needs to receive the transmission from the sequence of transmissions $\boldsymbol{x}$. In other words, we set the probability of using a path $\boldsymbol{x}$ that is not in $\mathcal{X}^w$ (the set of all possible paths that serve w) to zero, i.e., we have

$$p(\boldsymbol{x}|w) = 0, \qquad \forall \boldsymbol{x}\notin\mathcal{X}^w, w\in\mathcal{V}^2. \tag{3.8}$$

With the objective function and constraints defined, we proceed to formulate the optimization problem.

General Formulation

Given a network graph $\mathcal{G} = (\mathcal{V}, \mathcal{H})$, transmission cost $\{c_h\}_{h\in\mathcal{H}}$, the prior probabilities $\{p(w)\}_{w\in\mathcal{V}^2}$, the adversary's observation distribution $\{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}$, and the privacy budget η, find the path distribution $\{p(\boldsymbol{x}|w)\}_{\boldsymbol{x}\in\mathcal{X},w\in\mathcal{V}^2}$ that minimizes the adversary's detection probability P_{detect} in (3.2) such that the expected cost of the privacy-preserving routes is at most η for each source node u. The solution can be obtained by solving the minimax optimization in Problem (3.9).

$$\underline{\text{MMProb}(\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}, \eta):}$$

$$\begin{aligned}
\underset{\{p(\boldsymbol{x}|w)\}_{\boldsymbol{x}\in\mathcal{X},w\in\mathcal{V}^2}}{\text{minimize}} \quad & \sum_{\boldsymbol{y}\in\mathcal{Y}} \max_{w\in\mathcal{V}^2} \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x})\, p(\boldsymbol{x}|w)\, p(w) \\
\text{subject to} \quad & \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) = 1, \quad \forall\, w \in \mathcal{V}^2 \\
& 0 \le p(\boldsymbol{x}|w) \le 1, \quad \forall\, \boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2 \\
& p(\boldsymbol{x}|w) = 0, \qquad \forall\, \boldsymbol{x} \notin \mathcal{X}^w, w \in \mathcal{V}^2
\end{aligned}$$

$$\sum_{v\in\mathcal{V}} p(w) \left[\left[\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) \sum_{h\in\boldsymbol{x}} c_h \right] - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h \right] \le \eta, \quad \forall\, u \in \mathcal{V}. \tag{3.9}$$

Next, we show that the MMProb Problem can be reformulated as a linear program. This allows efficient algorithms such as the well-known Simplex algorithm [94] to be used for the computation of the optimal solution.

Linear Program Formulation

We can reformulate the minimax problem in Problem (3.9) as a linear program by introducing a variable $z_{\boldsymbol{y}}$ to match the value of $\max_{w\in\mathcal{V}^2} \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x})\, p(\boldsymbol{x}|w)\, p(w)$ in the objective function at the

optimal solution for each $\boldsymbol{y} \in \mathcal{Y}$, along with the inequality constraint:

$$z_{\boldsymbol{y}} - \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x}) p(\boldsymbol{x}|w) p(w) \geq 0, \ \forall \boldsymbol{y} \in \mathcal{Y}, w \in \mathcal{V}^2.$$

At the optimal solution, where $\sum_{\boldsymbol{y} \in \mathcal{Y}} z_{\boldsymbol{y}}$ is minimized, we have:

$$z_{\boldsymbol{y}} = \max_{w \in \mathcal{V}^2} \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x}) p(\boldsymbol{x}|w) p(w),$$

for each $\boldsymbol{y} \in \mathcal{Y}$. The detection probability of the adversary can then be expressed as: $P_{\text{detect}} = \sum_{\boldsymbol{y} \in \mathcal{Y}} z_{\boldsymbol{y}}$. Using the newly introduced $\{z_{\boldsymbol{y}}\}_{\boldsymbol{y} \in \mathcal{Y}}$ variables, we arrive at the linear program formulated in Problem (3.10).

$$\underline{\text{LPProb}(\mathcal{G}, \{c_h\}_{h \in \mathcal{H}}, \{p(w)\}_{w \in \mathcal{V}^2}, \{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y} \in \mathcal{Y}, \boldsymbol{x} \in \mathcal{X}}, \eta):}$$

$$\begin{aligned}
&\underset{\substack{\{p(\boldsymbol{x}|w)\}_{\boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2}, \\ \{z_{\boldsymbol{y}}\}_{\boldsymbol{y} \in \mathcal{Y}}}}{\text{minimize}} && \sum_{\boldsymbol{y} \in \mathcal{Y}} z_{\boldsymbol{y}} \\
&\text{subject to} && \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{x}|w) = 1, \quad \forall w \in \mathcal{V}^2 \\
& && 0 \leq p(\boldsymbol{x}|w) \leq 1, \quad \forall \boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2 \\
& && p(\boldsymbol{x}|w) = 0, \qquad \forall \boldsymbol{x} \notin \mathcal{X}^w, w \in \mathcal{V}^2
\end{aligned}$$

$$z_{\boldsymbol{y}} - \sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x}) p(\boldsymbol{x}|w) p(w) \geq 0, \quad \forall \boldsymbol{y} \in \mathcal{Y}, w \in \mathcal{V}^2$$

$$\sum_{v \in \mathcal{V}} p(w) \left[\Big[\sum_{\boldsymbol{x} \in \mathcal{X}} p(\boldsymbol{x}|w) \sum_{h \in \boldsymbol{x}} c_h \Big] - \min_{\boldsymbol{x}' \in \mathcal{X}^w} \sum_{h \in \boldsymbol{x}'} c_h \right] \leq \eta, \ \forall u \in \mathcal{V}. \tag{3.10}$$

Note that Problem (3.10) is a linear program because its objective function is simply the summation of the decision variables $z_{\boldsymbol{y}}$, which is a linear function, and all the constraints are also linear. Algorithm 3.1 summarizes the proposed Optimal Privacy Enhancing Routing Algorithm (OPERA) which probabilistically selects a path $\boldsymbol{x}$ that serves the source-destination pair w according to an optimized path distribution $p(\boldsymbol{x}|w)$.

Computational Complexity

The linear program formulation enables our problem to be solved in polynomial time. Despite this, the search space of the problem grows exponentially according to the network size.

Algorithm 3.1: OPERA algorithm for computing a privacy-preserving path $\boldsymbol{x}$ for a source-destination pair w.

OPERA($\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}, \eta, w$):

Input : Network graph $\mathcal{G}$, transmission cost $\{c_h\}_{h\in\mathcal{H}}$, the prior probabilities $\{p(w)\}_{w\in\mathcal{V}^2}$, the adversary's observation distribution $\{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}$, privacy budget η, and source-destination $w = (u, v)$.

Output : Privacy-preserving path $\boldsymbol{x}$.

Solve the optimization problem LPProb($\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}, \eta$) in (3.10) to obtain the optimized path distribution $p(\boldsymbol{x}|w)$ for using path $\boldsymbol{x}$ given w subjected to the budget constraint η.

Randomly select a routing path $\boldsymbol{x}$ according to the path distribution $p(\boldsymbol{x}|w)$.

For each path $\boldsymbol{x}$, the lossy observations adversary can observe $\binom{\|\boldsymbol{x}\|_0}{k}$ possible observations with k node transmissions (see example in Table 3.3) where $\|\boldsymbol{x}\|_0$ is the number of nodes that transmitted in $\boldsymbol{x}$. Given that the adversary may observe $k = 0, \ldots, \|\boldsymbol{x}\|_0$ number of node transmissions for a path $\boldsymbol{x}$, there are a total of $2^{\|\boldsymbol{x}\|_0}$ possible observations $\boldsymbol{y}$. The number of possible observations grows exponentially with the dimension of $\boldsymbol{x}$, resulting in a combinatorial explosion. Hence, we propose an approximation method for the adversary's lossy observation distribution in the Section 3.5.4. In addition, valid paths that contain a minimum spanning tree (MST) can be heuristically pruned to reduce the path search space $\mathcal{X}$.

3.5.4 Approximating the Lossy Observations Adversary

To reduce the computational cost for the optimal path distribution, we suggest approximating the adversary's observation model by replacing the observation distribution $\{p(\boldsymbol{y}|\boldsymbol{x})\}_{\boldsymbol{y}\in\mathcal{Y},\boldsymbol{x}\in\mathcal{X}}$ values for observations with more than n transmission losses from a path $\boldsymbol{x}$ with zero. More formally, for each $\boldsymbol{x} \in \mathcal{X}$, we let $p(\boldsymbol{y}|\boldsymbol{x}) = 0$ if $p(\boldsymbol{y}|\boldsymbol{x}) < \epsilon$ where $\epsilon = (1-\alpha)^{\|\boldsymbol{x}\|_0 - n}\alpha^n$, with $n \in (0, \|\boldsymbol{x}\|_0)$, and $\alpha \in [0, 0.5]$ is the probability of not observing a given transmission $h \in \boldsymbol{x}$.

A smaller parameter ϵ gives a better approximation of P_{detect} but offers less computational savings. Next, we have the following Proposition 3.1.

Proposition 3.1. *The approximation method in Section 3.5.4, which uses a truncated observation distribution provides a lower bound for P_{detect} obtained in Problem* (3.10).

Proof. We show that the feasible region in Problem (3.10) becomes larger in the approximation method, which leads to a lower P_{detect} value. Let the truncated observation probability be $q(\boldsymbol{y}|\boldsymbol{x}) = p(\boldsymbol{y}|\boldsymbol{x})$ if $p(\boldsymbol{y}|\boldsymbol{x}) \geq \epsilon$, and $q(\boldsymbol{y}|\boldsymbol{x}) = 0$ otherwise.

Consider the $z_{\boldsymbol{y}}$ constraint in Problem (3.10), which can be rewritten as:

$$z_{\boldsymbol{y}} \geq \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x})p(\boldsymbol{x}|w)p(w)\ , \forall\, \boldsymbol{y} \in \mathcal{Y}, w \in \mathcal{V}^2.$$

The set of possible $z_{\boldsymbol{y}}$ that satisfies the constraint $z_{\boldsymbol{y}} \geq \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{y}|\boldsymbol{x})p(\boldsymbol{x}|w)p(w)$ is a subset of the set of possible $z_{\boldsymbol{y}}$ that satisfies the constraint $z_{\boldsymbol{y}} \geq \sum_{\boldsymbol{x}\in\mathcal{X}} q(\boldsymbol{y}|\boldsymbol{x})p(\boldsymbol{x}|w)p(w)$ since $q(\boldsymbol{y}|\boldsymbol{x}) \leq p(\boldsymbol{y}|\boldsymbol{x})$. Hence, we obtain a larger feasible region when we use the truncated probability $q(\boldsymbol{y}|\boldsymbol{x})$. This may lead to a lower objective function value in the minimization problem which serves as a lower bound for P_{detect}. □

Example: Computation Reduction via Likelihood Truncation

Consider a small undirected line network with only three nodes. Assume that the adversary has lossy observations where the probability of not observing a transmission $\alpha = 0.1$. The possible observations for the lossy adversary are given in Table 3.3 for an arbitrary path distribution $p(\boldsymbol{x}|w)$. The highlighted rows (*) in the table represent the actual transmission path $\boldsymbol{x}$ which may not alway be observed perfectly due to lossy observations. The empty tuple () in the observed path column represents the case where no transmission is observed. For ease of reading, we only list the source node of each hyperarc h_i in the transmission paths $\boldsymbol{x}$ and $\boldsymbol{y}$ in the table.

The number of possible observations $\boldsymbol{y}$ is much larger compared to that of a lossless adversary who only observes the highlighted rows 1 and 5. This is because we have to consider all the combinations of a path $\boldsymbol{x}$ where $1,2,3,\ldots$ transmissions were transmitted but not observed by the adversary. However, we can approximate the adversary's detection probability P_{detect} by simply omitting paths with more than n missing transmissions as discussed in Section 3.5.4. When $\alpha = 0.1$, the probability of observing paths with more than one missing transmission

Table 3.3: Possible (lossy) observations $\boldsymbol{y}$ for $u = 1$ and their corresponding likelihood $P(Y = \boldsymbol{y}|W = w)$, and posterior probability $P(W = w|Y = \boldsymbol{y})$ for $\alpha = 0.1$, in a 3-node line network given that $\boldsymbol{x} = (1,2)$.

Source-dest. pair w	Prior prob. $P(W = w)$	Actual path $\boldsymbol{x}$	Path distribution $p(X = \boldsymbol{x}\|W = w)$	Observed path $\boldsymbol{y}$	Likelihood $P(Y = \boldsymbol{y}\|X = \boldsymbol{x})$	Posterior prob. $P(W = w\|Y = \boldsymbol{y})$
* (1,2)	1/6	(1, 2)	1	(1, 2)	0.81	0.5
(1,2)	1/6	(1, 2)	1	(1)	0.09	0.5
(1,2)	1/6	(1, 2)	1	(2)	0.09	0.0417
(1,2)	1/6	(1, 2)	1	()	0.01	0.0417
* (1,3)	1/6	(1, 2)	1	(1, 2)	0.81	0.5
(1,3)	1/6	(1, 2)	1	(1)	0.09	0.5
(1,3)	1/6	(1, 2)	1	(2)	0.09	0.0417
(1,3)	1/6	(1, 2)	1	()	0.01	0.0417

(e.g., the fourth row in Table 3.3) is only 1%. Hence, we obtain a lower bound of P_{detect} by omitting observations that occur with low probability.

In the next section, we consider the worst-case scenario for the wireless network where the adversary is able to perfectly observe all transmissions in the network.

3.6 Lossless Adversarial Observability (Worst-Case Scenario)

In this section, we consider the lossless observations adversary, which is a special case of the lossy observations adversary. The lossless observations adversary perfectly observes each transmission path $\boldsymbol{x}$, i.e., the probability of observing $\boldsymbol{y}$ given that $\boldsymbol{x}$ was actually transmitted, $p(\boldsymbol{y}|\boldsymbol{x}) = 1$ if $\boldsymbol{y} = \boldsymbol{x}$, and $p(\boldsymbol{y}|\boldsymbol{x}) = 0$ otherwise. Hence, it represents a worst-case adversary.

The objective function in the general problem formulated in Section 3.5.3 can simply be replaced by (3.3), i.e., $\sum_{\boldsymbol{x}\in\mathcal{X}} \max_{w\in\mathcal{V}^2} p(w,\boldsymbol{x})$. Similar to Section 3.5.3, we introduce a variable $z_{\boldsymbol{x}}$ to match the value of $\max_{w\in\mathcal{V}^2} p(w,\boldsymbol{x})$, at the optimal solution, along with the inequality constraint:

$$z_{\boldsymbol{x}} - p(\boldsymbol{x}|w)p(w) \geq 0,\ \forall \boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2.$$

This allows the optimization problem for the lossless observations adversary to be formulated as the linear program in Problem (3.11). In addition, the problem can be decomposed into smaller subproblems for each source node u to solve in a distributed fashion (see Propo-

sition 3.2). This allows the optimal solution to be computed in a distributed manner or in parallel for efficiency.

$$\underline{\text{DLPProb}(\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \eta)\text{:}}$$

$$\begin{aligned}
&\underset{\substack{\{p(\boldsymbol{x}|w)\}_{\boldsymbol{x}\in\mathcal{X}, w\in\mathcal{V}^2},\\ \{z_{\boldsymbol{x}}\}_{\boldsymbol{x}\in\mathcal{X}}}}{\text{minimize}} && \sum_{\boldsymbol{x}\in\mathcal{X}} z_{\boldsymbol{x}} \\
&\text{subject to} && \sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) = 1, \quad \forall w \in \mathcal{V}^2 \\
& && 0 \le p(\boldsymbol{x}|w) \le 1, \quad \forall \boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2 \\
& && p(\boldsymbol{x}|w) = 0, \qquad \forall \boldsymbol{x} \notin \mathcal{X}^w, w \in \mathcal{V}^2 \\
& && z_{\boldsymbol{x}} - p(\boldsymbol{x}|w)p(w) \ge 0, \forall \boldsymbol{x} \in \mathcal{X}, w \in \mathcal{V}^2 \\
& && \sum_{v\in\mathcal{V}} p(w) \left[\Big[\sum_{\boldsymbol{x}\in\mathcal{X}} p(\boldsymbol{x}|w) \sum_{h\in\boldsymbol{x}} c_h \Big] - \min_{\boldsymbol{x}'\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}'} c_h \right] \le \eta, \quad \forall u \in \mathcal{V}. \qquad (3.11)
\end{aligned}$$

Remark: Note that the difference between Problem (3.11) and the non-distributed optimization in Problem (3.10) is that the first constraint for $z_{\boldsymbol{x}}$ in (3.11) is localized. Specifically, each $\boldsymbol{x}$ is localized to a specific source node u whereas in (3.10), each $\boldsymbol{y}$ could be produced by many different source nodes.

Proposition 3.2. *The DLPProb problem in* (3.11) *is block separable.*

Proof. The key idea in proving the block separable property is that there are no *complicating variables* in the objective function. In a lossless observation, the observed source node u must be the first node to transmit. Hence, two routing paths $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ made by two different sources u_1 and u_2 cannot be observed to be the same observation, i.e., $\boldsymbol{y}_1 \neq \boldsymbol{y}_2$. In other words, given a $w = (u, v)$ pair, the term $p(\boldsymbol{y}|w = (u', v)) = 0$ for all $u' \in \mathcal{V}, u' \neq u$. Let $\mathbf{a}$ and $\mathbf{b}$ represent the column vector of decision variables $p(\boldsymbol{x}|w)$ and $z_{\boldsymbol{x}}$ respectively. Since the objective function $\sum_{\boldsymbol{x}\in\mathcal{X}} z_{\boldsymbol{x}}$ is a function of only $\mathbf{b}$, it can be partitioned into $|\mathcal{V}|$ summations of the subvectors $\mathbf{b}_1, \mathbf{b}_2, \ldots$ which corresponds to paths made by source node $u_1, u_2, \ldots$. Similarly, it can be easily shown that the optimization constraints can be partitioned to only include variables from the subvector $\mathbf{b}_i$ that correspond to a source node u_i. Therefore, we conclude that Problem (3.11) is block separable. □

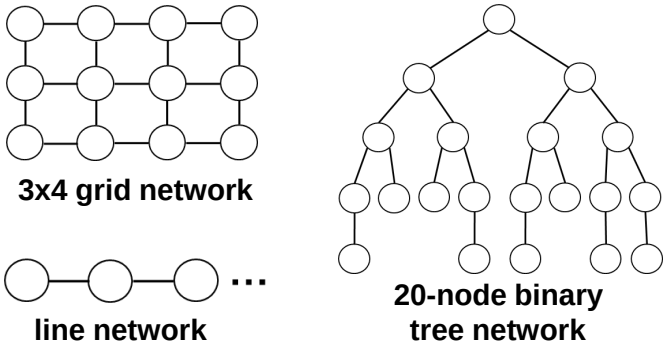


Figure 3.4: Used network topologies in our simulation.

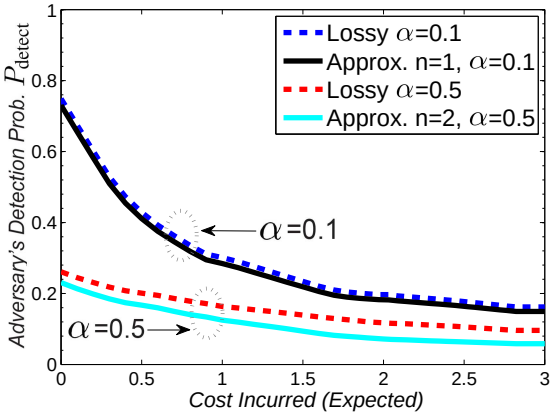


Figure 3.5: Adversary's detection probability P_{detect} for the lossy observations model in a 10-node line network with different α and n parameters.

3.7 Simulation Results and Discussion

In this section, we study the adversary's detection probability P_{detect} under the proposed OPERA and compared it with other privacy-preserving routing schemes based on the Greedy and Uniform heuristics, a baseline heuristic scheme [43], and the minimization of mutual information. We varied the privacy budget η and evaluated the P_{detect} values against the expected cost incurred by the schemes in various connected network topologies. We examined the various schemes using the basic line, binary tree, and grid network topologies (see Fig. 3.4), the random topology, in addition to two other real-world topologies from the Roofnet [95] and Indriya [96] testbeds.

We assume (except for Section 3.7.6) that the links are symmetric, i.e., for each hyperarc

$h = (i, \mathcal{R})$ in the network, there exists $|\mathcal{R}|$ hyperarcs given by $h_k = (k, \mathcal{R}_k), k \in \mathcal{R}$, where $i \in \mathcal{R}_k$. We let the cost of each hyperarc $h \in \mathcal{H}$ be one, i.e., $c_h = 1$. We also assume single-path routing in Sections 3.7.1 to 3.7.4 and multipath routing in Sections 3.7.5 to 3.7.6. Finally, we assume that $w = (u, v)$ is chosen uniformly at random from the set of all possible node pairs where $u \neq v$.

Performance metric: We plot the adversary's detection probability curve to study the privacy-utility tradeoff of OPERA and the baseline schemes. For a fixed cost incurred in expectation, we consider the routing protocol that achieves higher privacy to be the superior one. Recall that a higher privacy corresponds to a lower P_{detect}, which quantifies the amount of privacy provided by the routing protocol. The expected cost incurred can be interpreted as the expected number of additional dummy hops incurred by the privacy-preserving scheme and a high expected cost corresponds to lower utility for the network.

Implementation details: The adversary's detection probability curve is obtained by repeatedly solving the optimization problem and baseline schemes for each cost incurred (granularity of 0.1) and computing its corresponding P_{detect} value. We used MATLAB's linprog solver to solve the simulated scenarios for OPERA and the fmincon solver to solve the mutual information minimization problem in Section 3.7.4. The default 'dual-simplex' optimization algorithm was used in the linprog solver and the default 'interior-point' optimization algorithm was used in the fmincon solver. The default constraint violation parameters were used.

We now discuss our findings under various network settings.

3.7.1 Lossy Adversarial Observations

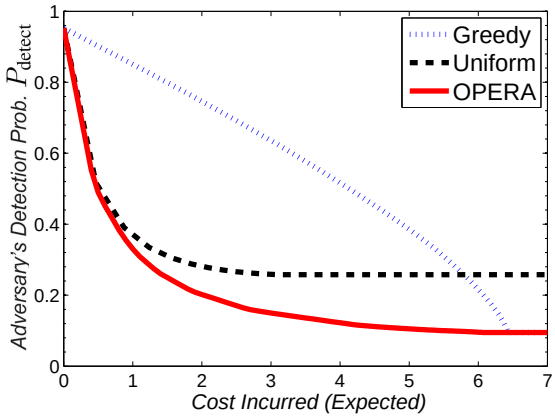
We solve Problem (3.10) to obtain the optimal P_{detect} values for the proposed OPERA. Fig. 3.5 shows the P_{detect} values for OPERA and the approximation method in Section 3.5.4 for a 10-node line network with the erasure probabilities $\alpha = 0.1$ and $\alpha = 0.5$. Recall that α is the probability of not observing a given transmission $h \in \boldsymbol{x}$ while n is the parameter in our approximation method in Section 3.5.4.

Generally, the P_{detect} values decreased as α is increased since the unobserved transmissions may belong to a larger set of possible source-destination pairs. Also, a larger n value is needed to better approximate P_{detect} for larger α values. There exists an inverse relationship between the value of n and the complexity of the optimization problem in (3.10), and a higher n results in a more accurate estimate of the true P_{detect} at the expense of additional computational costs. More performance degradation is experienced in the grid network compared to the line network as the number of possible w pairs increases when less transmissions are observed. Interestingly, the optimized paths from the approximation method coincided with the optimal paths of the original method in our simulation, i.e., the adversary's detection rate does not increase even if he uses (3.2) while the system uses the approximation method.

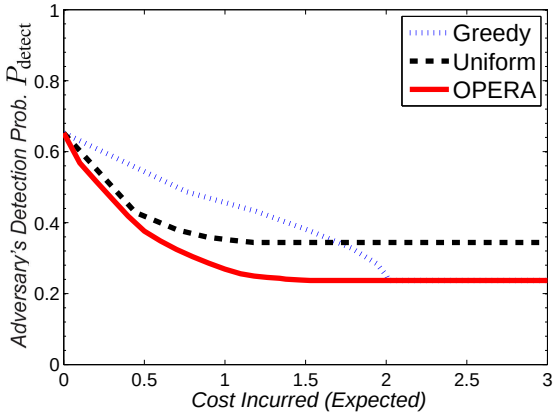
3.7.2 Comparison with Greedy and Uniform Heuristics

From this section onwards, we assume a lossless observations adversary. We solved Problem (3.11) to obtain the optimal P_{detect} values for the proposed OPERA. The details for the *Greedy* and *Uniform* heuristics are given in Algorithm 3.2 and Algorithm 3.3 respectively.

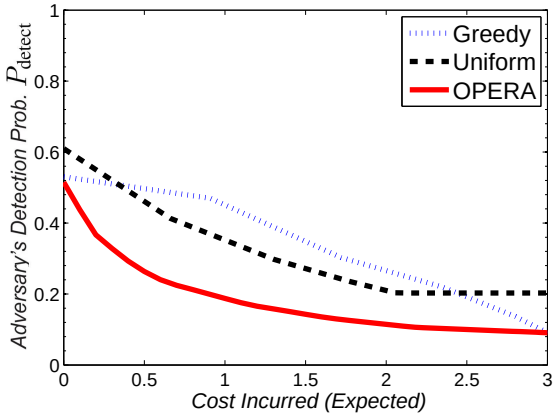
In the Uniform heuristic, we select a path uniformly at random from all valid paths that serve w (similar to [52] where the authors in [52] proposed a dummy packet injection scheme that randomly (uniformly) transmits a dummy packet to a chosen receiver located m hops away from the destination where $m > 1$. However, the scheme was designed for an adversary with local observability. Hence, we used a uniform heuristic that follows the authors' main idea of making the transmission paths "completely random instead of a directed one") subjected to the privacy budget. In the Greedy heuristic, we always greedily send the packets via the path containing the most number of receivers, subjected to the privacy budget. Similar to OPERA, the two heuristics exploit knowledge of the network graph $\mathcal{G}$ to provide better privacy. As such, they provide an upper bound on the achievable privacy for other heuristics that use only local network topology information. However, the privacy budget constraint applies to each path $\boldsymbol{x}$ instead of the expected privacy budget for each source node as used in OPERA.



(a) 20-node line network (single-path).



(b) 20-node binary tree network (single-path).



(c) 3 × 4 grid network (single-path).

Figure 3.6: Adversary's detection probability P_{detect} under the Greedy and Uniform heuristics and the proposed OPERA, for single-path routing in the line, binary tree, and grid networks.

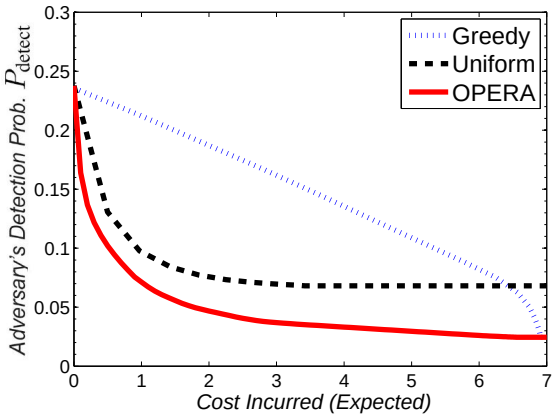


Figure 3.7: Adversary's detection probability P_{detect} under the Greedy and Uniform heuristics and the proposed OPERA (with single-path routing), averaged over five randomly generated 80-node networks.

Figs. 3.6a, 3.6b, and 3.6c show the P_{detect} values of the two heuristics and the proposed OPERA under different network topologies with the single-path constraint. For most values of the incurred cost, there existed a significant difference (up to 50%) in the performance of the two heuristics compared to OPERA. In Figs. 3.6a and 3.6b, the performance of the Greedy heuristic was worse than the Uniform heuristic at lower privacy budgets despite greedily choosing the path with the most number of receivers. This indicates that increasing the number of receiver nodes does not necessary translate to better privacy. In fact, the difference between the Greedy heuristic and OPERA can be quite significant as shown in the figures. The Uniform heuristic does not converge to the maximum achievable privacy even when the privacy budget is slack, unlike the Greedy heuristic. In Fig. 3.6c, which uses a grid topology, the Uniform heuristic will uniformly pick each valid shortest path that serve w (which leaks information about the destination) while the Greedy and OPERA methods tend to choose a single path. Hence, this resulted in a higher P_{detect} for the Uniform heuristic even when the expected cost is zero.

Lastly, Fig. 3.7 shows the P_{detect} values of the Greedy and Uniform heuristics and the proposed OPERA (with the single-path routing constraint), averaged over five randomly generated 80-node networks. The P_{detect} values have a similar trend to the results from the smaller 20-node line network in Fig. 3.6a where OPERA outperforms the Uniform and Greedy heuristics.

Table 3.4: Possible (lossless) observations and their corresponding likelihood $P(Y = \boldsymbol{y}|W = w)$ for the Greedy and Uniform heuristics (see Algorithms 3.2 and 3.3 respectively) in a 3-node line network. Assume that the privacy budget η is unbounded.

Source-dest. pair w	Prior prob. $P(W = w)$	Path $\boldsymbol{x} = \boldsymbol{y}$	Likelihood $P(Y = \boldsymbol{y}\|W = w)$	
			Greedy	**Uniform**
(1,2)	1/6	(1)	0	0.5
(1,2)	1/6	(1, 2)	1	0.5
(1,3)	1/6	(1, 2)	1	1
(2,1)	1/6	(2)	1	1
(2,3)	1/6	(2)	1	1
(3,1)	1/6	(3, 2)	1	1
(3,2)	1/6	(3, 2)	1	0.5
(3,2)	1/6	(3)	0	0.5

A simple example on the Greedy and Uniform Heuristics is provided to facilitate understanding.

Example: Greedy and Uniform Heuristics

Consider a 3-node line network, similar to our earlier example in Section 3.5.4. The path selection under the Greedy and Uniform heuristics is illustrated in Table 3.4. For ease of reading, we only list the source node of each hyperarc h_i in the transmission paths $\boldsymbol{x}$ and $\boldsymbol{y}$ in the table. Given $w = (1,2)$, the Uniform heuristic will select routing paths $\boldsymbol{x} = (1)$ and $\boldsymbol{x} = (1,2)$ with equal probability, see rows 1 and 2. The Greedy heuristic on the other hand, always picks $\boldsymbol{x} = (1,2)$ over $\boldsymbol{x} = (1)$ with probability one. Notice that the Greedy heuristic is deterministic (i.e., it always picks the path containing the most number of receivers) while the Uniform heuristic is probabilistic (i.e., it uniformly picks a path $\boldsymbol{x}$ from the set of valid paths $\mathcal{X}^w$).

3.7.3 Comparison with the Sink Simulation and Backbone Flooding Schemes

We compared our proposed OPERA against an existing protocol proposed by Mehta *et al.* [43]. Similar to our work, Mehta *et al.* proposed the sink simulation and backbone flooding schemes in [43, Section 5.2] to provide location privacy for the network sinks under the same global adversary assumption as considered in our work. As the work in [43] considered a wireless

Algorithm 3.2: Greedy routing for preserving source-destination privacy.

GreedyRouting($\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \eta, w$) :

Input : Network graph $\mathcal{G}$, transmission cost $\{c_h\}_{h\in\mathcal{H}}$, the prior probabilities $\{p(w)\}_{w\in\mathcal{V}^2}$, privacy budget η, and source-destination $w = (u, v)$.

Output : Path distribution $p(\boldsymbol{x}|w)$.

Compute the cost of the minimum-cost path from u to v: $c_{\min}(w) = \min_{\boldsymbol{x}\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}} c_h$.

Compute the set of paths $\mathcal{X}'$ that satisfy the privacy budget η where $\mathcal{X}' = \{\boldsymbol{x} : \boldsymbol{x} \in \mathcal{X}^w, \sum_{h\in\boldsymbol{x}} c_h - c_{\min}(w) \le \eta\}$

Initialize $p(\boldsymbol{x}|w) = 0$ for all $\boldsymbol{x} \in \mathcal{X}'$.

Select a path $\boldsymbol{x}^*$ with the most number of receivers, i.e., $\boldsymbol{x}^* = \arg\max_{\boldsymbol{x}\in\mathcal{X}'} \left|\{r : r \in \mathcal{R}_i, h_i = (s_i, \mathcal{R}_i), h_i \in \boldsymbol{x}\}\right|$.

Set $p(\boldsymbol{x}^*|w) = 1$ and use routing path $\boldsymbol{x}^*$.

Algorithm 3.3: Uniform routing for preserving source-destination privacy.

UniformRouting($\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, \eta, w$) :

Input : Network graph $\mathcal{G}$, transmission cost $\{c_h\}_{h\in\mathcal{H}}$, the prior probabilities $\{p(w)\}_{w\in\mathcal{V}^2}$, privacy budget η, and source-destination $w = (u, v)$.

Output : Path distribution $p(\boldsymbol{x}|w)$.

Compute the cost of the minimum-cost path from u to v: $c_{\min}(w) = \min_{\boldsymbol{x}\in\mathcal{X}^w} \sum_{h\in\boldsymbol{x}} c_h$.

Compute the set of paths $\mathcal{X}'$ that satisfy the privacy budget η where $\mathcal{X}' = \{\boldsymbol{x} : \boldsymbol{x} \in \mathcal{X}^w, \sum_{h\in\boldsymbol{x}} c_h - c_{\min}(w) \le \eta\}$

Set $p(\boldsymbol{x}|w) = \frac{1}{|\mathcal{X}'|}$ for each $\boldsymbol{x} \in \mathcal{X}'$.

Randomly select a routing path $\boldsymbol{x}$ according to the path distribution $p(\boldsymbol{x}|w)$.

sensor network setting where all source nodes transmit to a common sink, we have to modify their proposed sink simulation and backbone flooding schemes to suit our setting. Mainly, we arbitrarily assigned the same L simulated (fake) destination nodes for each destination node in the sink simulation technique and let the source node transmit to all the L simulated (and the true) destination nodes using the shortest path routes. To avoid double counting the transmission costs, we allow all transmissions to be piggybacked into a single transmission if the routes overlap. For the backbone flooding scheme, we do not use the proposed approximation algorithm for constructing the backbone network. Instead, we used the minimum spanning tree to flood a packet to the entire network. The minimum spanning tree minimizes the total transmission cost needed for flooding a packet to the entire network, and hence is an ideal backbone network.

Fig. 3.8 shows the P_{detect} values of the sink simulation and backbone flooding schemes and the proposed OPERA (with the single-path constraint), averaged over five randomly generated 80-node networks. In the sink simulation scheme, we varied the value of the L parameter from 2-79 and computed the corresponding P_{detect} values for the cost incurred. The performance of the sink simulation technique is significantly worse (up to five times higher P_{detect}) than OPERA for the same amount of cost incurred. This is true even for large L values as the privacy of the source-destination pair is not necessary proportional to the number of receiver nodes (simulated sinks). Although the performance of the backbone flooding scheme is slightly better than OPERA, it is not flexible enough to allow users to specify a privacy budget constraint. Hence, depending on the network application, it can result in excessive costs. Note that multipath routing was permitted in the backbone flooding scheme.

3.7.4 Comparison with Mutual Information Minimization

Mutual information [97–103] has been used in the literature to measure the information leakage of some anonymous event. Specifically, in our context, it can be used to quantify the source-destination anonymity of a protocol or to measure the privacy leakage (see Definition 3.3) by the routing protocol.

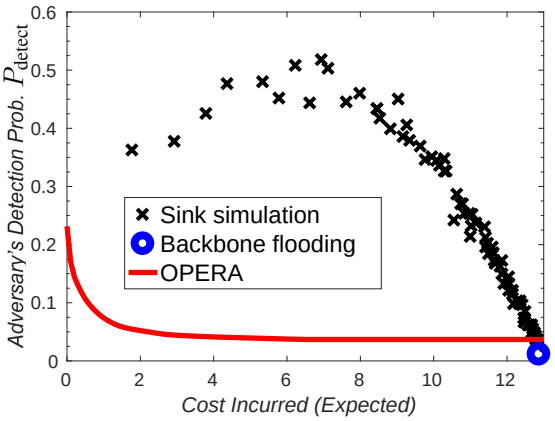


Figure 3.8: Adversary's detection probability P_{detect} under the sink simulation and backbone flooding schemes proposed in [43] and the proposed OPERA (with single-path routing), averaged over five randomly generated 80-node networks.

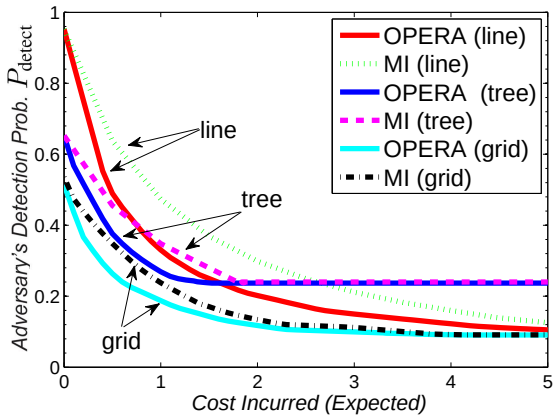


Figure 3.9: Adversary's detection probability P_{detect} under the mutual information minimization approach and the proposed OPERA, for single-path routing in the line, binary tree, and grid networks.

Definition 3.3 (Privacy Leakage)**.** *Consider a graph $\mathcal{G}$. Let W be a random variable representing the source-destination pair $w \in \mathcal{V}^2$, and Y be a random variable representing the observed node transmission path $\boldsymbol{y} \in \mathcal{Y}$. Let $p(w)$ be the prior probability for a source node u to communicate with the destination node v and $p(w, \boldsymbol{y})$ be the joint probability of observing both $\boldsymbol{y}$ and w. The average amount of information (or privacy) leaked by a protocol is measured by the mutual information, which is given by:*

$$\begin{aligned} I(W;Y) &= H(W) - H(W|Y) \\ &= \sum_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(w,\boldsymbol{y}) \log \frac{p(w,\boldsymbol{y})}{p(w)p(\boldsymbol{y})} \\ &= \sum_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)p(w) \log \frac{p(\boldsymbol{y}|w)p(w)}{p(w)p(\boldsymbol{y})} \\ &= \sum_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)p(w) \log \frac{p(\boldsymbol{y}|w)}{p(\boldsymbol{y})}. \end{aligned} \tag{3.12}$$

where $H(W)$ is the Shannon entropy (or uncertainty) of W given by $H(W) = -\sum_{w\in\mathcal{V}^2} p(w)\log p(w)$, and $H(W|Y)$ is the conditional entropy of W given by $H(W|Y) = \sum_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(w,\boldsymbol{y}) \log \frac{p(w)}{p(w,\boldsymbol{y})}$ $= \sum_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)p(w) \log \frac{p(w)}{p(\boldsymbol{y}|w)p(w)}$.

Entropy $H(W)$ can be interpreted as the amount of information needed (by an adversary) to identify the $w \in \mathcal{V}^2$ pair while mutual information $I(W;Y)$ is the reduction in the uncertainty of W due to the knowledge of Y. $I(W;Y)$ can be used to quantify the loss of privacy for w (or equivalently, the amount of privacy leakage) of the protocol where a smaller $I(W;Y)$ value indicates better privacy for w. The value of $I(W;Y)$ is zero (minimum) when W and Y are independent and equals to $H(W)$ (maximum) when A is a deterministic function of Y.

To fairly compare our proposed OPERA against the mutual information minimization, we replace the function in the objective function of Problem (3.11) with the mutual information term in (3.12).

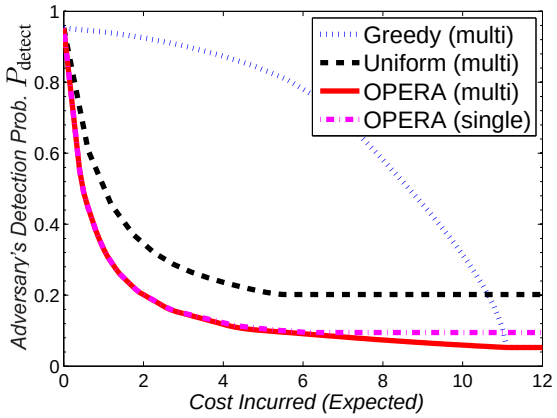
Fig. 3.9 shows the P_{detect} values of the mutual information minimization problem and the proposed OPERA for the line, binary tree, and grid networks. It is observed that minimizing mutual information results in a higher P_{detect} value (and hence, less privacy) compared to

OPERA when the privacy budget is tight. Interestingly, we observed that different mutual information values may correspond to the same P_{detect} value when the privacy budget is slack. However, the converse is not true in our simulations. For the same number of nodes, the privacy difference is largest in the line network (up to 15%) and smallest in the grid network (up to 6%). However, minimizing mutual information is still superior to the Greedy and Uniform heuristics. Therefore, despite being commonly proposed as a measure for privacy [99, 100, 102, 103], minimizing mutual information may not be ideal in our case where a MAP adversary was considered.

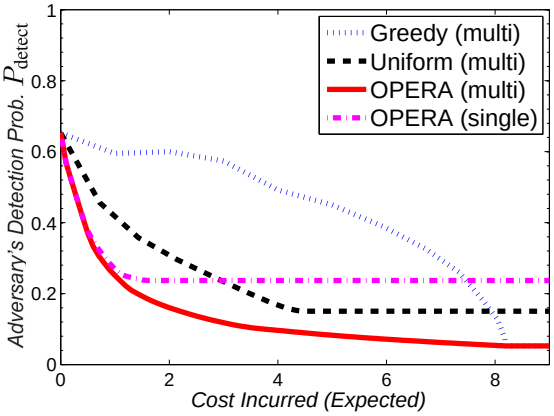
3.7.5 Comparison of Single-path and Multipath Routing

We studied the effects of using multipaths $\mathcal{M} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots\}$ where at least one path $\boldsymbol{x}_i$ will reach the destination node. In the multipath routing, the routing paths $\boldsymbol{x} \in \mathcal{X}$ in Problem (3.11) are replaced by a set of paths $\mathcal{M} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots\}$. The P_{detect} values for the single and multipath routing in the line, binary tree, and grid networks are given in Figs. 3.10a, 3.10b, and 3.10c respectively.

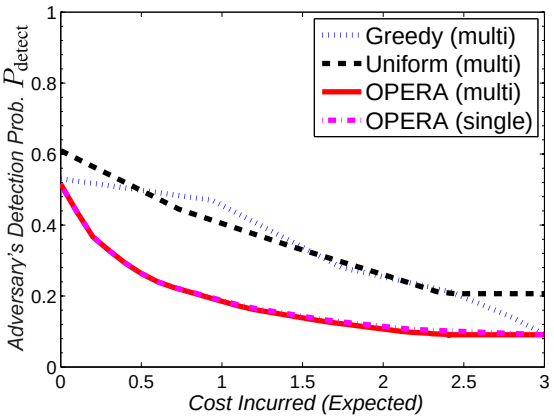
Generally, for a fixed incurred cost, the multipath variants are able to achieve more privacy compared to single-path at the expense of higher computational cost. The improvement in P_{detect} for the proposed OPERA appears to be mild in the line network and does not have any significant effect in the grid network. However, the improvement is more significant in the binary tree network as the privacy budget becomes slack. This is because the multipath approach can improve privacy in scenarios where a leaf node is communicating with another leaf node in the same subtree. When the route is restricted to only a single path, the destination can be easily linked to the same subtree as the path does not travel to other subtrees. This severely limits the number of receivers and lowers privacy when the privacy budget is slack. In practice, the single-path routing constraint can be used if the privacy budget is tight.



(a) 20-node line network (multipath).



(b) 20-node binary tree network (multipath).



(c) 3×4 grid network (multipath).

Figure 3.10: Adversary's detection probability P_{detect} under the Greedy and Uniform heuristics and the proposed OPERA, for multipath routing in the line, binary tree, and grid networks.

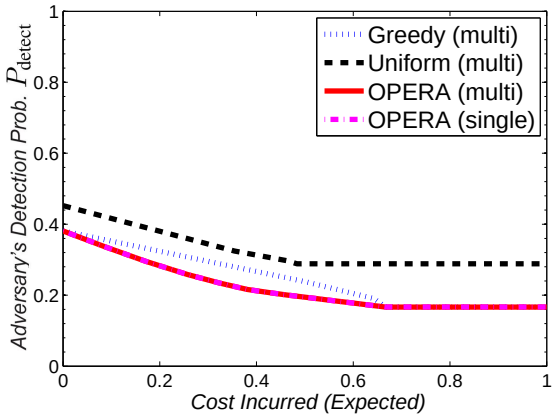


Figure 3.11: Adversary's detection probability P_{detect} under the Greedy and Uniform heuristics and the proposed OPERA for the Roofnet network with multipath routing.

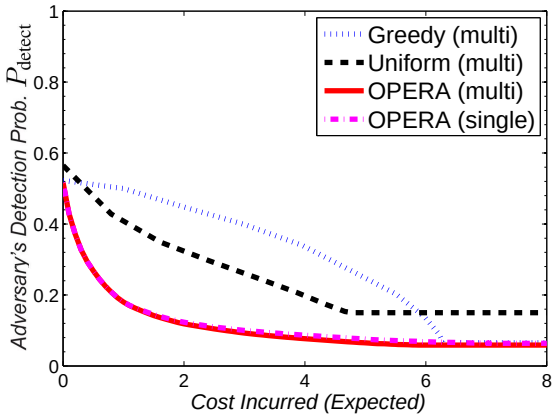


Figure 3.12: Adversary's detection probability P_{detect} under the Greedy and Uniform heuristics and the proposed OPERA for the Indriya network with multipath routing.

3.7.6 Using Network Topologies From Real-World Testbeds

To evaluate the practicality of OPERA in real-world topologies, we used topologies from the outdoor Roofnet [95] and indoor Indriya [96] testbeds, and the corresponding P_{detect} values are shown in Figs. 3.11 and 3.12 respectively. The Roofnet testbed consisted of nine IEEE 802.11b wireless nodes installed in the apartments of volunteers near Massachusetts Institute of Technology and covers approximately one square kilometer. On the other hand, Indriya [96] is a large-scale indoor wireless sensor network testbed deployed at the National University of Singapore. It consists of 127 TelosB motes and covers 3 floors of a building.

For the Roofnet network, we used links with more than 10% delivery rate (includes three

non-symmetric links). For the Indriya network, we considered a subset of 18 nodes, arbitrary selected from each room of the network to reduce the computation complexity. The performance of OPERA in the two mesh-like real-world topologies are similar to our earlier results in the grid topology. There exist little differences in P_{detect} between the single-path and multipath routing for the proposed OPERA. Hence, the single-path optimization problem which has lower computational complexity may be used for such real-world networks.

3.8 Conclusion and Future Work

In this chapter, we have developed a statistical decision-making framework to optimally solve the privacy-preserving routing problem in wireless networks given some utility constraints assuming a powerful global adversary that uses the optimal maximum-a-posteriori (MAP) estimation strategy. We showed an example of how heuristic methods may not be able to achieve the maximum possible privacy for a fixed transmission cost incurred and developed the OPERA algorithm, which uses linear programs to minimize the detection probability of the lossy and lossless observations adversary. We showed via simulations that our approach is significantly better than the Uniform and Greedy heuristics, the sink simulation and backbone flooding schemes, and the mutual information minimization scheme.

For future work, it would be interesting to study the privacy-utility trade-off problem for mobile networks. For mobility scenarios, our scheme may use source routing protocols that extend the well-studied dynamic source routing (DSR) routing protocol for wireless mobile ad hoc networks when the mobility is limited and the mobility patterns are known. The expected amount of transmission overhead may be computed when the mobility patterns are known but the computational complexity may be very costly when there is high mobility among the nodes. Also, note that the use of DSR introduces a large communication overhead as the protocol needs to map the routing information to all other nodes via a route discovery phase, which is basically flooding-based although it uses heuristics to avoid sending duplicate packets.

Since our proposed OPERA computes the optimal solution for the privacy-preserving routing problem, we are able to compare the performance of existing heuristic solutions. This allows one to find or design a good enough heuristic solution that is fast to compute and ideally has a consistent privacy performance in many network topologies.

Chapter 4

Wireless Routing with Privacy Guarantees

We consider the *routing with privacy guarantees* problem in a wireless network where a Bayesian maximum-a-posteriori (MAP) adversary is able to observe all the transmission activities in the entire network. We focus on protecting the privacy of the source-destination identities by designing a (k,ϵ)-*anonymous* routing protocol (see Definition 4.2). The latter ensures that the true source-destination pair w is safely hidden among a set of $(k-1)$ or more other distinct source-destination pairs where each w pair is just as likely to be the true source-destination pair. The routing with privacy guarantees problem is challenging as the interpretation of privacy guarantees is very subjective. For example, the work in [36] designed a periodic flooding scheme that provides statistical privacy guarantees against timing-based traffic analysis attempts. However, the authors did not considered the scenario where the adversary has (side) information on the prior probabilities of each source-destination pair communicating. We provide an example in Section 4.4 where the flooding scheme does not provide any privacy for a participating source-destination pair. As such, our introduced (k,ϵ)-anonymity property considers all prior information and assumes a Bayesian adversary that uses the optimal MAP inference strategy to identify the communicating source-destination pair. We use the optimization approach to compute the minimum-cost path distribution that achieves the (k,ϵ)-anonymity property.

Part of the work discussed in this chapter is included in [104].

4.1 Introduction to Privacy Guarantees

Ensuring the privacy of the communicating parties in wireless communications is a challenging problem that has been widely studied in the literature [37, 39, 44, 65, 105–108]. Due to the broadcast nature of the radio signals, the wireless communications are very vulnerable to passive eavesdropping attempts which are difficult to detect. After collecting enough sniffed traffic data, an adversary can use various traffic analysis techniques [37, 39, 44, 65, 107] to correlate the traffic patterns and compromise privacy, e.g., the source-destination identities of each wireless communication. Thus, various privacy-preserving routing schemes such as probabilistic routing [105, 106] (and our works [37, 65] described in Chapter 3) have been proposed for privacy-concerned users. These works mainly focus on *minimizing the adversary's average detection probability* but not directly on providing *privacy guarantees*.

Although minimizing the average adversarial detection probability does improve the privacy of most nodes, it may not provide privacy guarantees for the vulnerable nodes that require the most protection. Typical privacy metrics like the probability of successful packet tracing [39], probability of successful time correlation or rate monitoring attacks [37], or even entropy-related metrics [43, 109] depend heavily on the assumed adversary's capabilities and traffic analysis technique. As such, these techniques may not provide ample privacy when the adversary's observation capabilities are underestimated or the adversary uses a different traffic analysis technique not considered in the model.

On the other hand, *k-anonymity* [110] and *differential privacy* [111] are two widely studied privacy frameworks for strict privacy guarantees. The need for strict privacy guarantees have been motivated by past privacy leakage incidents as highlighted in [110]. With the increasing number of wireless devices being adopted in the Internet of things (IoT) era, there is a need to design a wireless routing scheme that provides strict privacy guarantees to prevent embarrassing privacy leakage incidents. This is essential if the new wireless IoT technologies are to be widely adopted by consumers. The key idea behind k-anonymity is to guarantee that each individual cannot be distinguished from at least $(k-1)$ other individuals. Despite

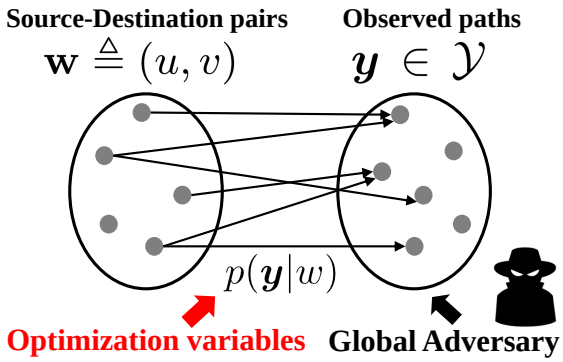


Figure 4.1: Mapping from the source-destination pairs $w \triangleq (u, v)$ to the actual observed node transmission paths $\boldsymbol{y}$ by an adversary who wants to identify w from $\boldsymbol{y}$.

this, some works [109, 112] have highlighted the vulnerability of a k-anonymized dataset to correlation attacks that exploit a lack of diversity as well as vulnerability to adversaries with side information. However, the privacy guarantees make k-anonymity very attractive and subsequently, k-anonymity was applied to the location privacy domain [113]. Another stronger notion of privacy is differential privacy [111]. Different from k-anonymity and its extensions, differential privacy does not permit the release of a sanitized dataset and instead limits users to submit database queries. Random noise (e.g., Laplacian) is added to the original query result, and the noisy result is returned to the users. While differential privacy offers a formal, rigorous mechanism for achieving privacy in database query-based applications, it is not directly applicable to our wireless routing problem because there is no query mechanism. As such, random noise (e.g., Laplacian) cannot be added to the query results.

Therefore, we adopt the (k,ϵ)-anonymity property (adapted from k-anonymity) for privacy guarantees in wireless networks. However, we use the *probabilistic routing* approach [37, 65] (as previously described in Chapter 3) instead of the traditional generalization and suppression methods in k-anonymity. Our routing with privacy guarantees problem is illustrated in Fig. 4.1, where for such a generic system setup, we design a statistical decision-making framework to optimize $p(\boldsymbol{y}|w)$, the probability of the wireless network transmitting a routing path $\boldsymbol{y}$, given a source-destination pair w. Our goal is to find a *minimum-cost* (k,ϵ)-anonymity routing solution for the wireless network.

We consider a Bayesian MAP adversary that acts based on the most probable a posterior belief of the most likely source-destination pair w. We consider two adversary models, one which provides worst-case guarantees of privacy where the adversary has (side) information on the prior probabilities of each source-destination pair communicating, and the second model is where the prior probabilities are not completely known. Furthermore, we derive the worst-case protection assuming the adversary is able to perfectly observe all wireless transmissions in the network. In this way, our strong adversarial assumptions mitigate the vulnerabilities of the original k-anonymity scheme [109, 112] and provide privacy guarantees in the worst-case scenario. In addition, we study in detail how the adversary's prior beliefs affect its detection rate.

4.1.1 Contributions

To the best of our knowledge, this is the first work that addresses the routing with privacy guarantees problem in wireless routing via a statistical decision-making framework that considers a powerful MAP adversary with global observability.

The key contributions of this work can be summarized as follows:

- We propose the (k,ϵ)-*anonymity* property for wireless communications to provide source-destination privacy guarantees and formulate a mixed-integer linear programing (MILP) problem to minimize the expected cost incurred by the (k,ϵ)-anonymous routing scheme.

- We design a statistical decision-making framework to model two types of Bayesian MAP adversaries, one with complete information on the communication patterns and the other will only partial information. We also study in detail how the adversary's prior beliefs affect its detection rate.

- Our simulation results show that our (k,ϵ)-anonymity routing scheme provides significantly better privacy guarantees while having comparable adversary detection rated

Table 4.1: Notation.

$\mathcal{G}$	connected hypergraph representing the network.
$\mathcal{V}$	set of nodes in the network.
$\mathcal{H}$	set of all (directed) hyperarcs in the network.
$h = (s, \mathcal{R})$	hyperarc that represents a source-receivers pair where $s \in \mathcal{V}$ is the source node and $\mathcal{R} \subseteq \mathcal{V}$ is a non-empty set of receiver nodes adjacent to s.
$w \triangleq (u, v)$	source-destination pair where $u \in \mathcal{V}$, $v \in \mathcal{V}$ are the source and destination nodes respectively.
$\boldsymbol{y} = (h_1, h_2, \ldots)$	observed routing path.
$\mathcal{Y}$	set of all possible paths $\boldsymbol{y}$ in the network.
$\mathcal{Y}^w$	set of all possible paths $\boldsymbol{y}$ that serve w.
c_h	cost (e.g., transmission cost) for using hyperarc h.
$\widehat{w}(\boldsymbol{y})$	estimator for w given observation $\boldsymbol{y}$.

compared to a baseline probabilistic routing scheme that minimizes the average detection rate (when ϵ is approximately zero).

4.1.2 Notation

The table of notation used in this chapter can be found in Table 4.1.

4.2 Related Work

In a multi-hop wireless network, any two communicating nodes will need to decide on a routing path to deliver their data packets. However, the routing paths may easily leak the location privacy of the communicating source-destination pair if they are not carefully chosen. For example, if the shortest path is used, then the source node is always the first node that transmits while the destination node has to be in the audible range of the last transmitting node (but not the second last or any other previous transmitting node). Depending on the network topology, the set of possible source-destination pairs may be very small, which may not provide ample privacy.

Hence, early works on location privacy relied on flooding-based approaches to cover the true traffic pattern of the communicating nodes. However, the flooding-based approaches

(e.g., the baseline flooding method in [105] or in [36]) are not viable solutions in general as they consume too much vital network resources like energy, throughput, and latency. In response, probabilistic (or randomized) routing approaches were developed. Probabilistic routing uses less overheads and can offer comparable privacy protection as the flooding-based approaches. The probabilistic flooding and random walk-based routing approaches were proposed in [105] to enhance the location privacy of the source node against a local (observability) adversary, and [114] designed a greedy random walk-based routing scheme to reduce the energy consumption of the flooding-based approach.

Subsequently, the work in [115] proposed routing packets via multiple dummy paths that disrupt packet tracing attempts and [21] proposed a similar dummy packet injection and path diversity scheme to de-correlate the incoming and outgoing traffic pattern at each node. The randomized routing scheme was further optimized in [106] where the randomly selected forwarder nodes were chosen based on their angle and quadrant from the source node to improve the source location privacy. To provide sink location privacy, the work in [43] proposed a backbone flooding and dummy sink scheme that mitigates a global adversary who is able to observe all node transmissions in the network.

As the prior works simply relied on heuristic approaches to fine-tune the privacy-utility trade-offs of the probabilistic routing, our work in [65] (described in Chapter 3) formulated the privacy-preserving route selection problem as a linear program, which optimizes the routing (path) distribution that minimizes the average detection probability of a Bayesian MAP adversary, subjected to a privacy budget. Although minimizing the average detection probability of an adversary generally provides privacy for the communicating nodes, there are no privacy guarantees for each source-destination pair. We highlight in our motivating example (Section 4.4) that there exists a subtle difference between minimizing the average detection probability of an adversary and providing privacy guarantees. The latter may be more attractive for privacy-sensitive users.

To provide privacy guarantees for nodes in a wireless network, cryptographic group signatures

were used to ensure k-anonymity for the destination node against intersection-based attacks in [116], and active tracing attacks in [117]. However, the cryptographic solutions alone do not provide protection against adversaries with global observability. The address this, the work in [113] proposed a routing scheme that achieves k-anonymity for the destination (sink) node. The authors then formulated a non-linear optimization problem to partition the network into k regions that are equally likely to contain the sink node given a constraint on the safety period of the sink detection. However, the authors did not rigorously quantify the amount of privacy of the sink node and instead rely on the heuristic safety period metric, which represents the amount of time for the adversary to location mine or visually search for the sink node. The heuristic safety period metric, also used in [105] decreases the reliability of the provided privacy guarantees.

The work in [36] proposed a periodic flooding scheme that provides statistical privacy guarantees against timing-based traffic analysis attempts. However, the authors did not considered the scenario where the adversary has (side) information on the prior probabilities of each source-destination pair communicating. Depending on the prior distribution, it may be hard for the proposed scheme to provide privacy guarantees.

Therefore, in this work, we considered a Bayesian adversary that uses the well-studied and optimal MAP estimation method [81] for estimating the source-destination identities of each observed routing path. As such, any other sub-optimal adversary is unable to perform better than our stated privacy guarantees, which considers the worst-case scenario.

4.3 System Model

In this section, we first present the network model and notation used before briefly describing the parameter identification problem, and the adversary model. We apply a similar network model and notation as used in our earlier Chapter 3 and consider the scenario where a source node wants to send a packet to a single destination node in a static multi-hop wireless network with an eavesdropping adversary. The source node must determine a routing path from itself

to the destination via a routing scheme (e.g., the shortest-path routing). We assume that source routing is used and we focus on designing a *probabilistic privacy-preserving* routing scheme (as illustrated in Fig. 4.1) that provides (k,ϵ)-*anonymity* for the communicating source-destination pair w. Our optimization variables are the observation distribution $p(\boldsymbol{y}|w)$ which determines the probability of observing $\boldsymbol{y}$ given a source-destination pair w. A motivating example for the proposed (k,ϵ)-*anonymity* (see Definition 4.2) is given in Section 4.4.

4.3.1 Network Model

We assume that only one node can transmit at any time instant and when a node transmits, all its one-hop neighbors are able to receive the transmission due to the wireless broadcast nature of the network. The graph notations (see Table 4.1) used in the this chapter are as follows:

- Let the static wireless network represented by a connected hypergraph $\mathcal{G} = (\mathcal{V}, \mathcal{H})$ where $\mathcal{V}$ represents the set of nodes and $\mathcal{H}$ represents the set of (directed) hyperarcs. A hyperarc $h = (s, \mathcal{R})$ represents a source-receivers pair where $s \in \mathcal{V}$ is the source node and $\mathcal{R} \subseteq \mathcal{V}$ is a non-empty set of receiver nodes adjacent to s.

- Let $w \triangleq (u, v)$ represent a source-destination pair, where $u \in \mathcal{V}$, $v \in \mathcal{V}$ are the source and destination nodes respectively.

- Let $\mathcal{Y}$ represent the set of all possible (observed routing) paths $\boldsymbol{y} = (h_1, h_2, \ldots)$ in the network comprising of the distinct hyperarcs h_i, and let $\mathcal{Y}^w$ be the set of all paths $\boldsymbol{y}$ that serve the source-destination pair $w = (u, v)$, i.e., $h_1 = (u, \mathcal{R}_1)$ and there exists a $h_i = (n_i, \mathcal{R}_i) \in \boldsymbol{y}$ and $v \in \mathcal{R}_i$. Note that $\boldsymbol{y}$ is not limited to a single-path only (multipath routing is possible as long as the destination node is able to receive the transmissions).

- Let $c_h \geq 0$ represent the cost (e.g., transmission or latency cost) for using a hyperarc h.

4.3.2 Preliminaries: The Parameter Identification Problem and (k,ϵ)-anonymity Property

In Bayesian theory, the unknown parameters of a model are treated as random variables with an *a priori* distribution. After observing realizations of the observations in the model, the *a priori* prior beliefs on the likely values of the parameters are updated with the observations through the likelihood and then re-quantified in the posterior distribution. This represents the conditional beliefs one holds about the likely parameter values of the model having seen a realization of the world through the observations.

In our context, the model parameters are the source-destination pair w. An adversary will hold an *a priori* belief on w, which is then updated in its posterior belief. This is achieved in the wireless routing problem, by the adversary estimating w from an observed sequence of wireless transmissions paths $\boldsymbol{y}$. However, if the model is said to be *non-identifiable*, then it is difficult to estimate the unknown parameter of interest [118], which is the source-destination pair w in our case (see Definition 4.1). This is because there could be multiple source-destination pairs that are equally likely to be the true source-destination pair.

Typically, the notation of identification of model parameters is a likelihood based concept, in which the maximum likelihood estimator is non-unique for a given observed sequence of data. In the posterior setting, we may consider a simple example where this may arise for posterior point estimation in an analogous manner. Consider the case of a non-identifiable likelihood for model parameters, say in our context w, for a given observation $\boldsymbol{y}$. Then if an uniformative prior is used by the adversary for w, the resulting posterior will have non-unique posterior maximum-a-posteriori (MAP) estimator [81]. We will consider in this sense, the notion of non-identifiability of the posterior point estimator, corresponding to the MAP estimator. Note, many classes of prior belief may result in non-unique MAP estimators, especially in the discrete network settings considered in this manuscript. We define this notion more formally below.

Definition 4.1 (Unidentifiable Source-Destination Pair)**.** *Consider the parameter space $\mathcal{W}$ and*

an observation $\boldsymbol{y}$*. A source-destination pair* $w_0 \in \mathcal{W}$ *is unidentifiable if there exists one or more* $w_1 \in \mathcal{W}$ *where* $w_1 \neq w_0$ *and* $p(w_0|\boldsymbol{y}) = p(w_1|\boldsymbol{y}) = \max_{w \in \mathcal{W}} p(w|\boldsymbol{y})$.

Identification problems may arise when the likelihood function (or observation distribution) is relatively flat, e.g., when $p(\boldsymbol{y}|w) = c$ for all $w \in \mathcal{W}$ where c is a constant. This results in the posterior probability being given by $p(w|\boldsymbol{y}) \propto p(w)$, and hence the observations $\boldsymbol{y}$ are considered non-informative. Since the unidentifiable parameters cannot be uniquely identified, they cannot be estimated consistently using Bayesian estimation methods [119]. However, in this chapter we consider identification challenges for the adversary in forming MAP estimates of w to be a significant advantage, the more we may induce this feature on the adversary's posterior beliefs, the more successful we will be at providing anonymity for w. Hence, the unidentifiable parameters are of interest to us because they impede estimation attempts by an adversary.

However, the unidentifiability property does not quantify the amount of "non-identifiability" of a parameter. Hence, we introduce the concept of (k,ϵ)-anonymity (see Definition 4.2) to quantify the amount of "non-unidentifiability" for a parameter. Mainly, we require there to be at least k number of unique source-destination pairs that have posterior probabilities *close to the maximum* posterior probability, i.e., within an ϵ tolerance of the posterior MAP probability. With respect to our wireless routing problem, the (k,ϵ)-anonymity property is a "hard" constraint that guarantees privacy for each source-destination pair w, i.e., the true source-destination pair w is safely hidden among a set of $(k-1)$ or more other distinct source-destination pairs where each w pair is just as likely to be the true source-destination pair. Note that the set of likely w pairs are commonly referred to as the anonymity set.

Definition 4.2 ((k,ϵ)-anonymity in routing)**.** *We say that a routing scheme satisfies the* (k,ϵ)*-anonymity property if for all observations* $\boldsymbol{y} \in \mathcal{Y}$*, there exist at least* k *source-destination pairs* w *that have posterior probabilities* $p(w|\boldsymbol{y})$ *within at most* ϵ *difference from the maximum posterior probability* $\max_{w \in \mathcal{V}^2} p(w|\boldsymbol{y})$ *where* $\epsilon \geq 0$*. The* (k,ϵ)*-anonymity property can be achieved*

by satisfying the following constraint:

$$\sum_{w \in \mathcal{V}^2} \mathbb{1}\Big(\max_{w' \in \mathcal{V}^2} p(w'|\boldsymbol{y}) - p(w|\boldsymbol{y}) \leq \epsilon \Big) \geq k, \qquad \forall \boldsymbol{y} \in \mathcal{Y}, \tag{4.1}$$

where $\mathbb{1}(\cdot)$ *is an indicator function which gives* 1 *if the condition inside the bracket* $(\cdot)$ *is true, and* 0 *otherwise.*

We include a small difference of ϵ in the posterior probabilities of the group of k most likely source-destination pairs. This is because from a practical point of view, the users may not distinguish between the probabilities 0.4999 and 0.5. However, depending on the network topology, not all (k,ϵ) values may be feasible. In practice, we could still obtain a flat likelihood for a sub-network of a larger network. The k value which satisfies our (k,ϵ)-anonymity Definition 4.2, can be obtained by solving for:

$$k = \min_{\boldsymbol{y} \in \mathcal{Y}} \sum_{w \in \mathcal{V}^2} \mathbb{1}\Big(\max_{w' \in \mathcal{V}^2} p(w'|\boldsymbol{y}) - p(w|\boldsymbol{y}) \leq \epsilon \Big). \tag{4.2}$$

Suppose we have a source-destination pair w_0 that has the highest posterior probability $p(w|\boldsymbol{y})$ for all observations $\boldsymbol{y} \in \mathcal{Y}$ in the worst-case scenario. Note, here we refer to the worst-case scenario to be the one in which the realized observation sequence produced the highest probability, amongst all possible observation sequences, of the true source-destination pair, that is trying to be kept anonymous from the adversary. In this case, the (k,ϵ)-anonymity condition would ensure that in this worst case, and therefore for all other possible observation sequence, there is at least $(k-1)$ or more other distinct source-destination pairs within an ϵ tolerance of the posterior MAP probability. If the (k,ϵ)-anonymity constraint in (4.1) is satisfied, then there will always be at least k source-destination pairs that are just as likely to be the true source-destination pair w_0 for each observation $\boldsymbol{y} \in \mathcal{Y}$.

4.3.3 Adversary Model

We consider an *external, passive, and global* adversary who observes a sequence of node transmissions path $\boldsymbol{y}$. The adversary's goal is to *detect the identities of the source-destination pair w for each observation $\boldsymbol{y}$*, i.e., it aims to identify which node is talking to which node. We assume that the adversary uses the detection strategy (4.5) to maximize its detection probability denoted by P_{detect}.

Adversary's Information

We assume that the adversary is *informed*, i.e., it has complete knowledge of the network graph $\mathcal{G}$, the observation distribution $p(\boldsymbol{y}|w)$, and the (k,ϵ) values used in our (k,ϵ)-anonymity scheme. In addition, the adversary may have knowledge of the prior probability for a source u to communicate with a destination v, denoted by $p(w)$ where $w \triangleq (u,v)$. In subjective Bayesian analysis [120], the prior $p(w)$ can be provided by a domain expert or inferred from a historical dataset of previous transmission paths. We consider the following two scenarios:

(i) Complete Information: In the complete information model, we assume that the adversary has complete access to the prior $p(w)$. The complete information adversary is assumed in Section 4.5.

(ii) Partial Information: In the partial information model, we assume that the adversary does not have complete access to the prior $p(w)$ and instead has a belief system on the prior, which will be studied in Section 4.6.

Adversary's Capabilities

We assume that the adversary is *external* and does not have access to the individual nodes in the network and the contents of the communications, including the packet headers, which are protected by encryption and do not leak any information on w. We also assume that the adversary is *passive* and does not manipulate the network traffic by dropping or injecting

packets to avoid detection. Lastly, we assume that the adversary has a *global* observability and perfectly observes all node transmissions in the network.

Adversary's Detection Strategy

Consider the problem of estimating w from observations $\boldsymbol{y} \in \mathcal{Y}$ related through the observation distribution $p(\boldsymbol{y}|w)$ and the prior $p(w)$. Given an observation $\boldsymbol{y}$, the adversary aims to find a good estimator for w, denoted by $\widehat{w}(\boldsymbol{y})$. To find a good estimator for w, we first define the adversary's loss function to be the commonly used binary loss function:

$$L(w, \widehat{w}(\boldsymbol{y})) = \begin{cases} 0 & \text{if } w = \widehat{w}(\boldsymbol{y}), \\ 1 & \text{otherwise.} \end{cases} \tag{4.3}$$

This means that the adversary does not incur any loss if its estimator $\widehat{w}(\boldsymbol{y})$ outputs the correct w while all other wrong estimates are penalized equally. The expected loss (or the posterior risk) is then given by:

$$\begin{aligned} \rho(w, \widehat{w}(\boldsymbol{y})) &= \sum_{w \in \mathcal{W}} L(w, \widehat{w}(\boldsymbol{y}))\, p(w|\boldsymbol{y}) \\ &= 1 - p(w = \widehat{w}(\boldsymbol{y})|\boldsymbol{y}). \end{aligned} \tag{4.4}$$

The optimal decision rule that minimizes the adversary's expected loss (4.4) is the MAP estimator, which selects the estimate for w corresponding to the maximum posterior probability, i.e.,

$$\widehat{w}(\boldsymbol{y}) = \arg\max_{w} p(w|\boldsymbol{y}). \tag{4.5}$$

This results in the minimum possible expected loss of $\rho(w, \widehat{w}(\boldsymbol{y})) = 1 - \max_{w} p(w|\boldsymbol{y})$ and the adversary's detection probability for an observation $\boldsymbol{y}$:

$$P_{\text{detect}}(\boldsymbol{y}) = p(w = \widehat{w}(\boldsymbol{y})|\boldsymbol{y}). \tag{4.6}$$

This leads to the adversary's *average detection probability* for all $\boldsymbol{y} \in \mathcal{Y}$ being:

$$P_{\text{detect}} = \sum_{\boldsymbol{y} \in \mathcal{Y}} p(w = \widehat{w}(\boldsymbol{y}) | \boldsymbol{y})\, p(\boldsymbol{y}). \tag{4.7}$$

Next, we provide a motivating example that highlights the need for strict privacy guarantees.

4.4 Motivating Example for (k, ϵ)-anonymity

We now give an example where minimizing the adversary's detection probability does not improve the privacy of a vulnerable source-destination pair.

Let w represent a source-destination pair. Suppose there are three sensitive source-destination pairs w_1, w_2, w_3 to be protected, each with some *a priori* chance of occurrence $p(w)$. Assume that there are two routing paths $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ for w_1, w_2, w_3. For instance, we let $w_1 = (1,7)$ where node 1 is the source and node 7 is the destination, and $\boldsymbol{y}_1 = (1,2,3)$ and $\boldsymbol{y}_2 = (1,4,5)$ if the destination node 7 is able to receive the packet transmissions from both $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$.

Consider the two routing schemes A and B with the observation path distributions $p(\boldsymbol{y}|w)$ listed in Table 4.2. Although both schemes have the same average adversarial detection probability of 0.5 (assuming the MAP adversary in Section 4.3.3), we say that scheme B outperforms scheme A in the context of privacy preservation when viewed from the perspective of (k, ϵ)-anonymity, according to Definition 4.2. This is because given that the adversary knows both $p(w)$ and $p(\boldsymbol{y}|w)$, it always selects w_1 as the actual source-destination pair every time $\boldsymbol{y}_1$ is observed in scheme A as this corresponds to the MAP posterior outcome, see Fig. 4.2. This makes w_1 vulnerable and not private (compared to w_2 and w_3) in scheme A as the adversary always selects w_1. In the event that the adversary is able to compromise the wireless node, then w_1 will always be compromised.

On the other hand, if scheme B is used, then both w_1 and w_2 are equally likely to be selected if $\boldsymbol{y}_1$ is observed (see Fig. 4.2), and w_1 and w_3 are equally likely to be selected if $\boldsymbol{y}_2$ is observed. Hence, w_1 is less vulnerable in scheme B as it only gets selected with 0.5 probability for any

Table 4.2: Adversary's detection probability P_{detect} for routing schemes A and B and ϵ is approximately zero.

		Scheme A ($k=1$)		**Scheme B** ($k=2$)	
parameter w	prior $p(w)$	path 1 $p(\boldsymbol{y}_1\|w)$	path 2 $p(\boldsymbol{y}_2\|w)$	path 1 $p(\boldsymbol{y}_1\|w)$	path 2 $p(\boldsymbol{y}_2\|w)$
w_1	0.5	1	0	0.5	0.5
w_2	0.25	1	0	1	0
w_3	0.25	1	0	0	1
P_{detect}		0.5		0.5	

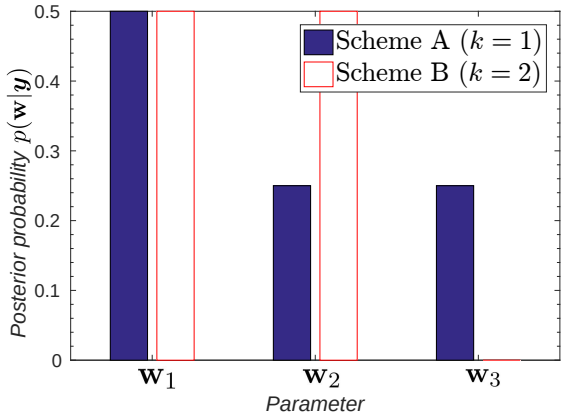


Figure 4.2: Posterior probability $p(w|\boldsymbol{y})$ distribution of w_1, w_2, w_3 under routing schemes A and B for path $\boldsymbol{y}_1$.

given observation $\boldsymbol{y}$. Therefore, we say that scheme B offers greater privacy guarantees since there are always $k=2$ equally likely source-destination pairs for any observation $\boldsymbol{y}$ whereas $k=1$ in scheme A due to the vulnerable w_1.

Note that our example also highlights the fact that scheme A, which is basically a flooding scheme does not always provide the highest possible level of privacy guarantees.

4.5 Optimizing for Privacy Guarantees

In this section, we present a statistical decision-making framework that minimizes the expected cost of the privacy-preserving routing scheme that achieves the (k,ϵ)-anonymity property in Definition 4.2 via probabilistic routing. To achieve this, we set the observation path distribution $p(\boldsymbol{y}|w)$ as the optimization variable in our cost minimization problem. The

optimization problem is solved by the source node u and if the source node finds a $p(\boldsymbol{y}|w)$ distribution that achieves (k,ϵ)-anonymity, then it can achieve the desired privacy preservation by transmitting according to the $p(\boldsymbol{y}|w)$ probabilities.

We first describe the objective function and constraints of our routing cost minimization problem before providing its mixed-integer linear programing (MILP) formulation.

4.5.1 Objective Function

Our objective is to minimize the expected cost of the (k,ϵ)-anonymous routing scheme. Let $c_h \geq 0$ represent the cost, e.g., transmission cost for using hyperarc h. For a given source-destination pair w, we define the cost of using a routing path $\boldsymbol{y}$ to be the sum of the costs of each hyperarc $h \in \boldsymbol{y}$ in the path, i.e., $\sum_{h\in\boldsymbol{y}} c_h$. Thus, the cost of using the minimum-cost path that serves w is simply $\min_{\boldsymbol{y}'\in\mathcal{Y}^w} \sum_{h\in\boldsymbol{y}'} c_h$. Due to the probabilistic nature of our routing scheme, the expected cost of using a (k,ϵ)-anonymous path is defined as the expectation of the costs of each path over all possible paths, i.e., $\mathbb{E}_{\boldsymbol{y}\in\mathcal{Y}}\Big[\sum_{h\in\boldsymbol{y}} c_h\Big]$.

Next, we define the additional transmission cost incurred by the (k,ϵ)-anonymous routing scheme for a given w to be the difference between the expected cost of using the (k,ϵ)-anonymous path and the cost of using the minimum cost path, i.e., $\mathbb{E}_{\boldsymbol{y}\in\mathcal{Y}}\Big[\sum_{h\in\boldsymbol{y}} c_h\Big] - \min_{\boldsymbol{y}'\in\mathcal{Y}^w} \sum_{h\in\boldsymbol{y}'} c_h$.

Finally, we define the cost of the (k,ϵ)-anonymous routing scheme to be given by the *expected amount of additional transmission cost incurred by the network*:

$$\begin{aligned}
&\mathbb{E}_{w\in\mathcal{V}^2}\left[\mathbb{E}_{\boldsymbol{y}\in\mathcal{Y}}\Big[\sum_{h\in\boldsymbol{y}} c_h\Big] - \min_{\boldsymbol{y}'\in\mathcal{Y}^w} \sum_{h\in\boldsymbol{y}'} c_h\right] \\
&= \sum_{w\in\mathcal{V}^2} p(w)\left[\Big[\sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w) \sum_{h\in\boldsymbol{y}} c_h\Big] - \min_{\boldsymbol{y}'\in\mathcal{Y}^w} \sum_{h\in\boldsymbol{y}'} c_h\right]. \qquad (4.8)
\end{aligned}$$

4.5.2 Network and Privacy Constraints

In order to correctly specify our (k,ϵ)-anonymous routing problem, our formulation must include: (i) the (k,ϵ)-anonymity constraint, (ii) the valid $p(\boldsymbol{y}|w)$ probabilities that satisfy the Kolmogorov's probability axioms, and (iii) the valid routing paths $\boldsymbol{y}$ for the specified network topology. Consider the following constraints:

Privacy constraint: The (k,ϵ)-anonymity property is achieved by satisfying the constraint stated in Definition 4.2:

$$\sum_{w\in\mathcal{V}^2} \mathbb{1}\Big(\max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y}) - p(w|\boldsymbol{y}) \leq \epsilon \Big) \geq k, \qquad \forall\, \boldsymbol{y}\in\mathcal{Y}.$$

Non-negativity of probabilities: A valid probability has to be non-zero and less than one.

$$0 \leq p(\boldsymbol{y}|w) \leq 1, \qquad \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2. \tag{4.9}$$

Sum of probabilities over support: The summation of the observation distribution $p(\boldsymbol{y}|w)$ over its entire support $\mathcal{Y}$ must equal one.

$$\sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w) = 1, \qquad \forall\, w\in\mathcal{V}^2. \tag{4.10}$$

Valid transmissions: The source node u by definition must be the first node that transmitted while the destination node v must receive the transmission at some point in the sequence of routing path $\boldsymbol{y}$. Hence, the following constraint restricts the valid paths $\boldsymbol{y}$ that serve the source-destination pair w.

$$p(\boldsymbol{y}|w) = 0, \qquad \forall\, \boldsymbol{y}\notin\mathcal{Y}^w, w\in\mathcal{V}^2. \tag{4.11}$$

$$\underline{\text{PrivProb}\left(\mathcal{G},\{c_h\}_{h\in\mathcal{H}},\{p(w)\}_{w\in\mathcal{V}^2},k,\epsilon\right)}:$$

$$\begin{aligned}
\underset{\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}}{\text{minimize}} \quad & \sum_{w\in\mathcal{V}^2} p(w)\Big[\big[\sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)\sum_{h\in\boldsymbol{y}} c_h\big] - \min_{\boldsymbol{y}'\in\mathcal{Y}^w}\sum_{h\in\boldsymbol{y}'} c_h\Big], & \\
\text{subject to} \quad & 0\le p(\boldsymbol{y}|w)\le 1, & \forall\,\boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2 \\
& \sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)=1, & \forall\, w\in\mathcal{V}^2 \\
& p(\boldsymbol{y}|w)=0, & \forall\,\boldsymbol{y}\notin\mathcal{Y}^w, w\in\mathcal{V}^2 \\
& \sum_{w\in\mathcal{V}^2}\mathbb{1}\Big(\max_{w'} p(w'|\boldsymbol{y})-p(w|\boldsymbol{y})\le\epsilon\Big)\ge k, & \forall\,\boldsymbol{y}\in\mathcal{Y}.
\end{aligned}$$

4.5.3 Problem Formulation: (k,ϵ)-anonymity for Privacy Guarantees

Problem PrivProb attempts to minimize the expected cost of the proposed (k,ϵ)-anonymous routing scheme. Note that the $p(w|\boldsymbol{y})$ term in the last constraint of Problem PrivProb can be explicitly expressed in terms of the optimization variables $p(\boldsymbol{y}|w)$ using Bayes' rule, i.e., $p(w|\boldsymbol{y})=\frac{p(\boldsymbol{y}|w)p(w)}{\sum_{w\in\mathcal{V}^2}p(\boldsymbol{y}|w)p(w)}$.

Mixed Integer Linear Programing (MILP) Formulation

Problem PrivProb is non-linear due to the privacy constraint (4.1). However, it can be reformulated as the MILP given in Problem PrivMILP by replacing (4.1) using the additional constraints (4.12)–(4.15). Mainly, to linearize (4.1), we first introduce the binary indicator variables $i_{\boldsymbol{y},w}$ to estimate $\mathbb{1}\Big(\max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y})-p(w|\boldsymbol{y})\le\epsilon\Big)$ for each observation $\boldsymbol{y}\in\mathcal{Y}$ and source-destination pair $w\in\mathcal{V}^2$. Next, we introduce the variables $m_{\boldsymbol{y}}$ to estimate $\max_{w'\in\mathcal{V}^2} p(w',\boldsymbol{y})$ for each $\boldsymbol{y}$, and finally, we have the following constraints:

(i) The sum of the indicator variables $i_{\boldsymbol{y},w}$ should be greater than or equal to k:

$$\sum_{w\in\mathcal{V}^2} i_{\boldsymbol{y},w}\ge k, \qquad \forall\,\boldsymbol{y}\in\mathcal{Y}. \tag{4.12}$$

(ii) The indicator variable $i_{\boldsymbol{y},w}$ can only be set to one when $\max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y})-p(w|\boldsymbol{y})\le\epsilon$. By definition of the max term, we have the constraint: $\max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y})\ge p(w|\boldsymbol{y}),\forall\,\boldsymbol{y}\in\mathcal{Y}$, which is

PrivMILP $(\mathcal{G}, \{c_h\}_{h\in\mathcal{H}}, \{p(w)\}_{w\in\mathcal{V}^2}, k, \epsilon)$:

$$\begin{aligned}
\underset{\substack{\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2},\\ \{i_{\boldsymbol{y},w}\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2},\\ \{m_{\boldsymbol{y}}\}_{\boldsymbol{y}\in\mathcal{Y}}}}{\text{minimize}} \quad & \sum_{w\in\mathcal{V}^2} p(w)\Big[\big[\sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w)\sum_{h\in\boldsymbol{y}} c_h\big] - \min_{\boldsymbol{y}'\in\mathcal{Y}^w}\sum_{h\in\boldsymbol{y}'} c_h\Big], \\
\text{subject to} \quad & 0 \le p(\boldsymbol{y}|w) \le 1, && \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2 \\
& \sum_{\boldsymbol{y}\in\mathcal{Y}} p(\boldsymbol{y}|w) = 1, && \forall\, w\in\mathcal{V}^2 \\
& p(\boldsymbol{y}|w) = 0, && \forall\, \boldsymbol{y}\notin\mathcal{Y}^w, w\in\mathcal{V}^2 \\
& \sum_{w\in\mathcal{V}^2} i_{\boldsymbol{y},w} \ge k, && \forall\, \boldsymbol{y}\in\mathcal{Y} \\
& m_{\boldsymbol{y}} \ge p(\boldsymbol{y}|w)p(w), && \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2 \\
& m_{\boldsymbol{y}} - p(\boldsymbol{y}|w)p(w) \le 1 - i_{\boldsymbol{y},w} + \epsilon\Big(\sum_{w\in\mathcal{V}^2} p(\boldsymbol{y}|w)p(w)\Big), && \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2 \\
& i_{\boldsymbol{y},w} = 0 \text{ or } 1, && \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2.
\end{aligned}$$

equivalent to $m_{\boldsymbol{y}} \ge p(w,\boldsymbol{y}), \forall\, \boldsymbol{y}\in\mathcal{Y}$, where $m_{\boldsymbol{y}}$ is used to represent the term $\max_{w'\in\mathcal{V}^2} p(w',\boldsymbol{y})$. For each $w\in\mathcal{V}^2$, we observe that $m_{\boldsymbol{y}} - p(\boldsymbol{y}|w)p(w) \le 1, \forall\, \boldsymbol{y}\in\mathcal{Y}$, is always true for all $p(\boldsymbol{y}|w)$ values, while $m_{\boldsymbol{y}} - p(\boldsymbol{y}|w)p(w) \le 0, \forall\, \boldsymbol{y}\in\mathcal{Y}$, is only true if $m_{\boldsymbol{y}} - p(\boldsymbol{y},w) \le \epsilon\Big(\sum_{w\in\mathcal{V}^2} p(\boldsymbol{y}|w)p(w)\Big)$. Hence, the following constraint (4.13) ensures that the correctness of the indicator variables $i_{\boldsymbol{y},w}$.

$$m_{\boldsymbol{y}} - p(\boldsymbol{y}|w)p(w) \le 1 - i_{\boldsymbol{y},w} + \epsilon\Big(\sum_{w\in\mathcal{V}^2} p(\boldsymbol{y}|w)p(w)\Big), \quad \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2. \tag{4.13}$$

(iii) The variable $m_{\boldsymbol{y}}$ by definition of $\max_{w'\in\mathcal{V}^2} p(w',\boldsymbol{y})$ should satisfy:

$$m_{\boldsymbol{y}} \ge p(\boldsymbol{y}|w)p(w), \qquad \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2. \tag{4.14}$$

(iv) We limit the values of the indicator variables $i_{\boldsymbol{y},w}$ to either 0 or 1:

$$i_{\boldsymbol{y},w} = 0 \text{ or } 1, \qquad \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2. \tag{4.15}$$

We show using Lemma 4.1 that Problems PrivProb and PrivMILP are equivalent. While the MILP formulation in Problem PrivMILP is still non-convex, its constraints (except the binary

variable constraints) are linear. This enables LP-relaxation-based techniques to be used for efficiently solving the problem. Solving MILP problems are addressed in [121] and efficient techniques for solving MILP like branch-and-bound algorithms have been developed [122], which have been widely studied and supported in many commercial solvers. In addition, Problem PrivMILP can be easily decomposed into smaller sub-problems for each source node u to solve in a distributed manner as there are no complicating variables between the different source nodes.

Lemma 4.1. *Problems PrivProb and PrivMILP are equivalent, i.e., the optimal solution* $\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ *obtained by solving Problem PrivProb is also an optimal solution of Problem PrivMILP and vice versa.*

Proof. Suppose we obtain the solution $\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ by solving Problem PrivMILP. Let $\mathcal{I}$ be the set of $i_{\boldsymbol{y},w}$ variables where $i_{\boldsymbol{y},w}=1$. For each $\boldsymbol{y}\in\mathcal{Y}$ and $w\in\mathcal{V}^2$ where $i_{\boldsymbol{y},w}\in\mathcal{I}$, the following constraint must be true due to constraints (4.13) and (4.14) of Problem PrivMILP:

$$p(\boldsymbol{y}|w)p(w) \le m_{\boldsymbol{y}} \le p(\boldsymbol{y}|w)p(w) + \epsilon\left(\sum_{w\in\mathcal{V}^2} p(\boldsymbol{y}|w)p(w)\right). \tag{4.16}$$

If we divide (4.16) by the constant term $p(\boldsymbol{y})$ (or equivalently $\sum_{w\in\mathcal{V}^2} p(\boldsymbol{y}|w)p(w)$), we obtain:

$$p(w|\boldsymbol{y}) \le \frac{m_{\boldsymbol{y}}}{p(\boldsymbol{y})} \le p(w|\boldsymbol{y}) + \epsilon, \tag{4.17}$$

for each $\boldsymbol{y}\in\mathcal{Y}$ and $w\in\mathcal{V}^2$ where $i_{\boldsymbol{y},w}\in\mathcal{I}$.

Separately, the expression inside the indicator function in constraint (4.1) of Problem PrivProb can be expressed as:

$$p(w|\boldsymbol{y}) - \epsilon \le \max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y}) \le p(w|\boldsymbol{y}) + \epsilon. \tag{4.18}$$

However, the max term in (4.18), should by definition satisfy:

$$p(w|\boldsymbol{y}) \le \max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y}), \forall\, \boldsymbol{y}\in\mathcal{Y}, w\in\mathcal{V}^2.$$

This means if the solution $\{p'(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ satisfies constraint (4.1) of Problem PrivProb, then it should also satisfy the tighter bound:

$$p(w|\boldsymbol{y}) \leq \max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y}) \leq p(w|\boldsymbol{y}) + \epsilon. \tag{4.19}$$

Thus, if the optimal solution $\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ of Problem PrivMILP satisfies constraint (4.18), then it also satisfies constraint (4.19) of Problem PrivProb since $m_{\boldsymbol{y}}/p(\boldsymbol{y})$ and $\max_{w'\in\mathcal{V}^2} p(w'|\boldsymbol{y})$ are both functions of $p(\boldsymbol{y}|w)$. This means that $\{p(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ is also a feasible solution in Problem PrivProb.

Similarly, suppose we obtain the solution $\{p'(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ by solving Problem PrivProb. If $\{p'(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ satisfies constraint (4.19) in Problem PrivProb, then it also satisfies constraint (4.17) of Problem PrivMILP. Hence, the optimal solution $\{p'(\boldsymbol{y}|w)\}_{\boldsymbol{y}\in\mathcal{Y},w\in\mathcal{V}^2}$ is also a feasible solution in Problem PrivMILP. Given that the objective functions of Problems PrivProb and PrivMILP are the same, and that the optimal solutions for both problems are also feasible solutions for the other problem, we conclude that Problems PrivProb and PrivMILP are equivalent. □

Computation Complexity and Heuristic Pruning

The computational cost for solving the MILP problem is influenced by the number of variables $p(\boldsymbol{y}|w)$ and more importantly, the number of integer variables $i_{\boldsymbol{y},w}$ and the number of constraints. The number of variables and constraints in Problem PrivMILP is proportional to the set of all possible paths $\mathcal{Y}$ in the network and the number of possible source-destination pair $\mathcal{V}^2$. While the size of $\mathcal{V}^2$ is fixed for a given network size, the size of $\mathcal{Y}$ depends heavily on the network topology, e.g., a denser network where every node has a large number of neighbors will have a larger set of $\mathcal{Y}$ compared to a sparser network of the same size. To reduce the optimization problem size, we can pre-prune the non-feasible paths $\boldsymbol{y} \notin \mathcal{Y}^w$, which in turn reduces the number of optimization variables $p(\boldsymbol{y}|w)$ and $i_{\boldsymbol{y},w}$. In addition, the size of $\mathcal{Y}$ can be further reduced by pruning paths that serve less than k source-destination pairs since the

paths clearly cannot achieve the (k,ϵ)-anonymity property.

4.6 Adversary Belief System Analysis

In this section, we consider an adversary that does not have complete information on the true prior $p(w)$ and study how it can strategically assign its prior $p_a(w)$ for the estimator $\widehat{w}(\boldsymbol{y})$. This is useful as it allows us to estimate the adversary's P_{detect} value given its prior $p_a(w)$. As the adversary may only have limited or no access to a historical dataset, its estimate $\widehat{w}(\boldsymbol{y})$ may not match the actual source-destination pair w when $p_a(w) \neq p(w)$. In other words, there could be a model mismatch for the adversary. Although the MAP estimator minimizes the adversary's expected loss, it may not be effective for an adversary with only partial information as it has to assign a prior $p_a(w)$, which may not correspond to the true prior $p(w)$. Hence, the adversary may use a uniform prior for $p_a(w)$ (see objective Bayesian analysis [120]). By Lemma 4.2, the uniform prior gives equal weights to all possible w pairs and reduces the expected loss in the event that $p_a(w)$ differs greatly from $p(w)$.

It is well-known that Bayesian methods may be strongly influenced by a given prior choice. It is interesting therefore to see the effects of a poorly chosen adversary *a priori* beliefs. To study this, we apply the concepts from decision theory and define a risk function to evaluate the appropriateness of an adversary's chosen prior $p_a(w)$, and how it affects the adversary's detection probability P_{detect}. First, we define the Bayes risk to be the expectation of the posterior risk function (4.4) over all observations $\boldsymbol{y} \in \mathcal{Y}$:

$$\begin{aligned} r(w, \widehat{w}(\boldsymbol{y})) &= \sum_{\boldsymbol{y}\in\mathcal{Y}} \rho(w, \widehat{w}(\boldsymbol{y}))\, p(\boldsymbol{y}) \\ &= \sum_{\boldsymbol{y}\in\mathcal{Y}} \Big(1 - p(w = \widehat{w}(\boldsymbol{y})|\boldsymbol{y})\Big)\, p(\boldsymbol{y}). \end{aligned} \tag{4.20}$$

The Bayes risk depends on the prior $p(w)$, posterior risk function $\rho(w, \widehat{w}(\boldsymbol{y}))$, the estimator $\widehat{w}(\boldsymbol{y})$, and implicitly, the prior $p_a(w)$ used by the estimator.

Next, we have the following Lemma 4.2, which states that the uniform prior always minimizes

the maximum adversary's Bayes risk.

Lemma 4.2. *Assume that the prior $p(w)$ is unknown to the adversary. The uniform prior $p_a(w) = 1/|\mathcal{V}^2|, \forall\, w \in \mathcal{V}^2$, used to construct the estimator $\widehat{w}(\boldsymbol{y})$ always minimizes the maximum adversary's Bayes risk, i.e.,*

$$\max_{p(w)\in\Theta} r(w, \widehat{w}(\boldsymbol{y})) \leq \max_{p(w)\in\Theta} r(w, \widehat{w}'(\boldsymbol{y})), \forall\, \widehat{w}'(\boldsymbol{y}) \in \widehat{\mathcal{W}},$$

where $\widehat{\mathcal{W}}$ is the set of possible estimators.

Proof. From (4.20), we obtain the maximum Bayes risk:

$$\max_{p(w)\in\Theta} r(w, \widehat{w}(\boldsymbol{y})) = \max_{p(w)\in\Theta} \sum_{\boldsymbol{y}\in\mathcal{Y}} \Big(1 - p(w = \arg\max_{\widehat{w}(\boldsymbol{y})} p(\widehat{w}(\boldsymbol{y})|\boldsymbol{y}))\Big) p(\boldsymbol{y}).$$

Suppose there exists a $p(w) \in \Theta$ where $p(w) = 1$ for some arbitrary w' and $p(w) = 0$ for all other $w \in \mathcal{V}^2$ where $w \neq w'$. For any given $p_a(w)$ and $p(\boldsymbol{y}|w)$, the maximum Bayes risk occurs when $w' = \arg\min_{w\in\mathcal{V}^2} \sum_{\boldsymbol{y}\in\mathcal{Y}} p(w, \boldsymbol{y})$. Given that the adversary can choose between the uniform prior denoted by $p_{a_{\text{unif}}}(w)$ and a non-uniform prior $p_{a_{\text{non-unif}}}(w)$, it is obvious that $\min_{w\in\mathcal{V}^2} p_{a_{\text{unif}}}(w) > \min_{w\in\mathcal{V}^2} p_{a_{\text{non-unif}}}(w)$. Therefore, the uniform prior $p_{a_{\text{unif}}}(w)$ always minimizes the adversary's maximum Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$. □

Finally, we analyze how $p(w)$ affects the adversary's Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$ under two special cases - the flooding scenario, and conjugate model assumption. This allows us to estimate the adversary's P_{detect} values under the proposed (k, ϵ)-anonymity scheme.

4.6.1 Flooding Scenario

To evaluate how $p(w)$ affects the adversary's Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$, we define the least favorable prior in Definition 4.3. The least favorable prior, from an adversary's perspective leads to the maximum Bayes risk, which is the worst case for the adversary's decision making. Suppose that each source node u uses the flooding approach to communicate with its destination node

v, Lemma 4.3 states that the uniform prior is least favorable for the adversary. However, given that the adversary has only limited or no access to a historical dataset and needs to assign the prior $p_a(w)$ for its estimator $\widehat{w}(\boldsymbol{y})$, by Lemma 4.2, the uniform prior always minimizes the maximum adversary's Bayes risk.

Definition 4.3 (Least Favorable Prior)**.** *Let Θ be the function space corresponding to all possible priors on the source-destination pairs. A prior distribution $p(w)$ is least favorable if $r(w,\widehat{w}(\boldsymbol{y})) \geq r(p(w),\widehat{w}(\boldsymbol{y}))$, $\forall\, p(w) \in \Theta$.*

Lemma 4.3. *Consider a flooding scenario where the observation distribution $p(\boldsymbol{y}'|w) = 1, \forall\, w \in \mathcal{V}^2$, for a specific $\boldsymbol{y}'$, and $p(\boldsymbol{y}|w) = 0$ for all $\boldsymbol{y} \in \mathcal{Y}$ where $\boldsymbol{y} \neq \boldsymbol{y}'$. Assume that the prior $p(w)$ is known to the adversary, the uniform prior where $p(w) = 1/|\mathcal{V}^2|$, $\forall\, w \in \mathcal{V}^2$, is least favorable.*

Proof. From (4.20), the Bayes risk under the MAP estimator is given by

$$r(w,\widehat{w}(\boldsymbol{y})) = \sum_{\boldsymbol{y}\in\mathcal{Y}} \left(1 - \max_{\widehat{w}(\boldsymbol{y})} p(\widehat{w}(\boldsymbol{y})|\boldsymbol{y})\right) p(\boldsymbol{y}). \tag{4.21}$$

The max term in (4.21) (which is related to P_{detect} (4.7)) is minimized when $p(w)$ is uniformly distributed in the parameter space $\mathcal{V}^2$. This leads to the maximum $r(w,\widehat{w}(\boldsymbol{y}))$ for the adversary. Additionally, (k,ϵ)-anonymity is achieved where $k = |\mathcal{V}| - 1$ since the posterior distribution $p(w|\boldsymbol{y})$ is uniform in $\mathcal{V} - 1$ when $p(w)$ is uniform and $p(\boldsymbol{y}'|w) = 1, \forall\, w \in \mathcal{V}^2$, for a specific $\boldsymbol{y}'$. This results in the lowest possible P_{detect} value of $1/(|\mathcal{V}| - 1)$. Therefore, we have shown that the uniform prior distribution $p(w)$ is least favorable. □

4.6.2 Conjugate Prior Assumption

Assume that the adversary has complete information on the prior $p(w)$. A closed-form expression of the adversary's risk function can be derived analytically using the conjugate prior assumption [123]. For example, if we assume the geometric-beta conjugate prior model, and approximate $p(\boldsymbol{y}|w)$ with the path length observation distribution $p(l|w)$ where l represents the length of the routing path, i.e., $p(l|w)$ comes from a geometric distribution with parameter

p_l and the prior $p(w)$ comes from a beta distribution with parameters (α, β), then the posterior distribution $p(w|\boldsymbol{y})$ also comes from a beta distribution with parameters $(\alpha + n, \beta + \sum_{i=1}^{n} l_i)$, where n is the number of observations and $l_i \in \mathcal{L}$ is the observed path length for the ith observation.

The conjugate prior assumption is analytically convenient and allows us to study the relationship between the adversary's prior beliefs and its corresponding Bayes risk. The beta distribution is commonly used in Bayesian statistical analyses and is appropriate as its support has a limited range from 0 to 1, which gives a valid prior probability in our case. More importantly, the beta distribution has exceptional shape flexibility [124] and allow values to be specified between an upper and lower bound. Thus, the distribution is general enough to model the prior $p(w)$ probabilities. The beta distribution has two parameters, commonly denoted by α and β, and is symmetrical when $\alpha = \beta$. Otherwise, the distribution becomes skewed towards certain values as the difference between α and β increases. The mode of the beta distribution happens at $\frac{\alpha+n-1}{\alpha+n+\beta+\sum_{i=1}^{n} l_i-2}$, and hence, from (4.20), the adversary's Bayes risk is given by

$$\begin{aligned} r(w, \widehat{w}(\boldsymbol{y})) &= \sum_{l \in \mathcal{L}} \Big(1 - \frac{\alpha + n - 1}{\alpha + n + \beta + \sum_{i=1}^{n} l_i - 2}\Big) p(l) \\ &= \sum_{l \in \mathcal{L}} \sum_{w \in \mathcal{V}^2} \Big(1 - \frac{\alpha + n - 1}{\alpha + n + \beta + \sum_{i=1}^{n} l_i - 2}\Big) p(l, w), \end{aligned} \tag{4.22}$$

where $p(l|w) = (1 - p_l)^l p_l$ and $p(w) = w^{\alpha-1}(1-w)^{\beta-1} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}$.

Next, we study the sensitivity of the adversary's Bayes risk and how the (α, β) parameters of the prior $p(w)$ affect the Bayes risk using Lemma 4.4.

Lemma 4.4. *The sensitivity of the adversary's Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$ are as follows:*

$$\begin{aligned} \frac{\partial r(w, \widehat{w}(\boldsymbol{y}))}{\partial \alpha} &= \sum_{l \in \mathcal{L}} \frac{1 - \beta - \sum_{i=1}^{n} l_i}{(\alpha + \beta + n + \sum_{i=1}^{n} l_i - 2)^2} p(l), \\ \frac{\partial r(w, \widehat{w}(\boldsymbol{y}))}{\partial \beta} &= \sum_{l \in \mathcal{L}} \frac{\alpha + n - 1}{(\alpha + \beta + n + \sum_{i=1}^{n} l_i - 2)^2} p(l). \end{aligned} \tag{4.23}$$

Proof. The partial derivatives of the Bayes risk are obtained by differentiating the Bayes risk

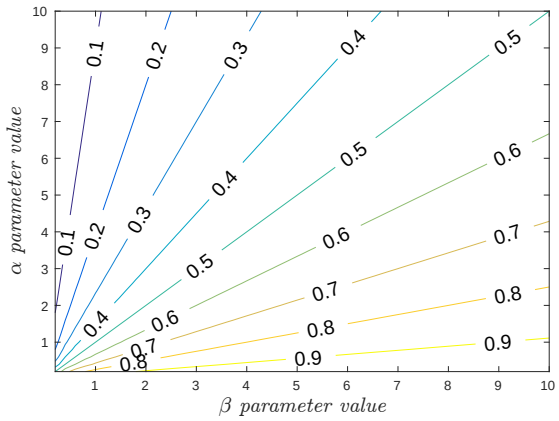
$r(w, \widehat{w}(\boldsymbol{y}))$ term in (4.22) with respect to parameters α and β respectively. □

To visualize the gradient of the Bayes risk, we set $p_l = 0.8$ (non-flat likelihood) and show the contour map for the Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$ and its gradient in Fig. 4.3 for $n = 2$ and Fig. 4.4 for $n = 20$. From the figures, we observe that the uniform prior (where $\alpha = \beta = 1$) may not necessarily result in the maximum Bayes risk for the adversary when the likelihood is not flat. However, it is clear that the α parameter caused a greater change in the gradient of the Bayes risk and thus, played a larger role in the Bayes risk compared to the β parameter. A similar pattern is observed when n is varied although the gradient of the Bayes risk decreased as n is increased. Also, the gradient of the α and β parameters increased when p_l is increased and vice versa. Other conjugate prior models, e.g., the Poisson-Gamma conjugate prior model may also be used when appropriate.

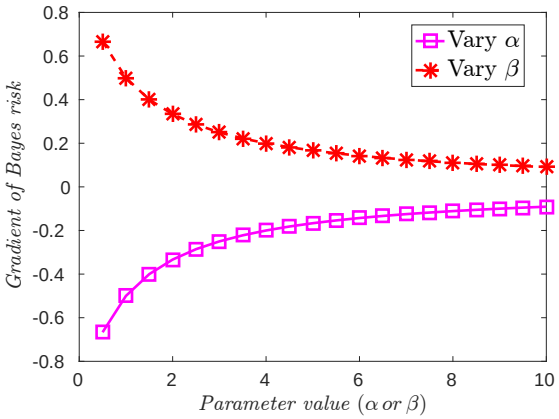
4.7 Simulation Results and Discussion

In this section, we study how our proposed (k, ϵ)-anonymity scheme (i.e., Problem PrivMILP) performs against a baseline scheme [65] (our work described in Chapter 3) that uses the optimization approach to minimize the average adversary detection probability P_{detect} (4.7) without providing privacy guarantees for each source-destination pair w. Recall from our adversarial model in Section 4.3.3 that the adversary seeks to maximize P_{detect} (i.e., look for source-destination pair with the highest posterior probability $p(w|\boldsymbol{y})$ value) while our proposed (k, ϵ)-anonymity scheme ensures that for each observation $\boldsymbol{y}$, there are at least k or more distinct source-destination pairs that are likely (within an ϵ tolerance of the maximum-a-posteriori probability [see (4.1)]) to be the true source-destination pair. In the second part of this section, we analyze how the adversary's belief system for the prior $p(w)$ affects its P_{detect} values.

Performance metric: We plot the anonymity set size curve for the proposed (k, ϵ)-anonymity scheme and the baseline scheme [65] to study the amount of privacy guarantees provided by the schemes. For a fixed cost incurred in expectation, we consider the routing scheme with a

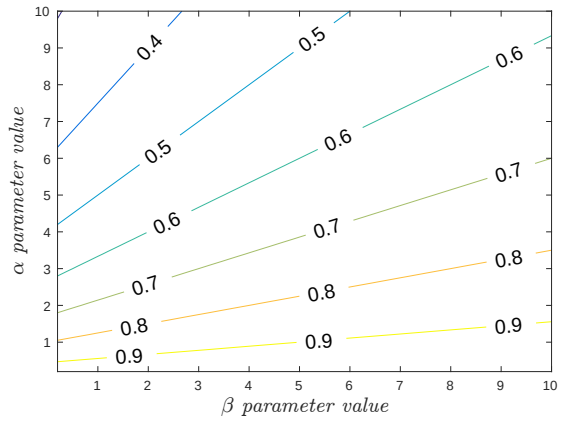


(a) Contour plot of Bayes risk for $n = 2$.

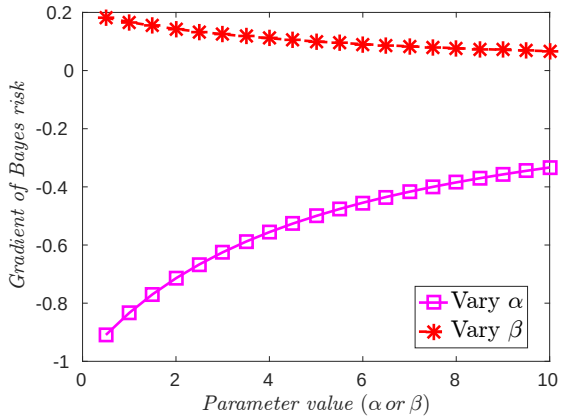


(b) Bayes risk gradient for $n = 2$.

Figure 4.3: Adversary's Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$ and its gradient for $p_l = 0.8$, and $n = 2$.



(a) Contour plot of Bayes risk for $n = 20$.



(b) Bayes risk gradient for $n = 20$.

Figure 4.4: Adversary's Bayes risk $r(w, \widehat{w}(\boldsymbol{y}))$ and its gradient for $p_l = 0.8$, and $n = 20$.

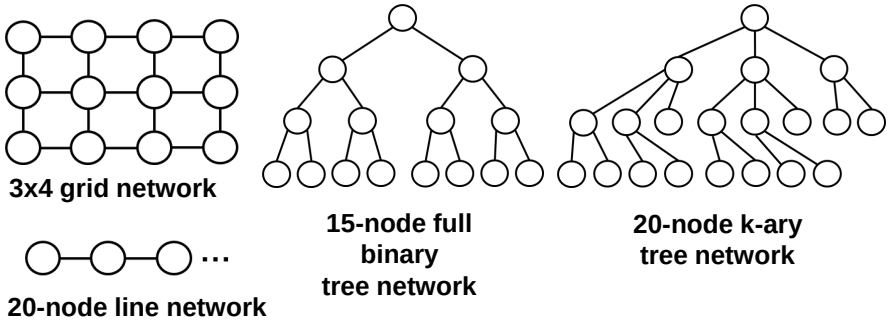


Figure 4.5: Used network topologies in our simulation.

larger anonymity set size k value to be the superior one in terms of privacy preservation of w. For comparison purposes, we also plot the adversary's detection probability curve. Note that in general, a lower P_{detect} value also provides privacy for w. However, in this work, we focus on providing strict privacy guarantees. As such, we place more importance in the k values.

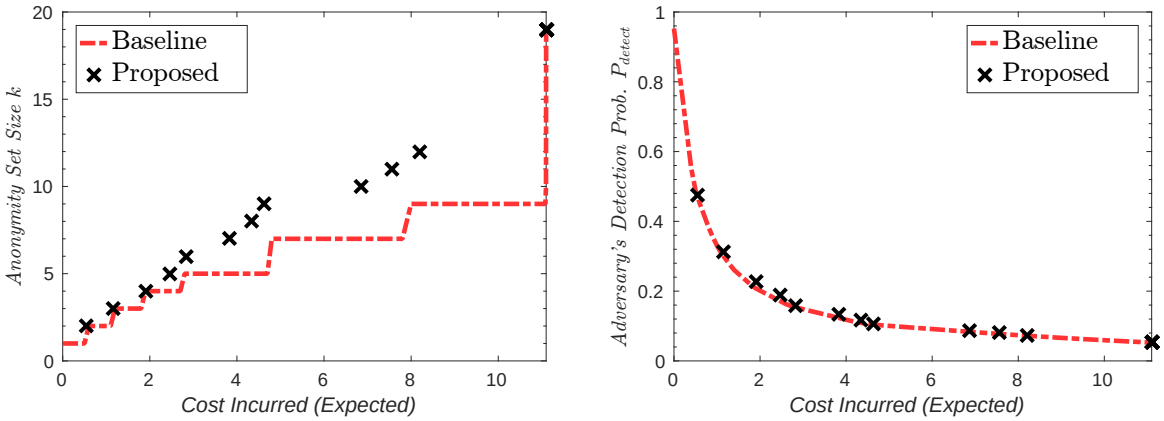
Implementation details: The anonymity set size and adversary's detection probability curves are obtained by repeatedly solving the optimization problems for each cost incurred (granularity of 1 and 0.1 respectively) and computing its corresponding k and P_{detect} values. We used the intlinprog and linprog functions from MATLAB's Optimization Toolbox [125] to solving the formulated Problem PrivMILP and the baseline scheme [65, DLPProb] respectively. After testing various optimization parameters for the intlinprog solver, we found the following parameters to be better in terms of solving time and accuracy: 'CutMaxIterations' = 50, 'CutGeneration' = advanced, 'HeuristicsMaxNodes' = 100.

We now discuss our findings under various network settings.

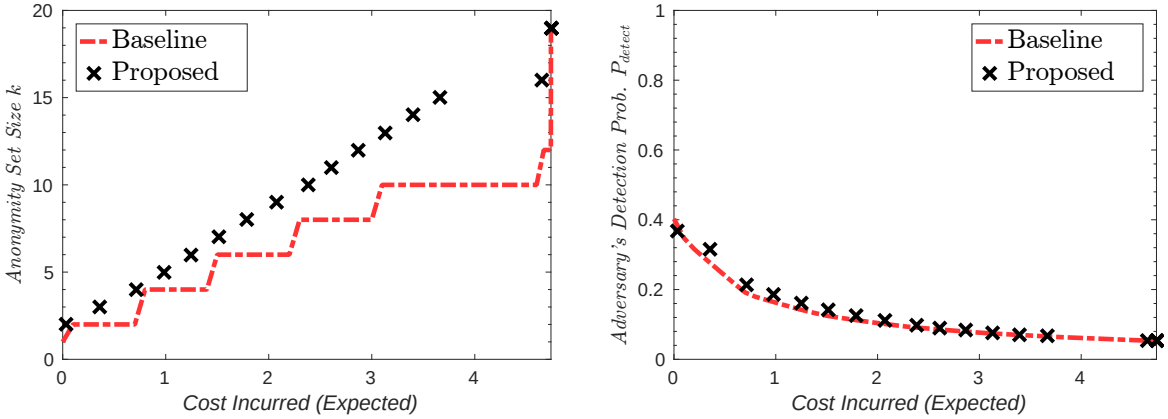
4.7.1 Comparison with Baseline P_{detect} Minimization Scheme

We study how our proposed (k,ϵ)-anonymity scheme performs against the baseline scheme [65] that minimizes P_{detect} without providing privacy guarantees. Note that the baseline scheme was proposed in Chapter 3. We used a uniform prior $p(w)$ for the source-destination pairs w and set ϵ to be approximately zero. Our chosen ϵ value is most conservative and so not all k values may be feasible in every network. The schemes were evaluated using the basic (line, binary tree, a k-ary tree, and grid) network topologies shown in Fig. 4.5. The chosen topologies represent some basic topologies common in wireless networks and we used small (12–20 nodes) networks as we believe it is unlikely that a wireless node needs to communicate with a large number of destination nodes. We vary the k value for our proposed (k,ϵ)-anonymity scheme and vary the expected cost incurred in the baseline scheme [65] to obtain their corresponding P_{detect} (4.7) and k values (4.2).

There exists a privacy-cost trade-off between providing (k,ϵ)-anonymity privacy guarantees

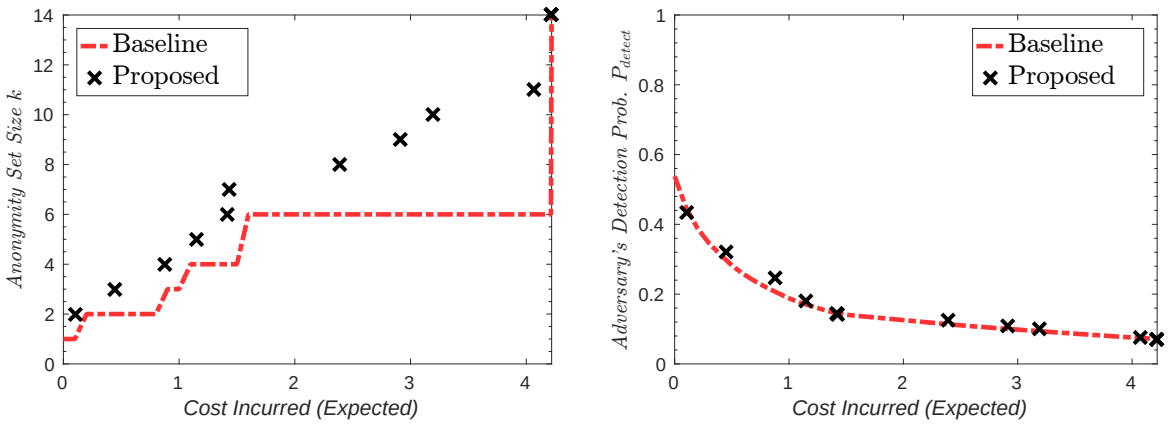


(a) 20-node line network.

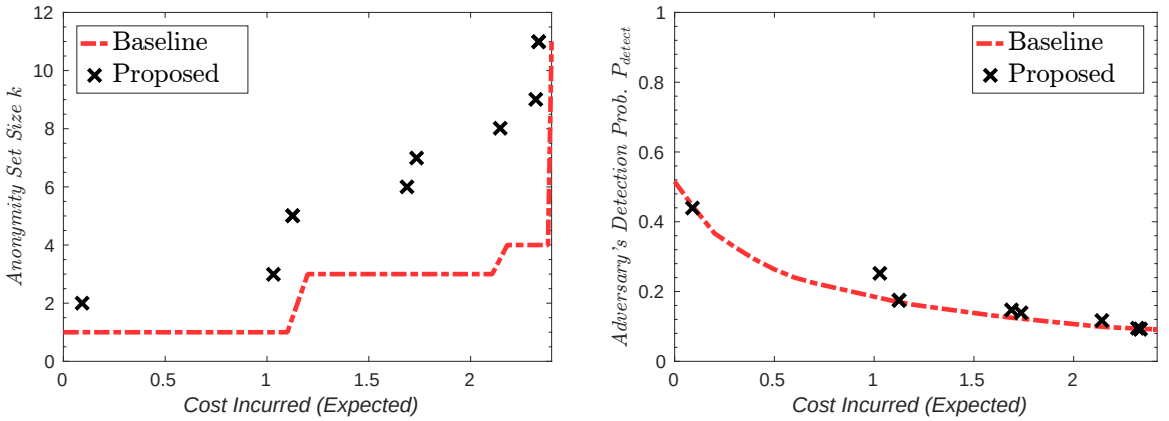


(b) 20-node k-ary tree network.

Figure 4.6: Anonymity set size k and the adversary's P_{detect} values in the proposed (k,ϵ)-anonymity and baseline (which minimizes P_{detect}) schemes under the line and k-ary tree networks.



(a) 15-node binary tree network.



(b) 3×4 grid network.

Figure 4.7: Anonymity set size k and the adversary's P_{detect} values in the proposed (k,ϵ)-anonymity and baseline (which minimizes P_{detect}) schemes under the binary tree and grid networks.

and minimizing P_{detect} as more dummy traffic is required in the former. Thus, we study this trade-off under four different network topologies and compared the k (first column) and P_{detect} values (second column) in Figs. 4.6 and 4.7. Our proposed scheme provides as much as 50% larger anonymity set size k values in the non-grid networks and up to 200% in the grid network for the same amount of cost incurred. This highlights the vulnerability of the baseline scheme in the context of (k,ϵ)-anonymity. Also, our proposed scheme uses lesser cost than the baseline scheme to achieve a specified k value. And interestingly, there are instances where the next larger k value can be obtained with only a small increment in the cost incurred. It is observed that the k values of the baseline scheme rapidly increase to the maximum achieved value at the rightmost corner of the x-axis as it represents the flooding scenario.

The P_{detect} values in the proposed and the baseline schemes are very close (within 3%) in the line, k-ary tree, and binary tree networks (see Figs. 4.6a, 4.6b, and 4.7a). However, the P_{detect} values provided by our scheme are slightly higher than the baseline scheme in the grid (Fig. 4.7b) network topology where the differences in P_{detect} values are up to 7%. However, the differences in the P_{detect} values decrease as the expected cost incurred increase. This is because the routes chosen by the two schemes become similar to flooding when the expected cost incurred approaches the rightmost corner of the x-axis in the figures.

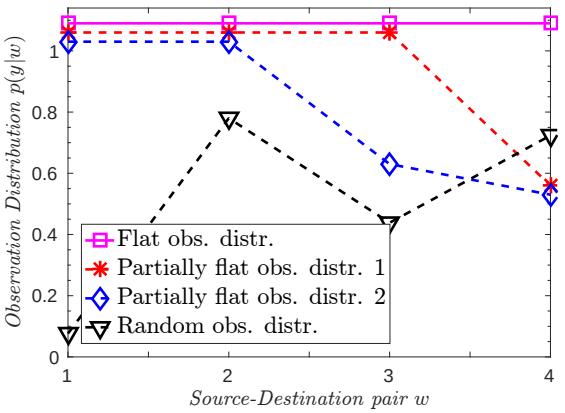
Overall, our approach is able to provide significantly better (k,ϵ)-anonymity privacy guarantees for a slight degradation in P_{detect} compared to the baseline scheme that only minimizes P_{detect}. One limitation of the proposed (k,ϵ)-anonymity scheme is that it takes a much longer time to compute the optimal (k,ϵ)-anonymous solution compared to the baseline scheme that solves a P_{detect} minimization problem. Unless a large ϵ or small k parameter is used (which speeds up the optimization time), it may not be practical to solved the proposed (k,ϵ)-anonymity scheme for large networks with thousands of nodes.

4.7.2 Prior Sensitivity Analysis

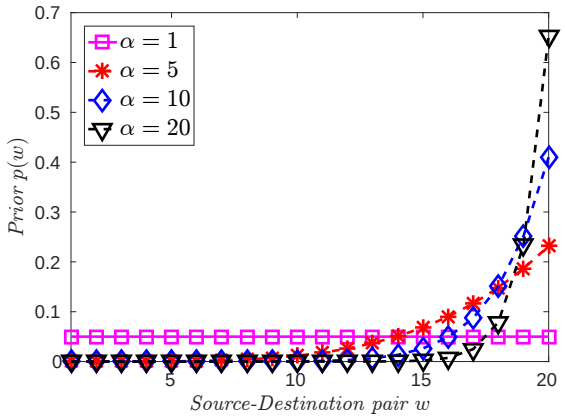
Next, we study how the prior $p(w)$ affects the adversary's P_{detect} for a given observation y. Consider a network with 20 possible source-destination pairs where $p(w)$ comes from a beta distribution parameterized by α and β as used in Section 4.6.2. To use the beta distribution in our discrete prior distribution, we quantized the support values over the number of source-destination pairs and normalized the probabilities to sum to one. We fixed $\beta = 1$ and varied the α parameter from 1 to 50 in the following figures as the beta distribution matches the uniform distribution when $\alpha = \beta = 1$ and becomes more concentrated around a small number of source-destination pairs as α increases while β remains constant. We chose to vary α as it causes a larger adversary Bayes risk as shown in Figs. 4.3 and 4.4, which allows us to study how the observation distribution affects P_{detect}. Fig. 4.8b shows an example of the used beta prior $p(w)$ distribution for different α values and Fig. 4.8a shows an instantiation of the four observation distributions $p(\boldsymbol{y}|w)$ used in our simulation;

We used four observation distributions $p(\boldsymbol{y}|w)$ in our simulation: the flat observation distribution has a probability of one for all the w pairs, and the partially flat observation distribution 1 has an almost flat distribution for the source-destination w pairs with one-quarter different probabilities (the other three-quarters are one), the partially flat observation distribution 2 has two-quarters different probabilities, while the probabilities of the random observation distribution are uniformly selected from 0 to 1. The following simulation results were obtained by taking the average of 1000 runs.

In Fig. 4.9a, we plot the P_{detect} values for a single observation y under four different observation distributions where we assume the adversary has complete information on $p(w)$. There exists little differences in P_{detect} (about 8% at most) for the different observation distributions when the adversary knows the true prior distribution and the difference is minimal when $\alpha = 22$. In Fig. 4.9b, we plot the P_{detect} values for a single observation y under various observation distributions where the adversary varies its chosen prior (according to the α parameter stated in the x-axis) given that the true prior is uniformly distributed over the source-destination

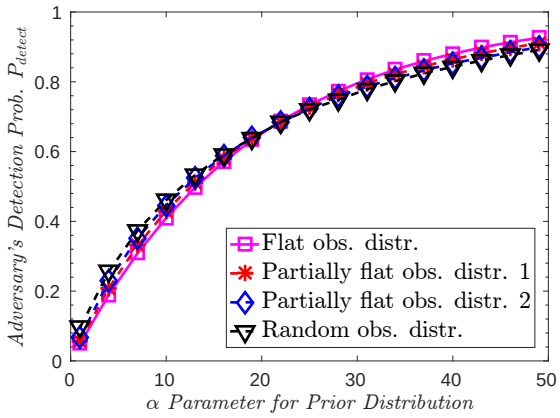


(a) Different observation distributions for a given observation y.

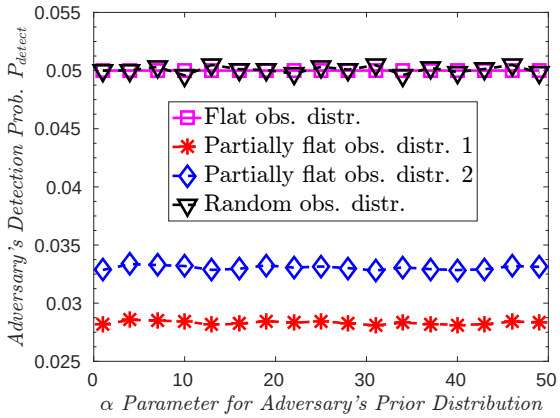


(b) Beta prior distribution $p(w)$ for various α values while β is fixed at one.

Figure 4.8: Observation and prior distributions used in our simulations.



(a) Complete information.



(b) Partial information - true prior is uniformly distributed in $\mathcal{V}^2$.

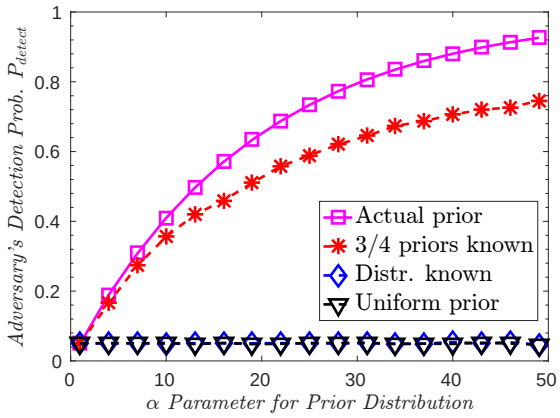
Figure 4.9: Adversary's detection probability P_{detect} under four different observation distributions (complete information).

pairs. The P_{detect} values are generally very low and largely unaffected by the adversary's prior beliefs.

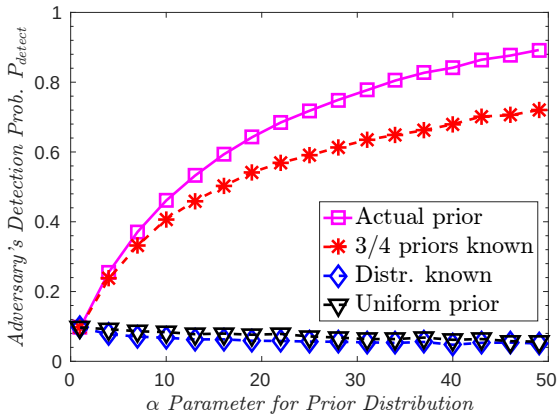
Next, we consider four scenarios where (i) the adversary has knowledge of the true prior, (ii) the adversary only knows three-quarter of the true prior and assigns a uniform prior for the other unknown values, (iii) the adversary knows the true prior distribution, but not its actual instantiation, and (iv) the adversary uses a uniform prior. We used a uniform prior for the adversary in scenario (ii) as we have shown in Lemma 4.2 that it always minimizes the maximum adversary's Bayes risk when the observation distribution is flat. In Fig. 4.10a, we plot the P_{detect} values for a single observation y with a flat observation distribution for different

adversarial prior distributions given that the true prior has the α parameter stated in the x-axis and set $\beta = 1$. The P_{detect} values are highest when the adversary knows the true prior and are very low when the adversary only knows the prior distribution, but not its actual instantiation or when the adversary uses a uniform prior that does not match the true prior. However, the P_{detect} values increase significantly when three-quarter of the true prior is known. In Fig. 4.10b, we repeat the same four scenarios but used an arbitrary observation distribution $p(\boldsymbol{y}|w)$ instead of the flat observation distribution used in Fig. 4.10b. Compared to the results in Fig. 4.10a, the P_{detect} values increased slightly under the scenarios where the prior distribution, but not its actual instantiation is known, and when the adversary uses a uniform prior for cases where $\alpha < 30$. Interestingly, the P_{detect} values also increased when $\alpha < 10$ but decreased as α increases. Therefore, the adversary's detection probability P_{detect} values depend heavily on both the fraction of true prior known to him and the prior distribution.

Finally, we analyze the impact of knowing varying portions of the true prior and plot the corresponding P_{detect} values in Fig. 4.11. The results show that the P_{detect} values decrease proportionally as less information on the prior is known to the adversary. It is observed that the adversary gains the most improvement in P_{detect} when it has knowledge of the first quarter of the prior and knowing additional quarters of the prior evenly increases its P_{detect}.



(a) Flat observation distribution.



(b) Arbitrary observation distribution.

Figure 4.10: Adversary's detection probability P_{detect} under four different prior beliefs (partial information).

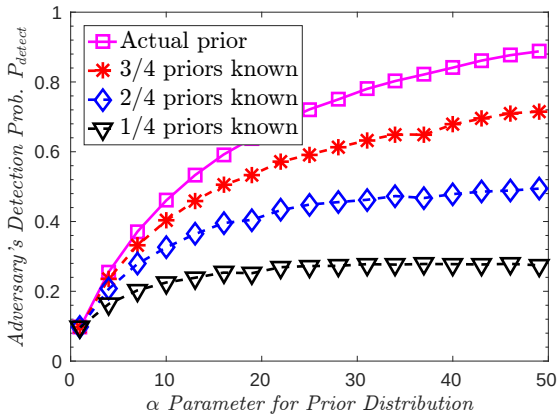


Figure 4.11: Adversary's detection probability P_{detect} under four different prior beliefs and an arbitrary observation distribution (partial information).

4.8 Conclusion and Future Work

In this chapter, we introduced the (k,ϵ)-anonymity property for privacy guarantees in wireless networks and designed a statistical decision-making framework that considers a maximum-a-posteriori (MAP) inference-based adversary with both full and partial information. We also highlighted via an example the subtle difference between maximizing the expected privacy level and providing privacy guarantees. We then formulated a mixed-integer linear programming (MILP) problem to select the minimum-cost (k,ϵ)-anonymous paths and compared our solution against a baseline scheme that minimizes the average detection probability of the adversary. Our simulation results show that the proposed scheme provides significantly larger anonymity set sizes while achieving comparable average detection probability for a fixed transmission cost incurred. We also studied how the adversary's prior beliefs affect its detection probability and Bayes risk. Under the partial information adversarial model, we proved that it is reasonable to assume that the adversary uses a uniform prior as it minimizes the adversary's Bayes risk.

The future work would be to study distributed solutions for our privacy-preserving routing problem or heuristic pruning methods to lower the time needed to search for the optimal solution. This is because it may not be practical to solve the formulated MILP problem for large scale network consisting of thousand of nodes unless ϵ is large or k is small, which is relatively easier to solve. But a large ϵ or small k value limits the effectiveness of the provided privacy guarantees.

Chapter 5

Incentive Mechanisms for Privacy-aware Mobile Crowd Sensing Applications

We consider the *privacy-aware incentive* problem for mobile crowd sensing (MCS) applications used in spatial monitoring. Existing privacy-aware incentive works do not seek to improve the spatial coverage of the collected dataset, which is particularly useful for spatial monitoring applications that require data for tasks such as spatial field reconstruction or estimation of some spatial characteristics for the process being sensed. Hence, we propose a privacy-aware Stackelberg incentive model that improves the spatial coverage of the collected dataset. Our proposed model is privacy-aware, in that it allows privacy-sensitive smartphone users to submit *coarse-grained (or quantized) location* information that could still be useful for regression purposes. We then study the properties of the proposed Stackelberg model analytically and present efficient algorithmic solutions.

5.1 Introduction to Privacy-aware Incentive Mechanisms

Many important mobile crowd sensing applications for spatial monitoring such as those used for traffic monitoring [56], earthquake detection [57] or noise monitoring [58] will benefit greatly if the coverage area of its dataset is maximized. Hence, improving the *spatial coverage*

The material in this chapter was presented in part in [126, 127].

of the collected dataset should be one of the main objectives of an incentive mechanism used by spatial monitoring applications. Additionally, current privacy-preserving works such as [22,59,60] have attempted to address the user *location privacy* problem in the crowd sensing domain. This is because the privacy issues can easily deter potential users from participating, which in turn reduces the amount of potential data available to the crowdsourcer.

However, the location privacy problem has not been fully addressed as existing incentive models [22, 59, 60] that offer location privacy via location or data perturbation are not directly applicable to crowd sensing applications that require specific and true locations. For example, it would be unacceptable for a traffic monitoring application if there was a traffic congestion in road X, but due to location or data perturbation, another road Y or a non-congested status was reported respectively. Thus, it is vital for incentive models to address the spatial coverage and location privacy issues concurrently.

An appropriate incentive mechanism to model the hierarchical relationship between the crowdsourcer and the mobile smartphone users is the *Stackelberg (leader-follower) game* incentive model used in [61–63]. In the Stackelberg model, the crowdsourcer (leader) commits a reward strategy that is observed by the smartphone users (followers) who then strategize the amount of data to sell. However, existing Stackelberg incentive models simply select user data independently of their physical location [64] and do not attempt to improve the spatial coverage of the dataset.

Therefore, we propose extending the existing Stackelberg incentive models to include the *privacy-awareness* property as well as to improve the *spatial coverage* of the collected dataset. Our model allows privacy-sensitive mobile smartphone users to submit *coarse-grained (or quantized) location* information which could still be useful to the crowdsourcer. We then study the properties of the proposed Stackelberg game analytically and present efficient algorithmic solutions. Our proposed model does not require a trusted third party for privacy and can protect users against a crowdsourcer who cannot be trusted to anonymize the mobile smartphone users' location information.

5.1.1 Contributions

To the best of our knowledge, this is the first work that proposes a privacy-aware Stackelberg incentive model that improves the spatial coverage of the collected dataset.

The key contributions of this work can be summarized as follows:

- We propose a novel privacy-aware Stackelberg incentive scheme that allows privacy-sensitive smartphone users to quantize their location information using *cloaking regions*. Our proposed model also improves the spatial coverage of the collected dataset.
- We prove the stability of the proposed model (i.e., there exists a unique Stackelberg equilibrium) and its dominant strategy incentive-compatibility property. We also prove the existence of a Stackelberg equilibrium when the leader imposes constraints on the minimum and maximum amount of data contribution from each user and studied the sufficient conditions for achieving Pareto-efficiency.
- We demonstrate via simulations using a real-world sensing dataset that the proposed Stackelberg game has better predictive performance compared to two other coverage-maximizing schemes that maximize a different coverage metric.

5.1.2 Notation

The table of notation used in this chapter can be found in Table 5.1.

To improve the presentation of the chapter, we present all the lengthy proofs (that occupy more than a page) in Section 5.8.

5.2 Related Work

Most of the existing incentive schemes designed for mobile crowd sensing applications [61–63] do not consider the privacy preferences of the participating workers. Thus, the schemes may not be able to incentivize privacy-concerned users. To effectively incentivize user participation,

Table 5.1: Notation.

c_i	Sensing cost incurred per unit of data by worker i where $c_i \in (0, \bar{c}]$.
$\boldsymbol{c_{-i}}$	Sensing costs incurred per unit of data by all workers other than worker i.
ρ_i	Location granularity of worker i where $\rho_i \in [\underline{\rho}, \bar{\rho}]$.
$\boldsymbol{\rho_{-i}}$	Location granularities of all workers other than worker i.
l_i, l_i'	Partitioned region and cloaking region of worker i respectively where $l_i' \in l_i$.
t_i	Amount of data contributed by worker i.
$\bar{t}, \underline{t}$	Maximum and minimum amount of data contribution permitted by the crowdsourcer.
$\boldsymbol{t_{-i}}$	Amount of data contributed by all workers other than worker i.
R_l	Sum of rewards allocated to workers in region l (similarly, R_{l_i} refers to the sum of rewards allocated to worker i's region).
λ_i	System parameter for crowdsourcer.
U_{CS}, u_i	Utility function of crowdsourcer and worker i respectively.
$\mathcal{I}$	Set of all workers.
N_l	Number of workers in region l.
$\mathcal{Q}_l$	Set of participating workers in region l (similarly, $\mathcal{Q}_{l_i}$ refers to the set of participating workers in the region l_i where worker i is located).
$\mathcal{J}_l$	Set of participating workers i in region l with $t_i = \bar{t}$.
$\mathcal{K}_l$	Set of participating workers i in region l with $t_i < \bar{t}$.

Nissim *et al.* [59] proposed a generic construction for a privacy-aware incentive mechanism design that requires only an upper bound on the workers' loss due to privacy leakage. Yang *et al.* [22] applied the k-anonymity framework to provide privacy for the set of participating workers and designed an auction-based incentive mechanism to incentivize workers to participate in the anonymity set.

Singla *et al.* [60] proposed an incentive-compatible incentive mechanism that allows workers to randomly perturb their location information. However, privacy-aware incentive mechanisms that use data perturbation or dummy locations [128] to protect location privacy for the participating workers may not be applicable to many spatial monitoring applications. This is because in traffic monitoring [56], earthquake detection [57] or even noise monitoring [58] applications, a dataset with perturbed data or dummy location may trigger a false alarm and make the application unreliable. In contrast, we allow privacy-concerned workers to obfuscate their precise location information by declaring a coarse-grained cloaking region (see Fig. 5.2) that encompasses their true location (similar to the location cloaking principle in [129, 130]) instead of providing fine-grained location information to the crowdsourcer. This

step is important as privacy concerns can deter potential workers from participating in the crowd sensing activity.

Interestingly, the work in [131] found that smartphone users were more willing to provide coarse-grained location information than fine-grained information. This supports the practicality of our proposed incentive model, which may still buy data (albeit with lower quality location information) from privacy-sensitive workers to improve the spatial coverage of the collected dataset. Furthermore, we argue that the cloaking region technique is more practical for real-world applications that require reliable information. Although the location information of the workers may be *imprecise* due to the location cloaking, but it is still *accurate* as there is no data perturbation or dummy locations involved.

Yang *et al.* [61] proposed a platform-centric Stackelberg (leader-follower) game incentive model for the crowd sensing platform (or the crowdsourcer) where the crowd sensing platform is the leader while the workers are the followers. The proposed model is platform-centric as the platform directly controls the amount of reward for each participating worker. Duan *et al.* [62] proposed a similar Stackelberg game incentive model and studied how the workers' sensing cost information affects the crowdsourcer's optimal reward allocation. In constrast to the previous two works that considered a single sensing task, Luo *et al.* [63] proposed a Stackelberg game incentive model that considers scenarios where the crowdsourcer has multiple collaborative tasks for the workers. However, the existing Stackelberg models do not consider the quality (e.g., spatial coverage area) of each worker's data.

The work in [64] proved that adding location information into the workers' assignment problem increases the computational complexity of the solution. The authors then proposed an auction-based approximation algorithm to assign the workers' sensing tasks. However, it was assumed that the crowd sensing platform periodically publishes sensing tasks for specific locations of interest and did not explicitly address the issue of improving the spatial coverage of the collected dataset in general. To improve the spatial coverage of the collected dataset, the work in [132] proposed an auction-based incentive mechanism to selects a representative

subset of workers while considering their location information. To quantify the sensing coverage of a worker's data, the authors considered a disk coverage model in their work. In contrast, the works in [133–135] designed a incentive scheme that considers a k-depth coverage model in the event that multiple worker data is needed in each region.

In this work, we consider both the worker's privacy preferences and its spatial location to improve the spatial coverage of our collected dataset.

5.3 System Model

The crowd sensing system consists of a set of $\mathcal{I} = \{1, \ldots, N\}$ workers and a single crowdsourcer who partitions the entire spatial area of interest into a set of L regions denoted by $\mathcal{L}$. We assume that the workers are rational and non-cooperative, i.e., each worker maximizes its own utility. Each worker $i \in \mathcal{I}$ has its own sensing cost per unit time $c_i \in (0, \bar{c}]$, location granularity $\rho_i \in [\underline{\rho}, \bar{\rho}]$, location l_i' (which may be of different granularity for each worker) and its corresponding cloaking region l_i defined by the system where $l_i' \in l_i$ and $l_i \in \mathcal{L}$.

The interaction model between the crowdsourcer and smartphone users is illustrated in Fig. 5.1. The crowdsourcer first collects the worker profiles, which consist of the each worker's sensing cost incurred per bit of data c_i, location granularity ρ_i, and region l_i. The crowdsourcer then selects the optimal set of workers that maximizes his utility and offers the selected workers a reward in exchange for some amount of sensing data. Next, the selected workers will proceed to collect their data and transmit them along with their location information to the crowdsourcer and receive their rewards. Note that there are two types of regions l_i and l_i' in our model, l_i is the initial coarse-grained region defined by the system and l_i' is the worker's cloaking region, which is submitted only when the worker is selected.

We model the incentive mechanism as a *Stackelberg game* consisting of the crowdsourcer (data buyer) as the *leader* and the N smartphone users (workers) as the *followers*. The crowdsourcer acts first and commits a reward strategy while the workers subsequently choose their best responses after observing the crowdsourcer's strategy. The strategy of the crowdsourcer is the

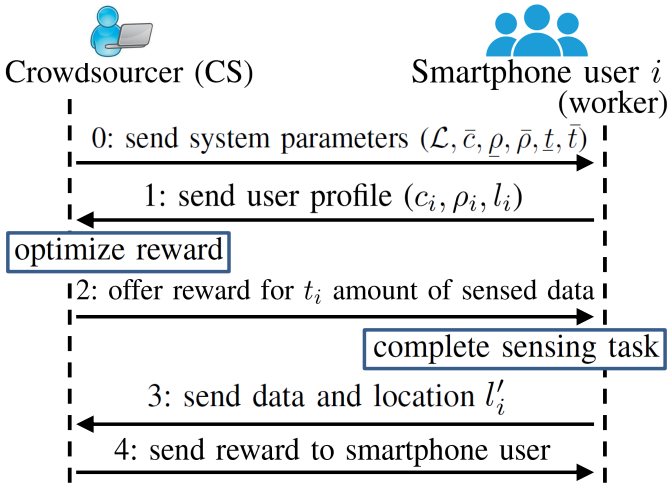


Figure 5.1: Interaction model between the crowdsourcer and smartphone users (workers).

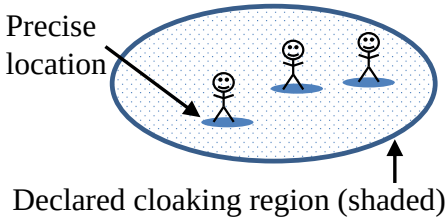


Figure 5.2: Privacy model of smartphone users (workers).

reward for each partitioned region $\boldsymbol{R} = (R_1, \ldots, R_L)$ and the strategy of worker i is the amount of data (in terms of sensing time) $t_i \geq 0$.

5.3.1 Privacy Model of Workers

We assume that the granularity of the worker i's submitted location l_i' is proportional to its location granularity ρ_i. The intuition behind this is that a privacy-sensitive worker (with low ρ_i) is more likely to provide only coarse-grained location information. Likewise, a privacy-insensitive worker (with high ρ_i) is more likely to provide finer-grained location information. Hence, the parameter ρ_i allows the crowdsourcer to differentiate between workers and preserve the privacy of unselected workers since they only reveal their true locations when they are selected. Note that the workers can anonymize their precise location information via cloaking regions (see Fig. 5.2) with regions inversely proportional to ρ_i and do not rely on the crowdsourcer for anoymization. In practice, this can be implemented in the crowdsourcing

software on the workers' smartphone devices to allow each worker to select various cloaking regions with (possibly discrete) location granularities.

5.3.2 Reward Function of Workers

The crowdsourcer only optimizes the reward R_l allocated to each partitioned region $l \in \mathcal{L}$ and subsequently offers each participating worker i a fraction of R_l depending on the proportion of their data contribution, location granularity, and location:

$$\text{Worker } i\text{'s offered reward} = \frac{t_i \rho_i}{\sum\limits_{j \in \mathcal{Q}_{l_i}} t_j \rho_j} R_{l_i}, \tag{5.1}$$

where $\mathcal{Q}_{l_i}$ is the set of participating workers i in location l_i with $t_i > 0$ and we assume $|\mathcal{Q}_{l_i}| > 1$. A similar reward function has also been used in [61].

5.3.3 Utility Function of Crowdsourcer

We define the utility function of the crowdsourcer to be $U_{CS}(\boldsymbol{R}; \boldsymbol{t}) = \sum\limits_{i \in \mathcal{I}} f_d(t_i, l_i, \rho_i)$, where $f_d(t_i, l_i, \rho_i)$ is a function of the quantity and quality (e.g., spatial coverage) of the data from each worker i and its location granularity ρ_i. For simplicity, we let $f_d(t_i, l_i, \rho_i) = \lambda_i \log(1 + t_i)$, where $\lambda_i \propto l_i, \rho_i$ is a system parameter and the log function models the diminishing returns on each worker's data. Thus, the crowdsourcer's utility function is given by:

$$U_{CS}(\boldsymbol{R}; \boldsymbol{t}) = \sum_{i \in \mathcal{I}} \lambda_i \log(1 + t_i). \tag{5.2}$$

To increase the coverage area of the collected dataset, the crowdsourcer can assign a higher λ_i value to workers located at less populated regions. In addition, a higher λ_i value can be assigned to workers who provide finer location information. By introducing the λ_i parameter, the crowdsourcer is able to differentiate between the quality (e.g., spatial coverage area and the granularity of the location information) of each worker's data.

5.3.4 Utility Function of Workers

The utility function of worker i is defined to be the amount of reward it receives from the crowdsourcer as defined in (5.1) minus the cost incurred for obtaining the data:

$$u_i(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, R_{l_i}) = \frac{t_i \rho_i}{\sum\limits_{j \in \mathcal{Q}_{l_i}} t_j \rho_j} R_{l_i} - c_i t_i, \tag{5.3}$$

where $t_i \geq 0$ is the amount of data (in terms of sensing time) sold to the crowdsourcer and $\boldsymbol{t}_{-\boldsymbol{i}}$ is a vector of the amount of data sold by all workers except worker i.

5.4 Problem Formulation and Analysis

We address the following problem statement: suppose there is a crowdsourcer (buyer) who aims to buy sensing data from smartphone users (workers), design an incentive mechanism such that the collected dataset (i) is privacy-preserving for the workers, and (ii) has good spatial coverage.

5.4.1 Stackelberg Game Formulation

Given that the crowdsourcer wants to increase the coverage area of his dataset while satisfying a budget constraint R^{budget} and a minimal amount of reward allocation $R_l^{\min} > 0$ for each region l (this allows the crowdsourcer to specify more important regions), it solves the following optimization problem:

Problem 1 ($\boldsymbol{\lambda}, \boldsymbol{R^{\min}}, \boldsymbol{R^{\max}}, R^{\text{budget}}$)

$$\begin{aligned} \underset{\boldsymbol{R}}{\text{maximize}} \quad & \sum_{i \in \mathcal{I}} \lambda_i \log(1 + t_i) \\ \text{subject to} \quad & R_l^{\min} \leq R_l \leq R_l^{\max} \quad , \forall\, l \in \mathcal{L}, \\ & \sum_{l \in \mathcal{L}} R_l \leq R^{\text{budget}}, \end{aligned} \tag{5.4}$$

where t_i is the optimal solution to Problem 2.

Each worker i solves the following optimization problem:

Problem 2 $(i, \boldsymbol{t}_{-\boldsymbol{i}}, \rho_i, \boldsymbol{\rho}_{-\boldsymbol{i}}, R_{l_i}, c_i)$

$$\begin{aligned} \underset{t_i}{\text{maximize}} \quad & \frac{t_i \rho_i}{\sum\limits_{j \in \mathcal{Q}_{l_i}} t_j \rho_j} R_{l_i} - c_i t_i, \\ \text{subject to} \quad & t_i \geq 0. \end{aligned} \tag{5.5}$$

Problems 1 and 2 form a Stackelberg game and our goal is to find the Stackelberg equilibrium point(s) where neither the crowdsourcer nor the workers have incentive to deviate. A Stackelberg equilibrium (see Definition 5.1) is a subgame-perfect Nash equilibrium such that no player can improve its utility by unilaterally deviating its strategy.

Definition 5.1 (Stackelberg Equilibrium)**.** *Let $\boldsymbol{R}^*$ be the optimal solution for the crowdsourcer, obtained by solving Problem 1, and $\boldsymbol{t}^*$ be the optimal solution for the workers, obtained by solving Problem 2. The strategy profile $(\boldsymbol{R}^*, \boldsymbol{t}^*)$ is a Stackelberg equilibrium for the proposed Stackelberg game if the following conditions are satisfied for any $(\boldsymbol{R}, \boldsymbol{t})$ where $\boldsymbol{R} \geq 0, \boldsymbol{t} \geq 0$:*

$$\begin{aligned} U_{CS}(\boldsymbol{R}^*; \boldsymbol{t}^*) &\geq U_{CS}(\boldsymbol{R}; \boldsymbol{t}^*), \\ u_i(t_i^*; \boldsymbol{t}_{-\boldsymbol{i}}^*, \boldsymbol{R}^*) &\geq u_i(t_i; \boldsymbol{t}_{-\boldsymbol{i}}^*, \boldsymbol{R}^*) \quad , \forall i \in \mathcal{I}. \end{aligned}$$

We apply the backward induction method to analyze the proposed Stackelberg game. First, we study with the Followers game (a non-cooperative game played by all the workers) and compute the predicted best response t_i^* (solution of Problem 2) for each worker i as a function of the reward R_{l_i} offered by the crowdsourcer and the strategies of the other workers $\boldsymbol{t}_{-\boldsymbol{i}}$. Subsequently, we analyze the best response of the crowdsourcer in Problem 1.

5.4.2 Nash Equilibrium Of Followers Game

We consider the Followers game given by the triplet $(\mathcal{I}, \{t_i\}_{i \in \mathcal{I}}, \{u_i\}_{i \in \mathcal{I}})$ where $\mathcal{I}$ is the player set of N workers and u_i is the utility function of worker i. We then derive the unique (pure-

strategy) Nash equilibrium of the Followers game in Theorem 5.1. At the Nash equilibrium point, no single worker can improve its utility by deviating unilaterally from the point. By studying the Nash equilibrium point, the crowdsourcer is able to predict the best responses of the workers in given region l for a fixed reward R_l.

Lemma 5.1. *A unique Nash equilibrium exists in the Followers game* $(\mathcal{I}, \{t_i\}_{i\in\mathcal{I}}, \{u_i\}_{i\in\mathcal{I}})$. *See Section 5.8.1 for proof.*

To study the best response strategy for worker i given the strategies of the other players, we set $\frac{\partial u_i}{\partial t_i} = 0$ to obtain:

$$R_{l_i} \sum_{j\in\mathcal{Q}_{l_i}: j\neq i} t_j^* \rho_j = c_i \left(\sum_{j\in\mathcal{Q}_{l_i}} t_j^* \rho_j \right)^2. \tag{5.6}$$

We now seek an expression for the optimal t_i^* value that is independent of the other t_j^* values. We say that worker i is a participating worker if $t_i^* > 0$.

Theorem 5.1. *The Followers game* $(\mathcal{I}, \{t_i\}_{i\in\mathcal{I}}, \{u_i\}_{i\in\mathcal{I}})$ *has a unique Nash equilibrium given by the following closed-form expression:*

$$t_i^* = \begin{cases} \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j\in\mathcal{Q}_{l_i}} c_j} \left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum_{j\in\mathcal{Q}_{l_i}} c_j} \right) \frac{R_{l_i}}{\rho_i}, & \text{if } i \in \mathcal{Q}_{l_i}, \\ 0, & \text{otherwise,} \end{cases} \tag{5.7}$$

where $\mathcal{Q}_{l_i}$ *is the set of participating workers in region* l_i. *See Section 5.8.2 for proof.*

Note that $t_i^* > 0$ for all participating workers i. Hence, from (5.7), all participating workers $i \in \mathcal{Q}_{l_i}$ should satisfy:

$$\begin{aligned} &\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j\in\mathcal{Q}_{l_i}} c_j} \left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum_{j\in\mathcal{Q}_{l_i}} c_j} \right) \frac{R_{l_i}}{\rho_i} > 0, \\ \Rightarrow \quad & c_i < \frac{\sum_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)}. \end{aligned} \tag{5.8}$$

Subsequently, we will make use of this constraint in Algorithm 5.1.

The optimal t_i^* for the workers is given by the Nash equilibrium solution (5.7) of the Followers

game. However, (5.7) requires knowledge of the set of participating workers' $\mathcal{Q}_l$, c_i, and ρ_i. Hence, we propose Algorithm 5.1 which makes use of (5.8) to greedily compute $\mathcal{Q}_l$ and solve for t_i^*. The values of t_i^* can then be input into Problem 1 which solves for $\boldsymbol{R}^*$.

By Theorem 5.2, the unique Nash equilibrium of the Followers game can be obtained using Algorithm 5.1. Note that it is assumed that there are at least two workers in the Followers game.

Lemma 5.2. *Assume that there are at least two workers in each region l, Algorithm 5.1 selects the optimal set of participating workers $\mathcal{Q}_l$ that achieves the unique Nash equilibrium of the Followers game. See Section 5.8.3 for proof.*

Theorem 5.2. *Assuming that there are at least two workers in each region l, and the set of $\mathcal{Q}_l$ from Lemma 5.2, Algorithm 5.1 outputs the unique Nash equilibrium solution of the Followers game. See Section 5.8.4 for proof.*

Algorithm 5.1: Compute the Nash equilibrium solution of the Followers game.

function SolveFollowerGame($\boldsymbol{c}, \boldsymbol{\rho}, \boldsymbol{l}, \boldsymbol{R}$)
Input : sensing costs $\boldsymbol{c}_{1,\dots,N}$, location granularities $\boldsymbol{\rho}_{1,\dots,N}$, workers' regions $\boldsymbol{l}_{1,\dots,N}$, rewards $\boldsymbol{R}_{1,\dots,L}$.
Output : data sold to crowdsourcer $\boldsymbol{t}^*_{1,\dots,N}$.
foreach *region* $l \in \mathcal{L}$ **do**
    Sort workers in l according to their privacy-weighted cost $\frac{c_i}{\rho_i}$ in ascending order where $\frac{c_i}{\rho_i} \leq \frac{c_{i+1}}{\rho_{i+1}}$.
    Let $\mathcal{Q}_l = \{1, 2\}$ be the set of participating workers with $t_i^* > 0$.
    Set $\mathcal{Q}_l \leftarrow \mathcal{Q}_l \cup \{i\}$ for each worker i in region l if the condition in (5.8) is met. (note: the looping can stop at the ith step when the condition is not met.)
    Set t_i^* according to (5.7) for all workers in l.
end

After computing the predicted best response t_i^* for each worker i as a function of the reward R_{l_i} offered by the crowdsourcer and the strategies of the other workers $\boldsymbol{t}_{-\boldsymbol{i}}$, we analyze the best response of the crowdsourcer in the Stackelberg equilibrium.

5.4.3 Stackelberg Equilibrium

Using the analytical result (5.7) for the Followers game, the crowdsourcer can optimize his reward strategy $\boldsymbol{R}$ efficiently by substituting the analytical result into his utility function in (5.2) to obtain:

$$U_{CS}(\boldsymbol{R};\boldsymbol{t}) = \sum_{i\in\mathcal{I}} \lambda_i \log(1+\tau_i R_{l_i}), \tag{5.9}$$

where $\tau_i = \frac{(|\mathcal{Q}_{l_i}|-1)}{\rho_i \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\right)$.

Although it is not trivial to obtain the closed-form expression that maximizes (5.9) while satisfying the constraints in (5.4), we show in Theorem 5.3 that there exists a unique Stackelberg equilibrium which results in a stable equilibrium strategy profile. This allows the crowdsourcer to predict the behaviors of the workers and efficiently compute the optimal $\boldsymbol{R}^*$. By Theorem 5.3, the optimal reward $\boldsymbol{R}^*$ has a unique maximizer and hence, can be efficiently computed using the well-known interior point methods. Both Theorems 5.1 and 5.3 extend [61, Theorem 2] to the case where the workers' location granularities ρ and locations l are also considered.

Theorem 5.3. *The proposed Stackelberg game has a unique Stackelberg equilibrium.*

Proof. Recall from Theorem 5.1 that the Followers game has a unique Nash equilibrium. It can be easily shown that the best response strategy set of the crowdsourcer is convex and compact since R_l is assumed to be bounded, and U_{CS} is continuous in $\boldsymbol{R}$. Hence, we need to show the strict concavity of U_{CS} to conclude that there exists a unique Stackelberg equilibrium. The second-order derivatives of U_{CS} with respect to R_l are as follows:

$$\begin{aligned}
&\frac{\partial U_{CS}}{\partial R_l} = \sum_{i:l_i=l} \lambda_i \left(\frac{\tau_i}{\tau_i R_l + 1}\right), \\
&\frac{\partial^2 U_{CS}}{\partial R_l^2} = -\sum_{i:l_i=l} \lambda_i \left(\frac{\tau_i^2}{(\tau_i R_l+1)^2}\right) < 0, \ \frac{\partial^2 U_{CS}}{\partial R_l \partial R_k} = 0,
\end{aligned} \tag{5.10}$$

where τ_i is given in (5.9). Since the Hessian matrix of U_{CS} is a diagonal matrix, its eigenvalues, i.e., $\frac{\partial^2 U_{CS}}{\partial R_l^2}$ are easily shown to be strictly negative. This implies that the Hessian matrix is

negative definite for all $R_l \in \boldsymbol{R}$ and thus, U_{CS} is strictly concave in $\boldsymbol{R}$. □

Next, we prove that our proposed Stackelberg game has the dominant strategy incentive-compatibility property.

5.4.4 Dominant Strategy Incentive-Compatibility Property

We first define the dominant strategy incentive-compatible property in Definition 5.2 and show that our proposed Stackelberg game has the dominant strategy incentive-compatible property. This property is useful because it ensures that every participating worker can achieve the best outcome itself when it acts according to its true preferences.

Definition 5.2 (Dominant Strategy Incentive Compatibility)**.** *We say that a strategy profile* $(\boldsymbol{R}, \boldsymbol{t})$ *is dominant strategy incentive-compatible (or strategyproof) if the following statement is true for all possible vectors* $\boldsymbol{c_{-i}}$ *consisting of the workers' true sensing costs (excluding worker i's).*

$$u_i(t_i; \boldsymbol{t_{-i}}, R_{l_i}, c_i, \boldsymbol{c_{-i}}) \geq u_i(t_i; \boldsymbol{t_{-i}}, R_{l_i}, c_i', \boldsymbol{c_{-i}}),$$

$$\forall i \in \mathcal{I}, c_i \in (0, \bar{c}_i], c_i' \in (0, \bar{c}_i].$$

where c_i *is worker i's true sensing cost and* c_i' *is worker i's reported sensing cost.*

Theorem 5.4. *Assume the Followers game given by the triplet* $(\mathcal{I}, \{t_i\}_{i\in\mathcal{I}}, \{u_i\}_{i\in\mathcal{I}})$*. The payment mechanism of the Followers game, i.e., worker i's reward* $= \frac{t_i\rho_i}{\sum_{j\in\mathcal{Q}_{l_i}} t_j\rho_j} R_{l_i}$ *is dominant strategy incentive-compatible. See Section 5.8.5 for proof.*

Corollary 5.1. *The dominant strategy incentive-compatible property of the Followers game applies to all regions with at least two workers.*

In the next section, we extending the basic Stackelberg model to allow minimum and maximum constraints on the data contribution from each worker and study the sufficient conditions for achieving Pareto-efficiency.

5.5 Extending the Basic Stackelberg Model

In this section, we study how the crowdsourcer is able to achieve bounds on the workers' data and how it can achieve Pareto efficiency.

5.5.1 Bounds On The Amount Of Contributed Data t_i

In a practical real-world crowdsourcing application, the crowdsourcer may impose (lower and upper) bounds on the amount of contributed data t_i from each worker i due to various reasons. For example, it may not be useful to the crowdsourcer if each worker sells only a small amount of data or if there are workers who are monopolies. Likewise, it may not be practical to expect each worker to have an unbounded amount of data to sell or the crowdsourcer may not need too much data from each individual worker. For simplicity, we assume that the same bounds $\underline{t}$ and $\bar{t}$ apply to all participating workers. Next, we have the following lemmas to introduce the lower and upper bounds on t_i.

Lemma 5.3. *The crowdsourcer is able to achieve a lower bound $\underline{t}$ for all workers in location l that satisfies the equivalent Stackelberg equilibrium arising from the unconstrained setting as detailed in Theorem 5.3 as long as the following constraint on the set of participating workers is satisfied:*

$$c_i \leq \frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1-\frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right], \quad \forall i \in \mathcal{Q}_l. \tag{5.11}$$

Proof. To achieve a lower bound $\underline{t}$ for all workers in location l, we require $t_i^* \geq \underline{t}, \forall i \in \mathcal{Q}_l$. From (5.7), we have:

$$R_l \geq \frac{\underline{t}\rho_i\Big(\sum\limits_{j\in\mathcal{Q}_l} c_j\Big)}{(|\mathcal{Q}_l|-1)\Big(1-\frac{(|\mathcal{Q}_l|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\Big)}, \quad \forall i \in \mathcal{Q}_l,$$

$$\overset{\text{(i)}}{\Rightarrow} \quad \sum_{j\in\mathcal{Q}_l} c_j - (|\mathcal{Q}_l|-1)c_i \geq \frac{\underline{t}\rho_i\Big(\sum\limits_{j\in\mathcal{Q}_l} c_j\Big)^2}{(|\mathcal{Q}_l|-1)R_l}, \quad \forall i \in \mathcal{Q}_l, \tag{5.12}$$

where (i) we move c_i from the denominator.

We can obtain (5.11) from (5.12) by moving c_i to the left hand side of the inequality. To verify that Lemma 5.3 is valid, we substitute the value of c_i that satisfies the strict equality in (5.11) to (5.7):

$$t_i^* = \frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(1 - \frac{(|\mathcal{Q}_l|-1)\frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right]}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\frac{R_l}{\rho_i},$$
$$= \frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1 - 1 + \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right)\frac{R_{l_i}}{\rho_i} = \underline{t}.$$

If the strictly equality is not satisfied, then $t_i^* > \underline{t}$ according to (5.7). □

To introduce the lower bound $\underline{t}$, constraint (5.11) should be used instead of constraint (5.8) in line 6 of Algorithm 5.1. To verify that the introduction of the lower bound preserves the convexity of the crowdsourcer's Problem 1, we analyze the Hessian matrix of U_{CS}. We first apply the chain rule: $\frac{\partial^2 U_{CS}}{\partial R_l^2} = \frac{\partial^2 U_{CS}}{\partial t_i^2} \times \frac{\partial^2 t_i}{\partial R_l^2}$. From (5.2), we obtain $\frac{\partial^2 U_{CS}}{\partial t_i^2} = -\sum\limits_{i\in\mathcal{I}} \frac{\lambda_i}{(1+t_i)^2}$. From (5.11), we let $c_i = \frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right] - \delta_i$. From (5.7),

$$t_i = \frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(1 - \frac{(|\mathcal{Q}_l|-1)\left(\frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right] - \delta_i\right)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\frac{R_l}{\rho_i},$$
$$= \frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1 - 1 + \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l} + \frac{(|\mathcal{Q}_l|-1)\delta_i}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\frac{R_{l_i}}{\rho_i},$$
$$= \underline{t} + \left(\frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)^2 \frac{R_{l_i}\delta_i}{\rho_i}. \tag{5.13}$$

If $c_i \in (0,1]$, then from (5.13), it is obvious that t_i is a monotonically non-decreasing function of R_{l_i}. Since t_i is continuous, this implies convexity, i.e., $\frac{\partial^2 t_i}{\partial R_l^2} \geq 0$. As $\frac{\partial^2 U_{CS}}{\partial t_i^2} \leq 0$ and $\frac{\partial^2 t_i}{\partial R_l^2} \geq 0$, we have $\frac{\partial^2 U_{CS}}{\partial R_l^2} \leq 0$.

In (5.10), it was shown that $\frac{\partial^2 U_{CS}}{\partial R_l \partial R_k} = 0$. Since $\frac{\partial^2 U_{CS}}{\partial R_l^2} \leq 0$, the Hessian matrix of U_{CS} is negative semidefinite for all $R_l \in \boldsymbol{R}$. Thus, we conclude that U_{CS} is concave in $\boldsymbol{R}$.

Next, we derive the constraints for the upper bound $\bar{t}$. Using (5.7), we are able to derive the maximum amount of data contributed by a worker in each region l. For each region l, let the sensing cost and location granularity of the worker i with the least $\frac{c_i}{\rho_i}$ value be denoted by c_l^m and ρ_l^m respectively. From (5.7), the maximum amount of data contributed by this worker is given by:

$$t_l^{\max} = \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\right)\frac{R_{l_i}}{\rho_l^m}. \tag{5.14}$$

This leads to the following Lemma 5.4.

Lemma 5.4. *The crowdsourcer is able to achieve an upper bound $\bar{t}$ for all workers in location l that satisfies the equivalent Stackelberg equilibrium arising from the unconstrained setting as detailed in Theorem 5.3 as long as the following reward constraint is satisfied:*

$$R_l^{\max} = \bar{t}\rho_l^m\left[\frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1 - \frac{(|\mathcal{Q}_l|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\right]^{-1}. \tag{5.15}$$

Proof. Consider the data $t_l^{\max}$ contributed by the participating worker with the least $\frac{c_i}{\rho_i}$ value. We require the $t_l^{\max}$ in (5.14) to be less than of equals to $\bar{t}$. In other words, we have

$$\begin{aligned} & \bar{t} \geq \frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1 - \frac{(|\mathcal{Q}_l|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\frac{R_l}{\rho_l^m}, \\ \overset{\text{(i)}}{\Rightarrow} \quad & R_l \leq \bar{t}\rho_l^m\left[\frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1 - \frac{(|\mathcal{Q}_l|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\right]^{-1}, \end{aligned} \tag{5.16}$$

where (i) the term $1 - \frac{(|\mathcal{Q}_l|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_l} c_j} > 0$. This is because in the unconstrained setting from (5.8), $\frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} < 1, \forall i \in \mathcal{Q}_l$. And in the constrained setting from (5.11), $\frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \leq 1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}, \forall i \in \mathcal{Q}_l$.

Therefore, this leads to the constraint in (5.15). To verify that Lemma 5.4 is valid, we substitute the $R_l^{\max}$ term from (5.15) to the $t_l^{\max}$ term from (5.14) to obtain $t_l^{\max} \leq \bar{t}$. Note that the constraint on R_l simply constraints the feasible region and does not affect the concavity of the crowdsourcer's maximization problem. □

Theorem 5.5. *The crowdsourcer is able to achieve both the lower bound $\underline{t}$ and upper bound $\bar{t}$ for all workers in location l that satisfies the Stackelberg equilibrium in the unconstrained setting if the following constraints are satisfied:*

$$c_i \leq \frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1-\frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right], \quad \forall i \in \mathcal{Q}_l, \tag{5.17}$$

and

$$R_l^{\max} = \bar{t}\rho_l^m\left[\frac{(|\mathcal{Q}_l|-1)}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\left(1-\frac{(|\mathcal{Q}_l|-1)c_l^m}{\sum\limits_{j\in\mathcal{Q}_l} c_j}\right)\right]^{-1}, \tag{5.18}$$

where each region l, we let the sensing cost and location granularity of the worker i with the least $\frac{c_i}{\rho_i}$ value be denoted by c_l^m and ρ_l^m respectively.

Proof. See Lemmas 5.3 and 5.4. □

Corollary 5.2. *The Stackelberg equilibrium can be shown to exist under the constraints in Theorem 5.5 but the uniqueness property of the unconstrained solution is lost. Furthermore, the solution can be obtained via the same algorithmic solution as utilized in the original unconstrained case, with an additional modification to line 5 of Algorithm 5.1 as shown in Algorithm 5.2.*

Interestingly, we also have the following Lemma 5.5.

Lemma 5.5. *Let $\mathcal{J}_l$ and $\mathcal{K}_l$ represent the set of participating workers i in location l with $t_i = \bar{t}$ and $0 < t_i < \bar{t}$ respectively. The crowdsourcer is able to achieve an upper bound $\bar{t}$ for all workers if he buys $t_j = \bar{t}$ amount of data for all $j \in \mathcal{J}_l$ and buys the following amount of data from all*

Algorithm 5.2: Compute the bounded Nash equilibrium of the Followers game.

function SolveBoundedFollowerGame($\boldsymbol{c}, \boldsymbol{\rho}, \boldsymbol{l}, \boldsymbol{R}, \underline{t}, \bar{t}$)

Input : sensing costs $\boldsymbol{c}_{1,\dots,N}$, location granularities $\boldsymbol{\rho}_{1,\dots,N}$, workers' regions $\boldsymbol{l}_{1,\dots,N}$, rewards $\boldsymbol{R}_{1,\dots,L}$.

Output : data sold to crowdsourcer $\boldsymbol{t}^*_{1,\dots,N}$.

foreach *region* $l \in \mathcal{L}$ **do**
  Compute t_i^* for all workers in l using Algorithm 5.1.
  if *there exists one or more participating worker* i *with* $t_i^* \geq \underline{t}$ **then**
    Sort workers in l according to their privacy-weighted cost $\frac{c_i}{\rho_i}$ in ascending order where $\frac{c_i}{\rho_i} \leq \frac{c_{i+1}}{\rho_{i+1}}$.
    Let $\mathcal{Q}_l = \{1,2\}$ be the set of participating workers with $t_i^* > 0$.
    Set $\mathcal{Q}_l \leftarrow \mathcal{Q}_l \cup \{i\}$ for each worker i in region l if condition (5.17) of Theorem 5.5 is met. (note: the looping can stop at the ith step when the condition is not met.)
    Set t_i^* according to (5.7) for all workers in l.
  else
    Set $t_i^* = 0$ for all workers i in l.
end

$i \in \mathcal{K}_l$:

$$t_i^* = \frac{1}{\rho_i}\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2\rho_i}{R_l}\sum_{k\in\mathcal{K}_l}c_k}$$
$$-\frac{c_i}{R_l\rho_i}\left[\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k}\right]^2.$$

See Section 5.8.6 for proof.

Next, we study the condition where Lemma 5.5 holds. From (5.40), we have

$$c_i = R_l\rho_i\left[\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k}\right]^{-2}$$
$$\times\left\{\frac{1}{\rho_i}\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l}c_k\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l}c_k\left(\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2\rho_i}{R_l}\sum_{k\in\mathcal{K}_l}c_k} - t_i^*\right\}. \tag{5.19}$$

Hence, Lemma 5.5 holds when (5.19) satisfies the constraint in (5.18).

Theorem 5.6. *The crowdsourcer is able to achieve both the lower bound $\underline{t}$ and upper bound $\bar{t}$ for all workers in location l that satisfies the Stackelberg equilibrium in the unconstrained setting if the following constraints are satisfied:*

$$c_i \leq \frac{\sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)}\left[1-\frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_l} c_j}{(|\mathcal{Q}_l|-1)R_l}\right], \quad \forall i \in \mathcal{Q}_l,$$

and $t_j = \bar{t}$ for all $j \in \mathcal{J}_l$, and for all $k \in \mathcal{K}_l$,

$$t_k^* = \frac{1}{\rho_i}\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k \sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j - |\mathcal{K}_l|\right) + \sqrt{\left(1+\frac{2}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k \sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j - |\mathcal{K}_l|\right)^2 - \frac{4}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k\left(\frac{1}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k\left(\sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2 - |\mathcal{K}_l|\sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2\rho_i}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k}$$

$$-\frac{c_i}{R_l\rho_i}\left[\sum_{j\in\mathcal{J}_l}\bar{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k \sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j - |\mathcal{K}_l|\right) + \sqrt{\left(1+\frac{2}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k \sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j - |\mathcal{K}_l|\right)^2 - \frac{4}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k\left(\frac{1}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k\left(\sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)^2 - |\mathcal{K}_l|\sum\limits_{j\in\mathcal{J}_l}\bar{t}\rho_j\right)}}{\frac{2}{R_l}\sum\limits_{k\in\mathcal{K}_l} c_k}\right]^2.$$

where we let $\mathcal{J}_l$ and $\mathcal{K}_l$ represent the set of participating workers i in location l with $t_i = \bar{t}$ and $0 < t_i < \bar{t}$ respectively.

Proof. See Lemmas 5.3 and 5.5. □

However, we do not currently have an algorithm that outputs the desired result in the Theorem 5.6. The difference between the solution of Lemma 5.4 compared to Lemma 5.5 is that the former requires an upper bound on the reward allocation for each region l while the latter states the sufficient conditions on the amount of data contribution from each worker.

Next, we have the following Theorem 5.7, which states the feasible bounds $\underline{t}$ and $\bar{t}$ for each worker i. This allows the crowdsourcer to estimate the number of participating workers in a region l given his reward allocation R_l.

Theorem 5.7. *The feasible bounds $\underline{t}$ and $\bar{t}$ for each worker i is given by:*

$$\underline{t}\rho_i + \delta_i R_l \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \right)^2 \leq \bar{t}\rho_i, \tag{5.20}$$

where $c_i = \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} \left[1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)R_{l_i}} \right] - \delta_i.$

Proof. From (5.36), we have $t_i^*\rho_i = \sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j - \frac{c_i}{R_{l_i}} \Big(\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j \Big)^2$.

If $t_i \leq \bar{t}$, then

$$\begin{aligned}
&\sum_{j\in\mathcal{Q}_{l_i}} t_j\rho_j - \frac{c_i}{R_{l_i}} \left(\sum_{j\in\mathcal{Q}_{l_i}} t_j\rho_j \right)^2 \leq \bar{t}\rho_i, \\
\overset{\text{(i)}}{\Rightarrow} \quad &\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} - \frac{c_i}{R_{l_i}} \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} \right)^2 \leq \bar{t}\rho_i, \\
\overset{\text{(ii)}}{\Rightarrow} \quad &\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} - \left(\frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} \left(1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)R_{l_i}} \right) - \delta_i \right) \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \right)^2 R_{l_i} \leq \bar{t}\rho_i, \\
&\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} - \left(\frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} - \left(\frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} \right)^2 \frac{\underline{t}\rho_i}{R_{l_i}} - \delta_i \right) \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \right)^2 R_{l_i} \leq \bar{t}\rho_i, \\
&\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} - \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i} + \underline{t}\rho_i + \delta_i R_{l_i} \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \right)^2 \leq \bar{t}\rho_i, \\
&\underline{t}\rho_i + \delta_i R_{l_i} \left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} \right)^2 \leq \bar{t}\rho_i,
\end{aligned}$$

where (i) we substitute $\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j = \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i}$ from (5.29) and (ii) we let $c_i = \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} \Big(1 - \frac{\underline{t}\rho_i \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)R_{l_i}} \Big) - \delta_i$. □

Remarks: The feasible $\underline{t}$ and $\bar{t}$ for each worker i varies according to the its sensing cost c_i, which affects δ_i (the difference between the maximum allowable sensing cost in the set of

participating workers and c_i). When $\delta_i = 0$, there is strict equality in (5.20). However, as δ_i increases, we have $\underline{t} << \bar{t}$. Also for a fixed reward R_l, the gap between $\underline{t}$ and $\bar{t}$ increases as the number of participating workers $\mathcal{Q}_{l_i}$ increases.

5.5.2 Achieving Pareto Efficiency

We examine the Pareto efficiency (see Definition 5.3) of our proposed incentive scheme and study how to achieve efficiency. A Pareto efficient incentive scheme implies that it is not possible to reallocate the rewards without making at least one worker or the crowdsourcer worse off. In other words, the rewards are allocated in the most efficient manner.

Definition 5.3 (Pareto Efficiency)**.** *A strategy profile* $(\boldsymbol{R}^P, \boldsymbol{t}^P)$ *is Pareto efficient if there exists no other strategy* $(\boldsymbol{R}, \boldsymbol{t})$ *where* $\boldsymbol{R} \succeq 0, \boldsymbol{t} \succeq 0$ *such that:*

$$U_{CS}(\boldsymbol{R}; \boldsymbol{t}) \geq U_{CS}(\boldsymbol{R}^P; \boldsymbol{t}^P),$$
$$u_i(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, \boldsymbol{R}) \geq u_i(t_i^P; \boldsymbol{t}_{-\boldsymbol{i}}^P, \boldsymbol{R}^P), \quad \forall i \in \mathcal{I},$$

with at least one strict inequality.

Theorem 5.8. *The proposed (unbounded) Stackelberg game has a unique Stackelberg equilibrium* $(\boldsymbol{R}^{SE}, \boldsymbol{t}^{SE})$ *that may not be Pareto efficient. See Section 5.8.7 for proof.*

To achieve efficiency, we first define a social welfare function $w(\boldsymbol{R}, \boldsymbol{t})$ to be the weighted sum of the crowdsourcer and the workers' utilities:

$$\begin{aligned} w(\boldsymbol{R}, \boldsymbol{t}) &= \gamma_{CS} U_{CS}(\boldsymbol{R}; \boldsymbol{t}) + \sum_{i \in \mathcal{I}} \gamma_i u_i(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, R_{l_i}) \\ &= \gamma_{CS} \sum_{i \in \mathcal{I}} \lambda_i \log(1 + t_i) + \sum_{i \in \mathcal{I}} \gamma_i \left(\frac{t_i \rho_i}{\sum_{j \in \mathcal{Q}_{l_i}} t_j \rho_j} R_{l_i} - c_i t_i \right), \end{aligned} \tag{5.21}$$

for some weights $\gamma_{CS}, \gamma_1, \ldots > 0$.

It is well-known that any allocation which maximizes a social welfare function is also Pareto-

efficient. Thus, to achieve efficiency, we can introduce a penalty function:

$$\Psi(\boldsymbol{t}) = \sum_{i \in \mathcal{I}} \gamma_i \left(\frac{t_i \rho_i}{\sum\limits_{j \in \mathcal{Q}_{l_i}} t_j \rho_j} R_{l_i} - c_i t_i \right),$$

to the crowdsourcer's utility function:

$$U_{CS}(\boldsymbol{R}; \boldsymbol{t}) = \gamma_{CS} \sum_{i \in \mathcal{I}} \lambda_i \log(1 + t_i) + \Psi(\boldsymbol{t}). \tag{5.22}$$

This induces the crowdsourcer to maximize $w(\boldsymbol{R}, \boldsymbol{t})$. An example of how to encourage the crowdsourcer to behave this way would be if there exists a regulator who can offer tax rebates proportional to the weighted sum of the worker's utilities.

5.6 Case Study

We designed a case study to evaluate the predictive performance of the dataset collected by our proposed Stackelberg incentive model, which attempts to maximize coverage. We studied a real-world mobile crowd sensing problem such as the spatial monitoring and prediction of environmental temperature [136, 137]. We compared the proposed Stackelberg model against two baseline schemes that seek to maximize the coverage of the collected dataset.

5.6.1 Baseline Coverage Metrics

We use the two baseline schemes: (i) the location-based incentive mechanism proposed in [132], which maximizes a geometric disk coverage model, and (ii) the works in [133–135], which maximizes a k-depth coverage model. The two coverage models (see Fig. 5.3) are detailed as followed.

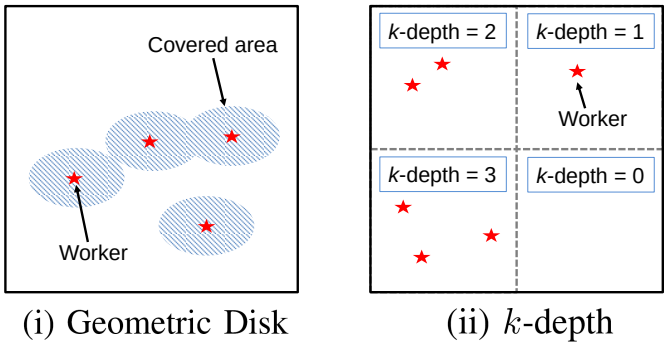


Figure 5.3: Illustration of the geometric disk and k-depth coverage metrics.

Geometric Disk Coverage Metric

The geometric disk model was proposed in [132] to measure coverage of a sensor data from a precise (uncloaked) location $\mathbf{x}_i$. The coverage is given by:

$$c(\mathbf{x}_i) = \begin{cases} 1 & \text{if } ||\mathbf{x}_i - \mathbf{x}_j||_2 \leq r, \\ 0 & \text{otherwise,} \end{cases} \tag{5.23}$$

where $||\cdot||_2$ denotes the Euclidean distance and r is the sensed radius of the sensor data.

To optimize this metric, the crowdsourcer will greedily buy the minimum data from all worker, starting with the cheapest worker first. If there exists a surplus after the greedy allocation, the crowdsourcer simply buys all the remaining data from the cheapest worker until the upper bound $\tilde{t}$ is reached, before continuing with the next cheapest worker and so on.

k-depth Coverage Metric

The following k-depth coverage model (and its variants) was proposed in [133–135] to measure coverage of a set of N sensor data $t_1, \ldots, t_N$ from a region l where $c(t_1, \ldots, t_N) = \min(N, k)$ or equivalently:

$$c(t_1, \ldots, t_N) = \begin{cases} N & \text{if } N \leq k, \\ k & \text{otherwise,} \end{cases} \tag{5.24}$$

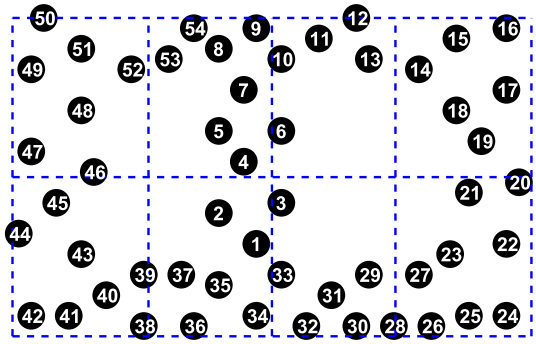


Figure 5.4: Partitioned regions of the Intel lab consisting of sensors 1–54.

where k is the depth parameter. The metric assumes that all sensing data t_i are of the same quantity.

To optimize this metric, the crowdsourcer will greedily buy the minimum data from the k cheapest workers in each region, starting with the cheapest worker first. If there exists some surplus after the greedy allocation, the crowdsourcer simply buys all the remaining data from the cheapest worker until the upper bound is reached, before continuing with the next cheapest worker and so on.

5.6.2 Simulation Setup

We use the temperature measurements from the Intel lab data [138], which contains the temperature, humidity, light, voltage, connectivity, and location information collected from 54 sensor nodes deployed in the Intel Berkeley Research lab between February 28th and April 5th, 2004. We partitioned the lab's spatial area into the eight regions as shown in Fig. 5.4. The proposed Stackelberg incentive model and the baseline schemes are then used to purchase a subset of the available temperature data. We randomly took a 1-hour interval from the dataset and apply the Gaussian process regression technique [139] (a supervised learning technique for regression) to evaluate how the two coverage metrics correspond to the actual amount of predictive uncertainty. The (Gaussian) radial basis function (RBF) kernel [139] is used for our Gaussian process regression.

We briefly introduce the main idea behind the Gaussian process regression. Given a set of n input location vector $\mathbf{x}$ and observations $\mathbf{y}$, we assume that the observed $\mathbf{y}$ are generated by some latent function f plus an independent and identically distributed Gaussian noise with zero mean and variance σ_y^2. Suppose there are n_* test points. Let $k(\cdot,\cdot)$ be a covariance function and let $K(X,X_*)$ denotes the $n \times n_*$ (kernel) matrix of the covariances evaluated at all pairs of training and test points, and similarly for $K(X,X), K(X_*,X_*)$ and $K(X_*,X)$. The predictive (posterior) equations for the Gaussian process regression for a new input test vector x_* are:

$$\begin{aligned} \bar{f}_*(x_*) &= K(X_*,X)[K(X,X)+\sigma_y^2 I]^{-1}\mathbf{y}, \\ V(x_*) &= K(X_*,X_*) - K(X_*,X)[K(X,X)+\sigma_y^2 I]^{-1}K(X,X_*). \end{aligned} \tag{5.25}$$

The following two test scenarios were examined.

Test Scenarios

Scenario (I): Spatial regression of the two cross intersections (second and fourth column from the left side of Fig. 5.4) where no sensor data is available. The workers' sensing cost c_i were set to be inversely proportional to the average of the distance to the two cross intersections and their location granularity ρ_i were inversely proportional to the number of workers in their respective regions. We conducted spatial Gaussian process regression to obtain the predictive variance $V(x_*)$ of the two cross intersections. A lower predictive variance implies better predictive performance.

Scenario (II): Spatial regression of the entire spatial area shown in Fig. 5.4. The workers' sensing cost c_i were uniformly selected and their location granularity ρ_i were inversely proportional to the number of workers in their respective regions. We conducted spatial Gaussian process regression to obtain the predicted (mean) temperature $\bar{f}_*(x_*)$ of all the sensor locations. We then compute the mean squared error (MSE) between the predicted temperature and the actual temperature measurement from the dataset. A lower MSE value implies better predictive performance.

Simulation Parameters

The following simulation parameters were used: sensing cost $c_i \in (0,1]$, location granularity $\rho_i \in [1,2]$, budget $R^{\text{budget}} = 15$, minimum data $\underline{t} = 1$, maximum data $\bar{t} = 3$. We set the budget constraint to limit the number of purchased data, i.e., purchase only a subset of the available temperature data. In the two baseline schemes, we offer each worker their sensing cost plus some bonus price for each unit of data. The bonus price is obtained by taking the total utility of the workers over the total amount of data purchased. We used $k = 2$ in the baseline k-depth coverage scheme. We let the crowdsourcer's system parameter $\lambda_i = \rho_i$.

5.6.3 Simulation Results and Discussion

We now discuss the simulation results for the following two test scenarios.

Scenario (I): We list the predictive variances of the two baseline schemes and the proposed Stackelberg incentive model at the two cross intersections of interest in Table 5.2, and the corresponding coverage scores in Table 5.3. From the results, we observed that the proposed Stackelberg incentive model has a significantly better predictive variances in the two cross intersections compared to the two baseline schemes. This is despite the k-depth score for the proposed Stackelberg incentive model being lower than the baseline schemes. The locations of the participating workers and the amount of data purchased from them are different under the three different coverage maximizing schemes. The proposed Stackelberg incentive model purchases less data (on average) from each participating worker but purchases data from more workers. To visualize the locations of the participating workers and the predictive variances, we plot the heat map of the predictive variances for the baseline schemes and the proposed Stackelberg incentive model in Figs. 5.5 and 5.6 respectively.

Scenario (II): We list the MSE values of the two baseline schemes and the proposed Stackelberg incentive model for the entire spatial area of interest in Table 5.4, and the corresponding coverage scores in Table 5.5. From the results, we observed that the proposed Stackelberg incentive model has a significantly better predictive performance (lower MSE and its standard

Table 5.2: Predictive standard deviation values for Scenario (I).

Scheme	Point 1	Point 2
Disk	0.3340	0.3209
k-depth	0.2673	0.2543
Proposed	0.2242	0.2525

Table 5.3: Baseline coverage scores for Scenario (I).

Scheme	Disk	k-depth
Disk	8	13
k-depth	8	16
Proposed	8	15

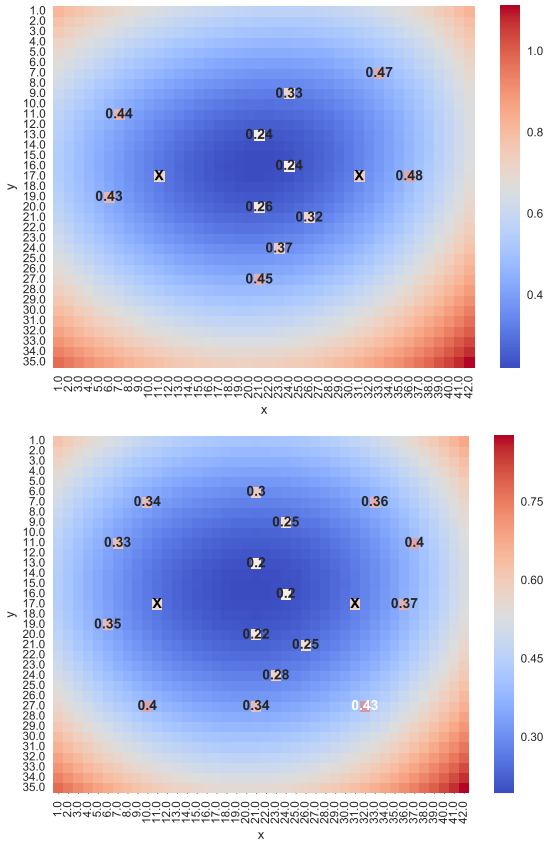


Figure 5.5: Scenario (I): Predictive standard deviation for (i) disk, and (ii) k-depth models.

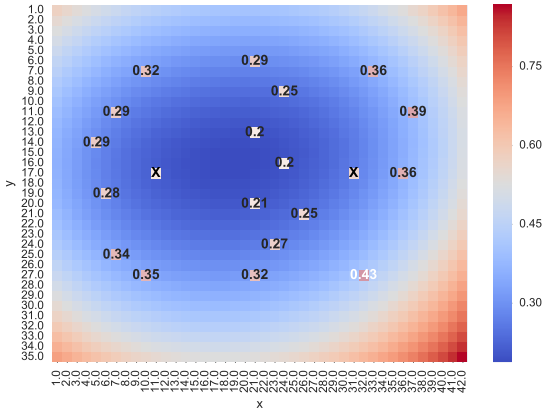


Figure 5.6: Scenario (I): Predictive standard deviation for the proposed Stackelberg incentive model.

Table 5.4: Mean square error (MSE) and its standard deviation for Scenario (II).

Scheme	MSE	Standard Deviation
Disk	28.8995	0.4093
k-depth	28.6062	0.3411
Proposed	27.7277	0.3231

derivation) in the entire spatial area of interest compared to the two baseline schemes. Similar to Scenario (I), the k-depth score for the proposed Stackelberg incentive model is lower than the baseline schemes. Hence, the k-depth scores may not be reflective of the predictive performance of the purchased dataset. To visualize the location of the participating workers and the predicted mean temperature values, we plot the heat map of the predicted mean for the baseline schemes and the proposed Stackelberg incentive model in Figs. 5.7 and 5.8 respectively.

Table 5.5: Baseline coverage scores for Scenario (II).

Scheme	Disk	k-depth
Disk	8	14
k-depth	8	16
Proposed	8	13

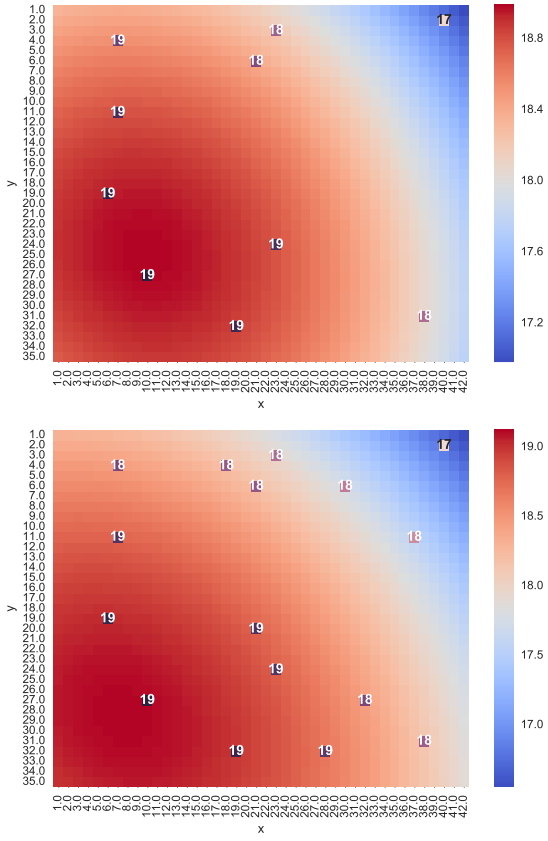


Figure 5.7: Scenario (II): Predictive mean for (i) disk, and (ii) k-depth models.

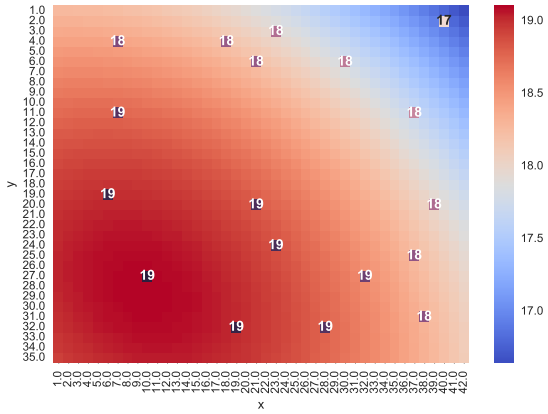


Figure 5.8: Scenario (II): Predictive mean for the proposed Stackelberg incentive model.

Accommodating Location Uncertainty

The Gaussian process regression technique accommodates location uncertainty of the workers' sensing data due to the use of cloaking regions. Assuming that the input locations of the sensing data $\mathbf{x}$ are corrupted by i.i.d. Gaussian noise with the noise variance set to the square of the approximated radius of the cloaking regions, the Gaussian process regression model proposed in [140] can applied to account for location uncertainty. Mainly, an additional corrective term can be added into the noise term in (5.25) to account for the location uncertainty of the training inputs. The corrective term is proportional to the gradient of the posterior mean.

5.7 Conclusion and Future Work

We designed a privacy-aware Stackelberg incentive model that improves the *spatial coverage* of the collected dataset. Our proposed model is privacy-aware, in that it allows privacy-sensitive users to submit coarse-grained (or quantized) location information to the crowdsourcer, and is also dominant strategy incentive-compatible. We then studied the properties of the proposed model analytically and presented efficient algorithmic solutions. We also extended the basic model to accommodate bounds on the users' data contributions and studied how Pareto-efficiency can be achieved. We showed via simulations that our proposed model is superior than two other coverage-maximizing schemes that maximize a different coverage metric.

For future work, it would be interesting to extend our (static game) Stackelberg model for dynamic games played over a period of time where the smartphone users are allowed to move between regions. While our Stackelberg equilibrium is stable in the studied static model played by the crowdsourcer and the mobile smartphone users in one time period, a different notation of equilibrium needs to be considered for the dynamic setting.

5.8 Proofs

5.8.1 Proof of Lemma 5.1

A unique Nash equilibrium exists in the Followers game if for all $i \in \mathcal{I}$ [141]: (i) the domain of the workers' strategy set $\{t_i\}_{i\in\mathcal{I}}$ is convex and compact, and (ii) u_i is continuous and strictly concave in t_i. Indeed, the domain of the workers' strategy set $\{t_i\}_{i\in\mathcal{I}}$ is convex and compact since t_i is assumed to be bounded, and u_i is continuous in t_i, and strictly concave in t_i as $\frac{\partial^2 u_i}{\partial t_i^2} < 0$:

$$\frac{\partial u_i}{\partial t_i} = \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}:j\neq i} t_j\rho_j}{\Big(\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j\Big)^2} R_{l_i} - c_i,$$

$$\frac{\partial^2 u_i}{\partial t_i^2} = \frac{-2\sum\limits_{j\in\mathcal{Q}_{l_i}:j\neq i} t_j\rho_j}{\Big(\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j\Big)^3} R_{l_i} < 0. \tag{5.26}$$

Therefore, a Nash equilibrium exists in the Followers game. □

5.8.2 Proof of Theorem 5.1

According to Lemma 5.1, there exists a unique strategy that maximizes the utility of each worker given the strategies of the other workers. Thus, if each worker i plays its best response strategy, it will achieve the unique Nash equilibrium point t_i^*. To prove Theorem 5.1, we derive t_i^* by solving $\frac{\partial u_i}{\partial t_i} = 0$. From (5.6),

$$R_{l_i}\Bigg(\sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j - t_i^*\rho_i\Bigg) = c_i\Bigg(\sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j\Bigg)^2 \tag{5.27}$$

$$\overset{\text{(i)}}{\Rightarrow} \qquad t_i^*\rho_i = \Bigg(\sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j\Bigg)\Bigg[1 - c_i\Big(\sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j\Big)R_{l_i}^{-1}\Bigg] \tag{5.28}$$

$$\overset{\text{(ii)}}{\Longrightarrow} \quad \sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j = |\mathcal{Q}_{l_i}| \sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j - \sum_{j\in\mathcal{Q}_{l_i}} c_j \left(\sum_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j \right)^2 R_{l_i}^{-1}$$
$$= \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i}, \tag{5.29}$$

where (i) we express $t_i^*\rho_i$ in terms of the other $t_j^*\rho_j$ values, and (ii) we sum up the $t_i^*\rho_i$ values in (5.28) for all participating workers in region l_i.

Finally, we substitute (5.29) into (5.28) to obtain the unique Nash equilibrium point for each worker i as required. □

5.8.3 Proof of Lemma 5.2

We use proof by contradiction to prove Lemma 5.2. Consider the following two possible scenarios where the set of participating workers $\mathcal{Q}_l$ differs from the set computed by Algorithm 5.1. In the first scenario, we remove a worker i from the optimal set and in the second scenario, we add a worker i to the set. Assume that there exists a Nash equilibrium (NE) point for worker i in the two scenarios. Since the strategy of each worker i does not affect the utility of another worker j where $l_i \neq l_j$ [see (5.3)], it is sufficient to only consider the best responses of workers in the region l_i.

Scenario (I): Assume that there exists a NE point for a worker i where $i \notin \mathcal{Q}_{l_i}$ and $c_i < \frac{1}{|\mathcal{Q}_{l_i}|-1} \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j$. The inequality term in the latter can be rewritten as an equality by introducing a variable $\Delta > 0$, assuming $c_i \in (0, \bar{c}]$ is satisfied:

$$c_i = \frac{1}{|\mathcal{Q}_{l_i}|-1} \left(\sum_{j\in\mathcal{Q}_{l_i}} c_j \right) - \Delta. \tag{5.30}$$

In Algorithm 5.1, we set $t_i = 0$ if $i \notin \mathcal{Q}_{l_i}$, and we have $\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j = \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j} R_{l_i}$, from (5.29). Thus,

we obtain the following $\frac{\partial u_i}{\partial t_i}$ expression [from (5.26)] for worker i.

$$\begin{aligned}
\frac{\partial u_i}{\partial t_i} &= \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j - 0}{\Big(\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j\rho_j\Big)^2} R_{l_i} - c_i \\
&= \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} - c_i \\
&\overset{\text{(i)}}{\Rightarrow} = \frac{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}{(|\mathcal{Q}_{l_i}|-1)} - \frac{1}{|\mathcal{Q}_{l_i}|-1}\Bigg(\sum_{j\in\mathcal{Q}_{l_i}} c_j\Bigg) + \Delta \\
&= \Delta - \frac{c_i}{|\mathcal{Q}_{l_i}|-1},
\end{aligned} \tag{5.31}$$

where (i) we substitute the expression for c_i from (5.30).

As $\Delta > 0$ and $\Delta \neq c_i$, we have $\frac{\partial u_i}{\partial t_i} \neq 0$. This indicates that $t_i = 0$ is not a stationary point for worker i, and thus, is not a NE solution for worker i. This is a contradiction and therefore, scenario (I) is not a valid NE solution in the Followers game.

Scenario (II): Assume that there exists a NE point for a worker i where $i \in \mathcal{Q}_{l_i}$ and $c_i \geq \frac{1}{|\mathcal{Q}_{l_i}|-1} \sum\limits_{j\in\mathcal{Q}_{l_i}} c_j$. The inequality term in the latter can be rewritten as an equality by introducing a variable $\Delta \geq 0$, assuming $c_i \in (0, \bar{c}]$ is satisfied:

$$c_i = \frac{1}{|\mathcal{Q}_{l_i}|-1} \sum_{j\in\mathcal{Q}_{l_i}} c_j + \Delta. \tag{5.32}$$

We substitute the expression for c_i from (5.32) into the output of Algorithm 5.1, given by (5.7)

to obtain the NE solution for worker i:

$$\begin{aligned} t_i^* &= \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left[1-\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(\frac{1}{|\mathcal{Q}_{l_i}|-1}\sum_{j\in\mathcal{Q}_{l_i}} c_j+\Delta\right)\right]\left(\frac{R_{l_i}}{\rho_i}\right) \\ &= \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left[1-1-\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\Delta\right]\left(\frac{R_{l_i}}{\rho_i}\right) \\ &= -\left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\right)^2\left(\frac{R_{l_i}\Delta}{\rho_i}\right). \end{aligned} \tag{5.33}$$

Since $R_{l_i}\geq 0$, $|\mathcal{Q}_{l_i}|>1$, $\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}>0$, and $\Delta\geq 0$, we have $t_i^*\leq 0$ and $i\in\mathcal{Q}_{l_i}$ according to (5.33). This contradicts our definition of a participating worker i, which assumes $t_i>0$. Hence, scenario (II) is not a valid scenario. Therefore, we conclude that Algorithm 5.1 selects the optimal set of participating workers $\mathcal{Q}_l$ since any deviation from the set leads to an invalid Nash equilibrium solution. □

5.8.4 Proof of Theorem 5.2

To show that the obtained solution from Algorithm 5.1 is the unique Nash equilibrium (NE) solution of the workers, we prove that the $\frac{\partial u_i}{\partial t_i}=0$ (stationary point) condition given in (5.27) is satisfied by the set of participating workers $i\in\mathcal{Q}_l$. By Lemma 5.1, there exists a unique NE in the followers game. Hence, any stationary point is the unique NE point for the workers. From Algorithm 5.1, we have $t_i^*=\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(1-\frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\right)\frac{R_{l_i}}{\rho_i}$, if $i\in\mathcal{Q}_{l_i}$, and $t_i^*=0$, otherwise. In addition, we have the expression $\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j=\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}R_{l_i}$ from (5.29). We substitute the expressions for t_i^* and $\sum\limits_{j\in\mathcal{Q}_{l_i}} t_j^*\rho_j$ into the $\frac{\partial u_i}{\partial t_i}$ expression in (5.27) to obtain the following equality:

$$\frac{(|\mathcal{Q}_{l_i}|-1)R_{l_i}}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\left(\frac{(|\mathcal{Q}_{l_i}|-1)c_i}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}\right)R_{l_i}=c_i\left[\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum\limits_{j\in\mathcal{Q}_{l_i}} c_j}R_{l_i}\right]^2. \tag{5.34}$$

Since (5.34) satisfies the expression for $\frac{\partial u_i}{\partial t_i}=0$, we conclude that Algorithm 5.1 correctly outputs the unique Nash equilibrium solution of the workers in $\mathcal{Q}_l$. Also, by Lemma 5.2,

Algorithm 5.1 also correctly computes the set of participating workers $\mathcal{Q}_l$. □

5.8.5 Proof of Theorem 5.4

Recall that the worker's utility function $u_i(t_i, R_{l_i})$ is strictly concave in t_i as shown in Lemma 5.1. Hence, to prove dominant strategy incentive-compatibility, we need to show that the worker's true sensing cost c_i maximizes u_i, i.e., $\frac{\partial u_i}{\partial c_i} = 0$ at the worker's true sensing cost c_i. Using the chain rule, we know that $\frac{\partial u_i}{\partial c_i} = \frac{\partial u_i}{\partial t_i} \times \frac{\partial t_i}{\partial c_i}$. This means that u_i is maximized, i.e., $\frac{\partial u_i}{\partial c_i} = 0$ when $\frac{\partial u_i}{\partial t_i} = 0$ and the term $\frac{\partial t_i}{\partial c_i}$ can take any arbitrary value. Thus, we only need to show that $\frac{\partial u_i}{\partial t_i} = 0$ is satisfied when the worker i declares his true sensing cost c_i to the crowdsourcer.

Suppose worker i declares a sensing cost of c_i' (where $c_i' = c_i + \delta$) while the remaining workers $j \neq i$ declare a sensing cost of $c_j + \Delta_j$. We first find the expressions for t_i^* and $\sum_{j \in \mathcal{Q}_{l_i}} t_j^* \rho_j$. Under the proposed game in Algorithm 5.1, the crowdsourcer offers to buy $t_i^* = \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}\left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)(c_i+\delta)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}\right)\frac{R_{l_i}}{\rho_i}$ amount of data from the worker i according to (5.7). Next, we obtain the expression: $\sum_{j \in \mathcal{Q}_{l_i}} t_j^* \rho_j = \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j} R_{l_i}$, from (5.29).

Finally, we substitute the two expressions for t_i^* and $\sum_{j \in \mathcal{Q}_{l_i}} t_j^* \rho_j$ into the $\frac{\partial u_i}{\partial t_i}$ term in (5.26) to obtain:

$$
\begin{aligned}
\frac{\partial u_i}{\partial t_i} &= \frac{\sum_{j \in \mathcal{Q}_{l_i}} t_j \rho_j - t_i \rho_i}{\left(\sum_{j \in \mathcal{Q}_{l_i}} t_j \rho_j\right)^2} R_{l_i} - c_i \\
&= \left[\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j} R_{l_i} - \frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}\left(1 - \frac{(|\mathcal{Q}_{l_i}|-1)(c_i+\delta)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}\right) R_{l_i}\right] \\
&\quad \times \left(\frac{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}{(|\mathcal{Q}_{l_i}|-1) R_{l_i}}\right)^2 R_{l_i} - c_i \\
&= \left[\left(\frac{(|\mathcal{Q}_{l_i}|-1)}{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}\right)^2 (c_i+\delta) R_{l_i}\right]\left(\frac{\sum_{j \in \mathcal{Q}_{l_i}} c_j+\delta+\Delta_j}{(|\mathcal{Q}_{l_i}|-1) R_{l_i}}\right)^2 R_{l_i} - c_i \\
&= (c_i+\delta) - c_i = \delta. \qquad (5.35)
\end{aligned}
$$

Hence, it is clear from (5.35) that $\frac{\partial u_i}{\partial t_i} = 0$ when $\delta = 0$. This is a necessary condition that is only true if $c_i' = c_i$. Therefore, we have shown that worker i does not have incentive to declare a false sensing cost $c_i' \neq c_i$. □

5.8.6 Proof of Lemma 5.5

To achieve an upper bound $\bar{t}$ for all workers i, we require $t_i^* \leq \bar{t}, \forall i \in \mathcal{Q}_{l_i}$. Given that $t_j = \bar{t}, \forall j \in \mathcal{J}_l$, we attempt to derive an expression for t_i^* for $i \in \mathcal{K}_l$. From (5.28),

$$\begin{aligned} t_i^* \rho_i &= \left(\sum_{j \in \mathcal{Q}_l} t_j \rho_j \right) - \frac{c_i}{R_l} \left(\sum_{j \in \mathcal{Q}_l} t_j \rho_j \right)^2 \\ &= \left(\sum_{j \in \mathcal{J}_l} t_j \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right) - \frac{c_i}{R_l} \left(\sum_{j \in \mathcal{J}_l} t_j \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right)^2 \\ &= \left(\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right) - \frac{c_i}{R_l} \left(\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right)^2 . \end{aligned} \tag{5.36}$$

Next, we sum up the $t_i^* \rho_i$ in (5.36) for all participating workers $i \in \mathcal{K}_l$ to obtain:

$$\begin{aligned} \sum_{i \in \mathcal{K}_l} t_i^* \rho_i &= |\mathcal{K}_l| \left(\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right) - \frac{1}{R_l} \sum_{k \in \mathcal{K}_l} c_k \left[\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j + \sum_{k \in \mathcal{K}_l} t_k \rho_k \right]^2 \\ &= |\mathcal{K}_l| \sum_{j \in \mathcal{J}_l} \bar{t} \rho_j + |\mathcal{K}_l| \sum_{k \in \mathcal{K}_l} t_k \rho_k \\ &\quad - \frac{1}{R_l} \sum_{k \in \mathcal{K}_l} c_k \left[\left(\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j \right)^2 + 2 \sum_{j \in \mathcal{J}_l} \bar{t} \rho_j \sum_{k \in \mathcal{K}_l} t_k \rho_k + \left(\sum_{k \in \mathcal{K}_l} t_k \rho_k \right)^2 \right]. \end{aligned} \tag{5.37}$$

We then rearrange (5.37) such that $\sum_{k \in \mathcal{K}_l} t_k^* \rho_k$ can be solved using the quadratic formula:

$$\begin{aligned} &\frac{1}{R_l} \sum_{k \in \mathcal{K}_l} c_k \left(\sum_{k \in \mathcal{K}_l} t_k \rho_k \right)^2 + \left(1 + \frac{2}{R_l} \sum_{k \in \mathcal{K}_l} c_k \sum_{j \in \mathcal{J}_l} \bar{t} \rho_j - |\mathcal{K}_l| \right) \sum_{k \in \mathcal{K}_l} t_k \rho_k \\ &\quad + \left(\frac{1}{R_l} \sum_{k \in \mathcal{K}_l} c_k \left(\sum_{j \in \mathcal{J}_l} \bar{t} \rho_j \right)^2 - |\mathcal{K}_l| \sum_{j \in \mathcal{J}_l} \bar{t} \rho_j \right) = 0. \end{aligned} \tag{5.38}$$

Given a quadratic equation, the solution for x is given by the formula $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

The optimal $\sum_{k\in\mathcal{K}_l} t_k^*\rho_k$ for all participating workers $k\in\mathcal{K}_l$ is obtained from (5.38):

$$\sum_{k\in\mathcal{K}_l} t_k^*\rho_k = \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)}}{\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k}. \tag{5.39}$$

Finally, we substitute (5.39) into (5.36) to obtain the optimal amount of t_i^* for all participating workers $i\in\mathcal{K}_l$:

$$t_i^* = \frac{1}{\rho_i}\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)}}{\frac{2\rho_i}{R_l}\sum_{k\in\mathcal{K}_l} c_k}$$
$$-\frac{c_i}{R_l\rho_i}\left[\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j + \frac{-\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)+\sqrt{\left(1+\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k \sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j-|\mathcal{K}_l|\right)^2-\frac{4}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\frac{1}{R_l}\sum_{k\in\mathcal{K}_l} c_k\left(\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)^2-|\mathcal{K}_l|\sum_{j\in\mathcal{J}_l}\tilde{t}\rho_j\right)}}{\frac{2}{R_l}\sum_{k\in\mathcal{K}_l} c_k}\right]^2. \tag{5.40}$$

□

5.8.7 Proof of Theorem 5.8

To prove Theorem 5.8, we make the following two claims.

Claim 5.1. *Suppose λ_i, ρ_i, and c_i values are constant for all $i\in\mathcal{I}$, the proposed Stackelberg game is Pareto efficient.*

Proof. To prove the claim, we use the following key observations:

$$\sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j;\boldsymbol{t}_{-\boldsymbol{j}},R_{l_j}) = R_{l_i} - \sum_{j\in\mathcal{Q}_{l_i}} c_j t_j. \tag{5.41}$$

$$U_{CS}(\boldsymbol{R};\boldsymbol{t}) = \lambda_{\text{constant}}\sum_{i\in\mathcal{I}}\log(1+t_i). \tag{5.42}$$

Consider a strategy profile $(\boldsymbol{R},\boldsymbol{t})\neq(\boldsymbol{R}^{SE},\boldsymbol{t}^{SE})$. If $U_{CS}(\boldsymbol{R};\boldsymbol{t}) > U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$, then $\exists i$ where $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) < u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE})$. It can be shown that the previous statement is true since

$\sum_{j\in\mathcal{Q}_{l_i}} t_j > \sum_{j\in\mathcal{Q}_{l_i}} t_j^{SE}$ is a necessary condition for $U_{CS}(\boldsymbol{R};\boldsymbol{t}) > U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$. From (5.41), we know that $\sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j;\boldsymbol{t}_{-\boldsymbol{j}},R_{l_j})$ is inversely proportional to $\sum_{j\in\mathcal{Q}_{l_i}} c_j t_j$. This means that if $\sum_{j\in\mathcal{Q}_{l_i}} t_j > \sum_{j\in\mathcal{Q}_{l_i}} t_j^{SE}$ is true, then we have $\sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j;\boldsymbol{t}_{-\boldsymbol{j}},R_{l_j}) < \sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j^{SE};\boldsymbol{t}_{-\boldsymbol{j}}^{SE},R_{l_j}^{SE})$. Hence, we conclude that $\exists i$ where $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) < u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE})$.

Similarly, it can be shown that if $\exists i$ where $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) > u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE})$ and $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) \geq u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE}), \forall i \in \mathcal{I}$, then $U_{CS}(\boldsymbol{R};\boldsymbol{t}) < U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$. This is because if $\exists i$ where $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) > u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE})$ and $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) \geq u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE}), \forall i \in \mathcal{I}$, then we have $\sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j;\boldsymbol{t}_{-\boldsymbol{j}},R_{l_j}) > \sum_{j\in\mathcal{Q}_{l_i}} u_j(t_j^{SE};\boldsymbol{t}_{-\boldsymbol{j}}^{SE},R_{l_j}^{SE})$. This is only possible if $\sum_{j\in\mathcal{Q}_{l_i}} c_j t_j < \sum_{j\in\mathcal{Q}_{l_i}} c_j t_j^{SE}$, which means $\sum_{j\in\mathcal{Q}_{l_i}} t_j < \sum_{j\in\mathcal{Q}_{l_i}} t_j^{SE}$. Therefore, from (5.42), we conclude that $U_{CS}(\boldsymbol{R};\boldsymbol{t}) < U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$.

Hence, the proof is complete.

□

Claim 5.2. *The proposed Stackelberg game may not have a Pareto efficient Stackelberg equilibrium. In other words, suppose that* $(\boldsymbol{R},\boldsymbol{t}) \neq (\boldsymbol{R}^{SE},\boldsymbol{t}^{SE})$ *and* $U_{CS}(\boldsymbol{R};\boldsymbol{t}) > U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$*, we have* $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) \geq u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE}), \forall i \in \mathcal{I}$.

Proof. Consider the scenario where there are 2 regions l_1 and l_3 with 2 workers each. Let $\rho_i = 1, c_i = 1$ for the workers in the 2 regions. Let $l_1 = l_2$ and $l_3 = l_4$, $\lambda_1 = \lambda_2, \lambda_3 = \lambda_4$, and $\lambda_1 < \lambda_3$. Intuitively, given that the worker costs are the same but $\lambda_1 < \lambda_3$, then $R_{l_1}^{SE} < R_{l_3}^{SE}$.

Since $U_{CS}(\boldsymbol{R};\boldsymbol{t}) > U_{CS}(\boldsymbol{R}^{SE};\boldsymbol{t}^{SE})$, suppose we have $R_{l_3} > R_{l_3}^{SE}$ and $R_{l_1} < R_{l_1}^{SE}$ (recall that the total rewards is bounded, so R_{l_1} must decrease if R_{l_3} increases). Let $R_{l_3} = R_{l_3}^{SE} + \Delta$ and $R_{l_1} = R_{l_1}^{SE} - \Delta$ where $\Delta > 0$.

First, we obtain the closed-form expressions for t_i. We substitute the ρ_i and c_i values into (5.7) and obtain:

$$t_i^{SE} = \frac{R_{l_i}^{SE}}{2}(1-\frac{1}{2}) = \frac{R_{l_i}^{SE}}{4}, \forall i \in \mathcal{I}. \tag{5.43}$$

Similarly, we substitute (5.43) into (5.3) to obtain

$$u_i(t_i^{SE}; \boldsymbol{t}_{-\boldsymbol{i}}^{SE}, R_{l_i}^{SE}) = \frac{R_{l_i}^{SE}}{2} - \frac{R_{l_i}^{SE}}{4} = \frac{R_{l_i}^{SE}}{4}. \tag{5.44}$$

Suppose $u_1(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, R_{l_i}) \geq u_1(t_i^{SE}; \boldsymbol{t}_{-\boldsymbol{i}}^{SE}, R_{l_i}^{SE})$, from (5.3), we have:

$$\frac{R_{l_1}^{SE} - \Delta}{2} - t_1 \geq \frac{R_{l_1}^{SE}}{4}, \tag{5.45}$$

$$t_1 \leq \frac{R_{l_1}^{SE} - 2\Delta}{4}, \tag{5.46}$$

$$t_1 = \frac{R_{l_1}^{SE} - 2\Delta}{4} - \Delta', \tag{5.47}$$

where $\Delta' \geq 0$.

Similarly, if $u_3(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, R_{l_i}) \geq u_3(t_i^{SE}; \boldsymbol{t}_{-\boldsymbol{i}}^{SE}, R_{l_i}^{SE})$, from (5.3), we have:

$$\frac{R_{l_3}^{SE} + \Delta}{2} - t_3 \geq \frac{R_{l_3}^{SE}}{4}, \tag{5.48}$$

$$t_3 \leq \frac{R_{l_3}^{SE} + 2\Delta}{4}, \tag{5.49}$$

$$t_3 = \frac{R_{l_3}^{SE} + 2\Delta}{4} - \Delta', \tag{5.50}$$

where $\Delta' \geq 0$.

Since we assume that $U_{CS}(\boldsymbol{R}; \boldsymbol{t}) > U_{CS}(\boldsymbol{R}^{SE}; \boldsymbol{t}^{SE})$, for $u_i(t_i; \boldsymbol{t}_{-\boldsymbol{i}}, R_{l_i}) \geq u_i(t_i^{SE}; \boldsymbol{t}_{-\boldsymbol{i}}^{SE}, R_{l_i}^{SE}), \forall i \in \mathcal{I}$

to be true, the following equation must be true:

$$2\lambda_1 \log(1+\frac{R_{l_1}^{SE}-2\Delta}{4}-\Delta')+2\lambda_3 \log(1+\frac{R_{l_3}^{SE}+2\Delta}{4}-\Delta') > 2\lambda_1 \log(1+\frac{R_{l_1}^{SE}}{4})+2\lambda_3 \log(1+\frac{R_{l_3}^{SE}}{4}), \tag{5.51}$$

$$\lambda_1 \log(1+\frac{R_{l_1}^{SE}-2\Delta}{4}-\Delta')+\lambda_3 \log(1+\frac{R_{l_3}^{SE}+2\Delta}{4}-\Delta') > \lambda_1 \log(1+\frac{R_{l_1}^{SE}}{4})+\lambda_3 \log(1+\frac{R_{l_3}^{SE}}{4}), \tag{5.52}$$

$$\lambda_3 \log\Big(\frac{4+R_{l_3}^{SE}+2\Delta-4\Delta'}{4+R_{l_3}^{SE}}) > \lambda_1 \log(\frac{4+R_{l_1}^{SE}}{4+R_{l_1}^{SE}-2\Delta-4\Delta'}\Big), \tag{5.53}$$

$$\Big(\frac{4+R_{l_3}^{SE}+2\Delta-4\Delta'}{4+R_{l_3}^{SE}}\Big)^{\lambda_3} > \Big(\frac{4+R_{l_1}^{SE}}{4+R_{l_1}^{SE}-2\Delta-4\Delta'}\Big)^{\lambda_1}. \tag{5.54}$$

Next, we try to obtain an expression for Δ to be satisfied if $u_i(t_i;\boldsymbol{t}_{-\boldsymbol{i}},R_{l_i}) = u_i(t_i^{SE};\boldsymbol{t}_{-\boldsymbol{i}}^{SE},R_{l_i}^{SE})$, for all $i \in \mathcal{I}$. From (5.54),

$$\frac{4+R_{l_3}^{SE}+2\Delta-4\Delta'}{4+R_{l_3}^{SE}} > \Big(\frac{4+R_{l_1}^{SE}}{4+R_{l_1}^{SE}-2\Delta-4\Delta'}\Big)^{\frac{\lambda_1}{\lambda_3}}, \tag{5.55}$$

$$\Delta > \frac{1}{2}\left[(4+R_{l_3}^{SE})(\frac{4+R_{l_1}^{SE}}{4+R_{l_1}^{SE}-2\Delta-4\Delta'})^{\frac{\lambda_1}{\lambda_3}}-4-R_{l_3}^{SE}+4\Delta'\right]. \tag{5.56}$$

□

Therefore, Claim 5.2 shows a scenario where the proposed Stackelberg incentive may not be Pareto-efficient for the crowdsourcer.

Chapter 6

Summary and Future Work

In this thesis, we addressed three specific security and privacy topics related to wireless networking and mobile crowd sensing:

Topic 1. How to effectively detect location spoofing attacks in TOA-based localization systems?

Topic 2. How to effectively mitigate wireless traffic analysis attacks against a powerful global observer?

Topic 3. How to effectively incentivize mobile smartphone user participation while preserving their location privacy?

The three topics were addressed in Chapters 2–5 where we explored a number of solutions and compared them against current works to demonstrate the effectiveness of the proposed solutions. A summary of contributions for my research work is listed as follows.

6.1 Summary

In Chapter 2, we studied the *location spoofing detection* problem in a wireless network where the network sink receives some TOA delay measurements from a target node and uses a detection test to check if the received measurements were spoofed. We proposed a new audibility-based framework for detecting location spoofing attacks in TOA-based localization systems. Next, we showed an example of how the conventional TOA-based detection methods

may not be able to detect location spoofing attacks, especially during inaudible scenarios. We then developed an detection test called Enhanced Location Spoofing Detection Using Audibility (ELSA) to mitigate the audibility problem. The proposed ELSA uses an audibility-aware GLRT to exploit the implicitly available audibility information and improve its detection rate. In addition, we proved that the proposed ELSA has a better detection performance compared to the conventional non-audibility-aware GLRT and evaluated the performance improvements using both synthetic data and a real-world sensor dataset. ELSA accommodates usage of low-cost IoT devices and lessens the need to deploy a dense network of anchors. It is also compatible with existing infrastructure-based TOA ranging schemes and does not require additional cryptographic operations or message exchanges between the anchors and the target node.

In Chapter 3, we studied the *privacy-preserving routing* problem in a wireless network where a Bayesian MAP adversary is able to observe all the transmission activities in the entire network. We focus on hiding the *source-destination identities* of each communication where we consider a global adversary that is able to observe node transmissions from the entire network. We designed a statistical decision-making framework to optimally solve the privacy-preserving routing problem in wireless networks given some utility constraints. We then designed the Optimal Privacy Enhancing Routing Algorithm (OPERA), which uses linear programs to compute the optimal routing path distribution that minimizes the adversary's detection probability under the lossy and lossless adversarial observation models. We showed via simulations that our approach is significantly better than the Uniform and Greedy heuristics, the baseline sink simulation and backbone flooding schemes, and the mutual information minimization scheme. Under the lossless observations adversary model, the formulated linear program can be decomposed into smaller subproblems for each source node to solve in a distributed fashion. This allows the optimal solution to be computed in a distributed manner or in parallel for efficiency.

In Chapter 4, we studied the *routing with privacy guarantees* problem in a wireless network where a Bayesian MAP adversary is able to observe all the transmission activities in the entire

network. To provide strict privacy guarantees for the communicating source-destination pair, we introduced the (k,ϵ)-anonymity property and designed a statistical decision-making framework that considers the full and partial information adversaries. We then formulated a mixed-integer linear programing problem to select the minimum-cost (k,ϵ)-anonymous paths. Next, we compared our solution against the baseline OPERA scheme that minimizes the average detection probability of the adversary. Our simulation results showed that the proposed scheme provides significantly larger anonymity set sizes, while achieving comparable average detection probability. We also studied how the adversary's prior beliefs affect its detection probability and Bayes risk, and showed that an adversary with only partial information will always use a uniform prior to minimize its Bayes risk.

In Chapter 5, we studied the *privacy-aware incentive* problem for mobile crowd sensing applications and proposed a privacy-aware Stackelberg incentive model that improves the *spatial coverage* of the collected dataset. Our proposed incentive model is privacy-aware, in that it allows privacy-sensitive mobile smartphone users to submit *coarse-grained (or quantized) location* information, which could still be useful to the crowdsourcer. We studied the properties of the proposed incentive model analytically and presented efficient algorithmic solutions. We also proved the incentive-compatibility property of our proposed incentive model and extended the basic model to accommodate bounds on the users' data contributions. In addition, we studied the sufficient conditions for achieving Pareto efficiency. Our proposed incentive model does not require a trusted third party for privacy and can protect users against a crowdsourcer who cannot be trusted to anonymize the smartphone users' location information. We showed via simulations that our proposed incentive model is superior than two other coverage-maximizing incentive schemes that maximize a different coverage metric.

Finally, we list the possible future work of the topics explored.

6.2 Future Work

There are still many interesting research questions that remained unanswered in the thesis. We now discuss the possible research directions.

In Chapter 2, we studied the *location spoofing detection* problem in a wireless network where the network uses a detection test to check for spoofed TOA delay measurements. Our proposed ELSA detection test does not specifically considers non-line-of-sight (NLOS) conditions or an adversarial target node that uses directional antennas. A possible future research direction will be to extend our general TOA and RSS-based statistical models to include deployment-specific conditions for the TOA or RSS measurements. This can help improve the existing detection performance, although the amount of improvement may be incremental. For example, a more complex TOA model [142] may be used to model NLOS conditions in the TOA values and a more complex RSS model may be used to model the Rician [14] or Rayleigh [143] fading conditions in the RSS values. It would also be interesting to design a detection test that accounts for an adversarial target node that is able to manipulate the RSS measurements using directional antennas in contrast to the assumed omnidirectional antennas in our system model.

In Chapter 3, we studied the *privacy-preserving routing* problem in a wireless network where a powerful Bayesian MAP adversary is able to observe all the transmission activities in the entire network. We focus on protecting the *source-destination identities* of each communication in a static wireless network. For future work, it would be interesting to study the privacy-utility trade-off problem for mobile networks. To extend our proposed OPERA for mobility scenarios, a source routing protocol similar to the well-studied dynamic source routing (DSR) routing protocol, e.g., [144, 145] may be used when the nodes' mobility are limited and the mobility patterns are known. The expected amount of transmission overhead may be computed when the mobility patterns are known, but the computational complexity of the optimal solution can be very costly when there is high mobility among the nodes. Also, the use of a dynamic source routing-based protocol introduces a large communication overhead as the protocol

needs to map the routing information to all other nodes via a route discovery phase, which is basically flooding-based although it uses heuristics to avoid sending duplicate packets.

In Chapter 4, we studied the *routing with privacy guarantees* problem in a wireless network where a Bayesian MAP adversary is able to perfectly observe all the transmission activities in the entire network. We introduced the (k,ϵ)-anonymity property for strict privacy guarantees and formulated a mixed-integer linear program to compute the minimum-cost path distribution that achieves the (k,ϵ)-anonymity property. However, it may not be practical to solve the formulated mixed-integer linear programs for large scale networks consisting of thousands of nodes. Hence, it would be interesting to study distributed solutions for our (k,ϵ)-anonymous routing problem. The challenge in designing a distributed solution is to allow sequential computation of the optimal solution without requiring knowledge of the entire network graph at each step. It would be ideal if a dynamic programming formulation [146] can be formulated to compute the optimal path distribution.

In Chapter 5, we studied the *privacy-aware incentive* problem for mobile crowd sensing applications and proposed a privacy-aware Stackelberg incentive model that improves the spatial coverage of the collected dataset. As our proposed Stackelberg model considers a static game setting, it would be interesting to extend our Stackelberg model for dynamic games played over a period of time where the smartphone users are allowed to move between regions. A new definition of privacy would be needed to account for user mobility as the currently used cloaking region method may not be enough for spatial-temporal settings. While our Stackelberg equilibrium is stable in the studied static game model played by the crowdsourcer and the mobile smartphone users in one time period, a different notation of equilibrium needs to be considered for the dynamic setting. Also, the existing incentive-compatibility property may not hold for the mobility model.

Bibliography

[1] R. Hasan, R. Khan, S. Zawoad, and M. Haque, "WORAL: A witness oriented secure location provenance framework for mobile devices," *IEEE Trans. Emerging Topics in Comput.*, vol. 4, no. 1, pp. 128–141, Jan. 2016.

[2] M. Aime, G. Calandriello, and A. Lioy, "Dependability in wireless networks: Can we rely on WiFi?" *IEEE Security & Privacy*, vol. 5, no. 1, pp. 23–29, Jan. 2007.

[3] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel and Distr. Syst.*, vol. 24, no. 5, pp. 938–950, May 2013.

[4] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 275–285, Jan. 2012.

[5] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security games for node localization through verifiable multilateration," *IEEE Trans. Dependable and Secure Comput.*, vol. 11, no. 1, pp. 72–85, Jan. 2014.

[6] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 497–510, Jun. 2008.

[7] H.-Y. Lin, S.-C. Chen, D.-B. Lin, and H.-P. Lin, "Multidimensional scaling algorithm for mobile location based on hybrid SADOA/TOA measurement," in *Proc. IEEE Wireless Commun. and Netw. (WCNC)*, Mar. 2008, pp. 3015–3020.

[8] B. Radunovic, C. Gkantsidis, P. Key, and P. Rodriguez, "Toward practical opportunistic routing with intra-session network coding for mesh networks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 2, pp. 420–433, Apr. 2010.

[9] J. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[10] W. Trappe, R. Howard, and R. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.

[11] P. Yang, "PRLS-INVES: A general experimental investigation strategy for high accuracy and precision in passive RFID location systems," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 159–167, Apr. 2015.

[12] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Veh. Technol.*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.

[13] F. Malandrino, C. Borgiattino, C. Casetti, C.-F. Chiasserini, M. Fiore, and R. Sadao, "Verification and inference of positions in vehicular networks through anonymous beaconing," *IEEE Trans. Mobile Comput.*, vol. 13, no. 10, pp. 2415–2428, Oct. 2014.

[14] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Location verification systems for VANETs in rician fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5652–5664, Jul. 2016.

[15] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 37–46, Sep. 2013.

[16] D. Huang, "Unlinkability measure for IEEE 802.11 Based MANETs," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 1025–1034, Mar. 2008.

[17] S. Misra, G. Xue, and S. Bhardwaj, "Secure and robust localization in a wireless ad hoc environment," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1480–1489, Mar. 2009.

[18] M. Fiore, C. Ettore Casetti, C. Chiasserini, and P. Papadimitratos, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 289–303, Feb. 2013.

[19] T. Brown, "Security in SCADA systems: how to handle the growing menace to process automation," *Comput. Control Engineering Journal*, vol. 16, no. 3, pp. 42–47, Jun. 2005.

[20] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2013, pp. 2778–2786.

[21] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2007, pp. 1955–1963.

[22] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 2994–3002.

[23] S. Yan, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *Proc. IEEE Conf. Global Commun. (GLOBECOM)*, Dec. 2012, pp. 5415–5420.

[24] N. Patwari, J. N. Ash, S. Kyperountas, A. O. H. III, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 54–69, Jul. 2005.

[25] S. Capkun, K. Bonne Rasmussen, M. Cagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.

[26] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst., Man, Cybern., Syst. , Part C: Applications and Reviews*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[27] I. Guvenc and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 3, pp. 107–124, Aug. 2009.

[28] "IEEE Standard for IEEE Amendment to Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN): Amendment to MAC Sublayer," *IEEE Std 802.15.3b-2005 (Amendment to IEEE Std 802.15.3-2003)*, 2006.

[29] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.

[30] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 96–101, Apr. 2008.

[31] J. Chiang, J. Haas, J. Choi, and Y.-C. Hu, "Secure location verification using simultaneous multilateration," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 584–591, Feb. 2012.

[32] J. Neyman and E. S. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, vol. 231, pp. 289–337, 1933.

[33] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Win, "Ranging with ultrawide bandwidth signals in multipath environments," *Proc. IEEE*, vol. 97, no. 2, pp. 404–426, Feb. 2009.

[34] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proc. ACM Mobile Comput. and Netw. (MobiCom)*, Sep. 2003, pp. 81–95.

[35] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proc. Conf. Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*, Sep. 2005, pp. 113–126.

[36] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2008.

[37] J. Y. Koh, J. Teo, D. Leong, and W.-C. Wong, "Reliable privacy-preserving communications for wireless ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 6271–6276.

[38] P. Zhang, C. Lin, Y. Jiang, P. Lee, and J. Lui, "ANOC: Anonymous network-coding-based communication with efficient cooperation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1738–1745, Oct. 2012.

[39] H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs," *IEEE Trans. Mobile Comput.*, vol. 12, no. 6, pp. 1079–1093, Jun. 2013.

[40] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, Jan. 2013.

[41] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell-counting-based attack against tor," *IEEE/ACM Trans. Networking*, vol. 20, no. 4, pp. 1245–1261, Aug. 2012.

[42] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. IEEE Int. Conf. Network Protocols (ICNP)*, Oct. 2007, pp. 314–323.

[43] ——, "Protecting location privacy in sensor networks against a global eavesdropper," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 320–336, Feb. 2012.

[44] Z. Wan, K. Xing, and Y. Liu, "Priv-Code: Preserving privacy against traffic analysis through network coding for multihop wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Mar. 2012, pp. 73–81.

[45] U. Acharya and M. Younis, "Increasing base-station anonymity in wireless sensor networks," *Elsevier Ad Hoc Networks*, vol. 8, no. 8, pp. 791–809, Nov. 2010.

[46] X. Gong and N. Kiyavash, "Quantifying the information leakage in timing side channels in deterministic work-conserving schedulers," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1841–1852, Jun. 2016.

[47] C. Troncoso and G. Danezis, "The bayesian traffic analysis of mix networks," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*. ACM, 2009, pp. 369–379.

[48] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[49] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 482–494, May 1998.

[50] S. Mathur and W. Trappe, "BIT-TRAPS: building information-theoretic traffic privacy into packet streams," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 752–762, Sep. 2011.

[51] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proc. ACM Workshop on Security of Ad Hoc and Sensor Netw.*, 2004, pp. 88–93.

[52] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3769–3779, Oct. 2008.

[53] A. Diyanat, A. Khonsari, and S. P. Shariatpanahi, "A dummy-based approach for preserving source rate privacy," *IEEE Trans. Inf. Forens. Security*, vol. 11, no. 6, pp. 1321–1332, Jun. 2016.

[54] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," (v0.34). tech. rep., TU Dresden and ULD Kiel, Aug. 2010.

[55] B. Guo, Z. Wang, Z. Yu, Y. Wang, N. Y. Yen, R. Huang, and X. Zhou, "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 7–31, Aug. 2015.

[56] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, "Vtrack: Accurate, energy-aware road traffic delay estimation using mobile phones," in *Proc. ACM Conf. Embedded Networked Sensor Syst. (SenSys)*, 2009, pp. 85–98.

[57] S. E. Minson, B. A. Brooks, C. L. Glennie, J. R. Murray, J. O. Langbein, S. E. Owen, T. H. Heaton, R. A. Iannucci, and D. L. Hauser, "Crowdsourced earthquake early warning," *Science Advances*, vol. 1, no. 3, Apr. 2015.

[58] R. K. Rana, C. T. Chou, S. S. Kanhere, N. Bulusu, and W. Hu, "Ear-phone: An end-to-end participatory urban noise mapping system," in *Proc. ACM/IEEE Conf. Inf. Process. in Sensor Netw. (IPSN)*, 2010, pp. 105–116.

[59] K. Nissim, C. Orlandi, and R. Smorodinsky, "Privacy-aware mechanism design," in *Proc. ACM Conf. Electronic Commerce (EC)*, 2012, pp. 774–789.

[60] A. Singla and A. Krause, "Truthful incentives for privacy tradeoff: Mechanisms for data gathering in community sensing," in *Proc. Int. Conf. Machine Learning (ICML)*, Jun. 2013.

[61] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. ACM Mobile Comput. and Netw. (MobiCom)*, 2012, pp. 173–184.

[62] L. Duan, T. Kubo, K. Sugiyama, J. Huang, T. Hasegawa, and J. Walrand, "Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2012, pp. 1701–1709.

[63] S. Luo, Y. Sun, Y. Ji, and D. Zhao, "Stackelberg game based incentive mechanisms for multiple collaborative tasks in mobile crowdsourcing," *Mobile Networks and Applications*, vol. 21, no. 3, pp. 506–522, 2016.

[64] Z. Feng, Y. Zhu, Q. Zhang, L. M. Ni, and A. V. Vasilakos, "TRAC: truthful auction for location-aware collaborative sensing in mobile crowdsourcing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2014, pp. 1231–1239.

[65] J. Y. Koh, D. Leong, G. W. Peters, I. Nevat, and W.-C. Wong, "Optimal privacy-preserving probabilistic routing for wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. PP, no. 99, pp. 1–14, 2017.

[66] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, pp. 829–835, Apr. 2006.

[67] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Timing information in wireless communications and optimal location verification frameworks," in *Proc. Australian Commun. Theory Workshop (AusCTW)*, Feb. 2014, pp. 144–149.

[68] D. B. Rubin, "Inference and missing data," *Biometrika*, vol. 63, no. 3, pp. 581–592, 1976.

[69] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. Dependable and Secure Comput.*, vol. 3, no. 4, pp. 377–385, Oct. 2006.

[70] L. Taponecco, P. Perazzo, A. D'Amico, and G. Dini, "On the feasibility of overshadow enlargement attack on IEEE 802.15.4a distance bounding," *IEEE Commun. Letters*, vol. 18, no. 2, pp. 257–260, Feb. 2014.

[71] S. Capkun, M. Cagalj, G. Karame, and N. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 11, pp. 1608–1621, Nov. 2010.

[72] O. H. Abdelrahman and E. Gelenbe, "Signalling storms in 3G mobile networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2014, pp. 1017–1022.

[73] M. Pavloski and E. Gelenbe, "Mitigating for signalling attacks in UMTS networks," in *Proc. Int. Symp. Computer and Information Sciences*, Oct. 2014, pp. 159–165.

[74] P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," *Comput. Netw.*, vol. 53, no. 15, pp. 2601–2616, Oct. 2009.

[75] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2001.

[76] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs): Amendment 1: Add Alternate PHYs," *IEEE Std. 802.15.4a-2007*, 2007.

[77] S. Lanzisera, D. Zats, and K. Pister, "Radio frequency time-of-flight distance measurement for low-cost wireless sensor localization," *IEEE Sensors Journal*, vol. 11, no. 3, pp. 837–845, Mar. 2011.

[78] N. Patwari, A. Hero, M. Perkins, N. Correal, and R. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2137–2148, Aug. 2003.

[79] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "The cicada attack: Degradation and denial of service in IR ranging," in *Proc. IEEE Conf. Ultra-Wideband (ICUWB)*, Sep. 2010.

[80] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ: Prentice-Hall, Inc., 1993.

[81] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. Cambridge, MA: MIT Press, 2012.

[82] N. Patwari, A. Hero, M. Perkins, N. Correal, and R. O'Dea, *Wireless Sensor Network Localization Measurement Repository*, 2006 (accessed June 1, 2017). [Online]. Available: http://web.eecs.umich.edu/~hero/localize/

[83] *MATLAB code for our simulation results*, 2015 (accessed June 1, 2017). [Online]. Available: http://idonevat.wix.com/idonevat#!about2/c1hlk

[84] DecaWave, *ScenSor DW1000 - DecaWave's Precise Indoor Location and Communication Chip*, 2015 (accessed June 1, 2017). [Online]. Available: http://www.decawave.com/products/overview

[85] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. ACM Mobile Comput. and Netw. (MobiCom)*, Sep. 2007, pp. 111–122.

[86] J. Y. Koh, J. Teo, D. Leong, and W.-C. Wong, "Reliable privacy-preserving communications for wireless ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015.

[87] R. Rios, J. Cuellar, and J. Lopez, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Elsevier Inf. Sciences*, vol. 321, pp. 205–223, Nov. 2015.

[88] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective probabilistic approach protecting sensor traffic," in *Proc. IEEE Military Comm. Conf. (MILCOM)*, Oct. 2005, pp. 169–175.

[89] T. He and L. Tong, "Detection of information flows," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 4925–4945, Nov. 2008.

[90] N. Shah and D. Huang, "A-WEOR: communication privacy protection for wireless mesh networks using encoded opportunistic routing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Mar. 2010.

[91] J. Yao and G. Wen, "Preserving source-location privacy in energy-constrained wireless sensor networks," in *Proc. Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 412–416.

[92] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Trans. Parallel and Distr. Syst.*, vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[93] Y. Guan, X. Fu, R. Bettati, and W. Zhao, "An optimal strategy for anonymous communication protocols," in *Proc. Int. Conf. Distrib. Comput. Syst.*, 2002, pp. 257–266.

[94] K. G. Murty, *Linear Programming*. Hoboken, NJ: Wiley, 1983.

[95] B. A. Chambers, "The grid roofnet: a rooftop ad hoc wireless network," Master's thesis, M.S. thesis, EECS, MIT, Cambridge, MA, 2002.

[96] M. Doddavenkatappa, M. Chan, and A. Ananda, "Indriya: A low-cost, 3D wireless sensor network testbed," in *Proc. Int. Conf. Testbeds and Research Infrastructures for the Development of Networks & Communities*, 2011.

[97] Y. Zhu and R. Bettati, "Anonymity vs. information leakage in anonymity systems," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2005, pp. 514–524.

[98] H. Chen and P. Malacaria, "Quantifying maximal loss of anonymity in protocols," in *Proc. Int. Symp. Inf. Comput. and Commun. Security (ASIACCS)*, 2009, pp. 206–217.

[99] S. Zhioua, "A geometric view of mutual information: Application to anonymity protocols," in *Proc. Inf. Theory and its Applications (ISITA)*, Oct. 2010, pp. 60–65.

[100] L. Sankar, S. Rajagopalan, and H. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[101] K. Chatzikokolakis, T. Chothia, and A. Guha, "Statistical measurement of information leakage," in *Proc. Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2010, pp. 390–404.

[102] A. R. Coble, "Anonymity, information, and machine-assisted proof," University of Cambridge, Cambridge, UK, Rep. UCAM-CL-TR-785, Tech. Rep., 2010.

[103] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Privacy aware learning," *J. ACM*, vol. 61, no. 6, pp. 1–57, Dec. 2014.

[104] J. Y. Koh, G. W. Peters, I. Nevat, D. Leong, and W.-C.Wong, "Probabilistic routing in wireless networks with privacy guarantees," *submitted to the IEEE Trans. Signal Process.*, pp. 1–11, 2017.

[105] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2005, pp. 599–608.

[106] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Mar. 2010, pp. 1–9.

[107] X. Luo, X. Ji, and M. S. Park, "Location privacy against traffic analysis attacks in wireless sensor networks," in *Proc. Int. Conf. Information Science and Applications*, Apr. 2010.

[108] S. Kadloor, X. Gong, N. Kiyavash, and P. Venkitasubramaniam, "Designing router scheduling policies: A privacy perspective," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 2001–2012, Apr. 2012.

[109] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE Int. Conf. Data Engineering (ICDE)*, Apr. 2007, pp. 106–115.

[110] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[111] C. Dwork, "Differential privacy," in *Proc. Int. Colloquium Automata, Languages and Programming (ICALP)*, 2006.

[112] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, Mar. 2007.

[113] G. Chai, M. Xu, W. Xu, and Z. Lin, "Enhancing sink-location privacy in wireless sensor networks through k-anonymity," *Int. Journal Distr. Sensors Netw.*, vol. 8, no. 4, pp. 1–16, Apr. 2012.

[114] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proc. IEEE Int. Symp. Parallel Distrib. Process.*, Apr. 2006.

[115] J. Deng, R. Han, and S. Mishra, "Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks," *Pervasive Mobile Comput.*, vol. 2, no. 2, pp. 159–186, Apr. 2006.

[116] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358, Sep. 2011.

[117] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE J. Sel. Areas Commun*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[118] J. Aldrich, "How likelihood and identification went Bayesian," *International Statistical Review*, vol. 70, no. 1, pp. 1–12, Apr. 2002.

[119] E. Lehmann and G. Casella, *Convergence in Probability and in Law*. New York, NY: Springer-Verlag, 1998.

[120] J. Berger, "The case for objective Bayesian analysis," *Bayes. Anal.*, vol. 1, no. 3, pp. 385–402, 2006.

[121] J. P. Vielma, "Mixed integer linear programming formulation techniques," *SIAM Review*, vol. 57, no. 1, pp. 3–57, Feb. 2015.

[122] L. Wolsey, "Integer programming," *IIE Transactions*, vol. 32, no. 3, pp. 273–285, 2000.

[123] J. Bernardo and A. Smith, *Conjugate analysis*. Hoboken, NJ: Wiley, 1994.

[124] K. Bury, *Introduction to Continuous Distributions*, 1st ed. New York, NY: Cambridge University Press, 1999.

[125] MATLAB, *MathWorks Optimization Toolbox version 7.4 (R2016a)*. The MathWorks Inc., 2016.

[126] J. Y. Koh, G. W. Peters, D. Leong, I. Nevat, and W.-C. Wong, "Privacy-aware incentive mechanism for mobile crowd sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017.

[127] J. Y. Koh, G. W. Peters, D. Leong, I. Nevat, and W.-C.Wong, "Spatial stackelberg incentive mechanisms for privacy-aware mobile crowd sensing," *in preparation*.

[128] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. Int. Conf. Pervasive Services.*, Jul. 2005, pp. 88–97.

[129] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructures," in *Proc. Int. Workshop on Privacy Enhancing Technologies (PET)*, Jun. 2006, pp. 393–412.

[130] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2013, pp. 901–914.

[131] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symp. Usable Privacy and Security (SOUPS)*, Jul. 2014.

[132] L. G. Jaimes, I. Vergara-Laurens, and M. A. Labrador, "A location-based incentive mechanism for participatory sensing systems with budget constraints," in *Proc. IEEE Int. Conf. Pervasive Comput. and Commun.*, Mar. 2012, pp. 103–108.

[133] H. Xiong, D. Zhang, G. Chen, L. Wang, V. Gauthier, and L. E. Barnes, "iCrowd: Near-optimal task allocation for piggyback crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 2010–2022, Aug. 2016.

[134] H. Xiong, D. Zhang, G. Chen, L. Wang, and V. Gauthier, "Crowdtasker: Maximizing coverage quality in piggyback crowdsensing under budget constraint," in *Proc. IEEE Conf. Pervasive Comput. and Commun. (PerCom)*, Mar. 2015, pp. 55–62.

[135] D. Zhang, H. Xiong, L. Wang, and G. Chen, "Crowdrecruiter: Selecting participants for piggyback crowdsensing under probabilistic coverage constraint," in *Proc. ACM Conf. Pervasive and Ubiquitous Comput. (UbiComp)*, 2014, pp. 703–714.

[136] P. Y. Chen, S. M. Cheng, P. S. Ting, C. W. Lien, and F. J. Chu, "When crowdsourcing meets mobile sensing: a social network perspective," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 157–163, Oct. 2015.

[137] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda, "PEIR, the personal environmental impact report, as a platform for participatory sensing systems research," in *Proc. ACM Mobile Syst., Applications, and Services (MobiSys)*, 2009, pp. 55–68.

[138] S. Madden, *Intel Lab Data*, 2004 (accessed June 1, 2017). [Online]. Available: http://db.csail.mit.edu/labdata/labdata.html

[139] C. E. Rasmussen and C. K. I. Williams, *Gaussian Processes for Machine Learning (Adaptive Computation and Machine Learning)*. Cambridge, MA: MIT Press, 2005.

[140] A. Mchutchon and C. E. Rasmussen, "Gaussian process training with input noise," in *Proc. Advances in Neural Information Processing Systems (NIPS)*, 2011, pp. 1341–1349.

[141] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.

[142] K. Yu and Y. J. Guo, "Statistical NLOS Identification Based on AOA, TOA, and Signal Strength," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 274–286, Jan. 2009.

[143] C.-H. Liu and J. Andrews, "Multicast outage probability and transmission capacity of multihop wireless networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4344–4358, Jul. 2011.

[144] Z. W. Wang, M. G. Liang, and J. X. Zhang, "Vector switching scheme (VSS) for source routing protocol of MANET," in *Proc. IET Conf. Wireless, Mobile and Multimedia Networks (ICWMMN)*, Oct. 2008, pp. 58–61.

[145] S. Rehman, G. Heo, and W. C. Song, "Associativity-based dynamic source routing in manets," in *Proc. Int. Conf. Inf. Netw.*, Jan. 2009.

[146] B. Richard, *Dynamic Programming*. Princeton, NJ: Princeton University Press, 2003.