PRESERVING ACCURACY AND PRIVACY IN PARTICIPATORY SENSING SYSTEMS

by

MOHANNAD ALI ALSWAILIM

A thesis submitted to the School of Computing in conformity with the requirements for the degree of Doctor of Philosophy

Queen's University
Kingston, Ontario, Canada
September 2018

Copyright © Mohannad Ali Alswailim, 2018
Dedication

To my father, Ali;

my mother, Norah;

my wife, Marwa and

my children, Abdullah and Norah
Abstract

Participatory Sensing (PS) is an approach that offers individuals and interest groups the opportunity to contribute to an application using their handheld sensor devices such as smartphones and tablets. These sensor devices are able to sense, collect available data and use cellular and Internet communication infrastructure such as LTE and WiFi to transmit the data to the application server. The application server processes the collected data and makes the data available to the end-users. Participant contributions consist of sensor data, location, date and time. In addition, PS applications usually need to collect additional data about participants such as identity, age, gender and contact.

Notwithstanding the numerous benefits the PS approach brought to the application domain, there are two main challenges that threaten the success of PS: data trustworthiness and participant privacy. The additional data collected from participants’ devices are essential to verify the credibility of participants and the accuracy of their contributions. Moreover, these additional participant data are considered private. Thus, ensuring data trustworthiness and accuracy sacrifices the participant privacy, and vice versa.

In this thesis, we propose a framework for PS that involves three major schemes to overcome the challenges of accuracy-privacy trade-off. The framework ensures participant contribution data trustworthiness in PS applications, verifies the accuracy of participant contributions in critical situations, and protects participant privacy in critical situations.
PS applications are usually open to the public, and receive sensor data from multiple participants. This openness feature of PS applications allows inaccurate and corrupted contributions to affect the quality of the application services negatively. A way of ensuring contribution validity is by evaluating participant reputation values through a designed reputation system. Therefore, we propose a Reputation System to Evaluate Participants (RSEP) to ensure participant contribution data trustworthiness and provide accurate participant contributions.

When a crisis occurs, immediate response by rescue personnel is crucial. Decisions for a rescue plan are based solely on data about the crisis from the location. Receiving data from the public could potentially result in corrupted and inaccurate data that will negatively impact the rescue plans. Therefore, we propose a Participant Contribution Trust scheme (PCT) that allows the PS application to verify the accuracy of contributions before sending the data to the crisis response system that requires all available data in order to reach its optimal performance.

In critical situations when a crisis occurs, the accuracy-privacy trade-off becomes more complex. Adding more weight to one side needing accurate data, over the other, risking breach of privacy, may become essential due to the specific situation. When a participant is at risk, data accuracy becomes more important than participant privacy. Thus, we propose a Context-Aware Privacy scheme (CAP) that balances the privacy-accuracy trade-off. The CAP scheme eventually provides privacy-preserved data to authorized recipients based on the status of the participants. Depending on the recipient category, their role and policies enforced, a different level of participants’ private data may be received.
Co-Authorship


Acknowledgments

All praise be to Allah, the creator and sustainer of this universe, for blessing me with guidance, strength and patience to complete this work.

I would like to express my sincere thanks to my supervisors and mentors, Prof. Hossam S. Hassanein and Prof. Mohammad Zulkernine. The freedom they gave me as a graduate student to take ownership of my own research interest along with the valuable guidance, support, and motivation was vital to achieving this degree. I would also like to thank Prof. Bob Crawford and Prof. Patrick Martin for serving as supervisory committee members and for their valuable feedback.

To Telecommunication Research Lab (TRL) and Queen’s Reliable Software Technology (QRST) members, it has been a pleasure to work with many of you. Special thanks to Dr. Sharief Oteafy, Dr. Hesham Farahat, Mohannad Alharthi, Abdulrahman Abahsain and Dr. Mahmoud Qutqut for their academic help and support throughout the past years. I would also like to thank Mrs. Basia Palmer for her hard work and continues help.

All of my achievements are owed to my family’s sacrifices, and so is my deepest and greatest gratitude. My parents, for their genuine and unconditional support and sacrifices. My wife, my partner in life, has been an invaluable source of much-needed support and encouragement; my children continue to be the truest joy in my world. My brothers, Suliman, Mohammad, Faisal and Naif; my sisters, Sahar, Shahla, Shahd, Lamees, Lamar and Rasha have consistently stood behind
me and boosted my moral throughout the course of this journey. I am sincerely grateful and indebted to each one of you as I could not have gotten where I am today without you all.

To my lifetime friends Abdulaziz and Suliman Alhussan, Saad Alamer, Abdullah Alorini, Dr. Saad and Bader Alaboodi, Dr. Zaid Alyami, Hesham Banasr, Alawi Assaggaf and Maher Alhalabi, thanks for always being there when I need you. I wish you the best of luck in your lives.

Finally, I am grateful to the Qassim University (QU) for granting me the graduate program scholarship to achieve this work. Special thanks to Dr. Mohammed Alodib, Dr. Ajlan Alajlan and Dr. Obaid Almotairy for their support in overcoming difficulties through my years in Canada.
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>Accurate Sensed data</td>
</tr>
<tr>
<td>ASD</td>
<td>Average Sensed Data</td>
</tr>
<tr>
<td>BMI</td>
<td>Body Mass Index</td>
</tr>
<tr>
<td>CAP</td>
<td>Context-Aware Privacy</td>
</tr>
<tr>
<td>CCHS</td>
<td>Canadian Community Health Survey</td>
</tr>
<tr>
<td>CRS</td>
<td>Crisis Response System</td>
</tr>
<tr>
<td>DP</td>
<td>Differential Privacy</td>
</tr>
<tr>
<td>DRCS</td>
<td>Double Recent Contribution Score</td>
</tr>
<tr>
<td>DRPC</td>
<td>Double Recent Positive Contribution</td>
</tr>
<tr>
<td>FN</td>
<td>False Negative</td>
</tr>
<tr>
<td>FP</td>
<td>False Positive</td>
</tr>
<tr>
<td>FS</td>
<td>Filtered Sensed data</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HGV</td>
<td>Highest Group Value</td>
</tr>
<tr>
<td>HPRV</td>
<td>High Participant Reputation Value</td>
</tr>
<tr>
<td>IC</td>
<td>Identification Confidence</td>
</tr>
<tr>
<td>IS</td>
<td>Inaccurate Sensed data</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>nc</td>
<td>newcomer participant</td>
</tr>
<tr>
<td>ns</td>
<td>negative score</td>
</tr>
<tr>
<td>PA</td>
<td>Participant Attribute</td>
</tr>
<tr>
<td>PCT</td>
<td>Participant Contribution Trust</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PL</td>
<td>Participant Location</td>
</tr>
<tr>
<td>PP</td>
<td>Privacy-Preserved</td>
</tr>
<tr>
<td>ps</td>
<td>positive score</td>
</tr>
<tr>
<td>PS</td>
<td>Participatory Sensing</td>
</tr>
<tr>
<td>PSP</td>
<td>Participatory Sensing Privacy</td>
</tr>
<tr>
<td>PSS</td>
<td>Participatory Sensing System</td>
</tr>
<tr>
<td>PST</td>
<td>Participatory Sensing Trust</td>
</tr>
<tr>
<td>RCQS</td>
<td>Reputation and Contribution Quality Scheme</td>
</tr>
<tr>
<td>RS</td>
<td>Reputation System</td>
</tr>
<tr>
<td>RSEP</td>
<td>Reputation Scheme to Evaluate Participants</td>
</tr>
<tr>
<td>rv</td>
<td>reputation value</td>
</tr>
<tr>
<td>TP</td>
<td>True Positive</td>
</tr>
<tr>
<td>TPS</td>
<td>Total Positive Score</td>
</tr>
<tr>
<td>WHO</td>
<td>World Health Organization</td>
</tr>
</tbody>
</table>
# List of Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>Participant groups index</td>
</tr>
<tr>
<td>$l$</td>
<td>Set of participant groups</td>
</tr>
<tr>
<td>$G_x$</td>
<td>Group $x$</td>
</tr>
<tr>
<td>$V_{G_x}$</td>
<td>Value of group $x$</td>
</tr>
<tr>
<td>$w$</td>
<td>Participant weight</td>
</tr>
<tr>
<td>$q$</td>
<td>Sensed data</td>
</tr>
<tr>
<td>$i$</td>
<td>Participants index</td>
</tr>
<tr>
<td>$m$</td>
<td>Set of participants</td>
</tr>
<tr>
<td>$P_i$</td>
<td>Participant $i$</td>
</tr>
<tr>
<td>$t$</td>
<td>Contributions index in Aging mode</td>
</tr>
<tr>
<td>$X$</td>
<td>Set of contributions in Aging mode</td>
</tr>
<tr>
<td>$Z$</td>
<td>Specified number of contributions in Aging mode</td>
</tr>
<tr>
<td>$gp$</td>
<td>A range percentage of grouping parameter</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Ground truth value</td>
</tr>
<tr>
<td>$\delta$</td>
<td>Error range of sensing data</td>
</tr>
<tr>
<td>$c$</td>
<td>Sets and subsets index</td>
</tr>
<tr>
<td>$Set_c$</td>
<td>A Set of participants</td>
</tr>
<tr>
<td>$o$</td>
<td>Participant contributions index in DRCS and DRPC</td>
</tr>
<tr>
<td>$v$</td>
<td>Specified number of contributions in DRCS and DRPC</td>
</tr>
<tr>
<td>$j$</td>
<td>Zones index</td>
</tr>
<tr>
<td>$n$</td>
<td>Set of zones</td>
</tr>
</tbody>
</table>

$x$
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_j$</td>
<td>Radius of zone $j$</td>
</tr>
<tr>
<td>$S_j$</td>
<td>Situation of zone $j$</td>
</tr>
<tr>
<td>$d$</td>
<td>Cardinal directions</td>
</tr>
<tr>
<td>$u$</td>
<td>A range percentage of sensed data acceptance</td>
</tr>
<tr>
<td>$k$</td>
<td>Recipient categories index</td>
</tr>
<tr>
<td>$h$</td>
<td>Set of recipient categories</td>
</tr>
<tr>
<td>$C_k$</td>
<td>Recipient category $k$</td>
</tr>
<tr>
<td>$A$</td>
<td>Participant attributes</td>
</tr>
<tr>
<td>$E$</td>
<td>Participant element of an attribute</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Specified attribute in an equation</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Participant occurrence in a sector</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>Situation degree of danger</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>Data position in Laplace mechanism</td>
</tr>
<tr>
<td>$\varepsilon$</td>
<td>Privacy level</td>
</tr>
<tr>
<td>$\Delta f$</td>
<td>Sensitivity level</td>
</tr>
<tr>
<td>$b$</td>
<td>Noise level</td>
</tr>
</tbody>
</table>
Content

Chapter 1 Introduction ................................................................................................. 1
  1.1 Motivation ............................................................................................................. 2
  1.2 Thesis Contributions ........................................................................................... 4
  1.3 Thesis Organization .............................................................................................. 6

Chapter 2 Background and Related Work ................................................................. 8
  2.1 Participatory Sensing Systems ............................................................................ 8
  2.2 Privacy, Security and Trust ................................................................................ 12
  2.3 Participatory Sensing Privacy ............................................................................ 12
  2.4 Participatory Sensing Trust .............................................................................. 14
  2.5 Crisis Response Systems ................................................................................... 16

Chapter 3 Framework Overview .............................................................................. 18
  3.1 The Framework .................................................................................................... 18
  3.2 Datasets ............................................................................................................. 20
  3.3 Evaluation Metrics .............................................................................................. 23

Chapter 4 A Reputation Scheme to Evaluate Participants for Participatory Sensing (RSEP) .................................................................................................................. 25
  4.1 Introduction ......................................................................................................... 25
  4.2 The RSEP Scheme ............................................................................................. 26
    4.2.1 The RSEP Overview ....................................................................................... 26
    4.2.2 The RSEP Algorithm .................................................................................... 28
    4.2.3 Reputation Value Computation Algorithm .................................................... 31
  4.3 Experimental evaluation ................................................................................... 32
    4.3.1 Evaluation Environment ............................................................................... 33
6.4.2 Dataset............................................................................................................................................. 86
6.4.3 Experiment Results .......................................................................................................................... 89
6.5 Discussion ........................................................................................................................................... 94
6.5.1 Predefine New Policies at The Context-Aware Scheme ................................................................. 95
6.5.2 Re-classifying Attribute Sensitivity Parameters ............................................................................. 98
6.5.3 Comparison of the four settings ..................................................................................................... 102
6.6 Summary ........................................................................................................................................... 104

Chapter 7 Conclusion .............................................................................................................................106
7.1 Summary and Concluding Remarks ............................................................................................... 106
7.2 Limitations and Assumptions ......................................................................................................... 110
7.3 Future Work ..................................................................................................................................... 111

Bibliography ...........................................................................................................................................114
List of Figures

Figure 2.1: Participatory sensing system architecture .............................................................. 9
Figure 2.2: Classification of participatory sensing applications ............................................... 10
Figure 2.3: Participatory sensing modes .................................................................................... 11
Figure 2.4: Participatory sensing privacy through a trusted third party ................................... 13
Figure 3.1: The framework architecture overview .................................................................. 21
Figure 4.1: The RSEP architecture .......................................................................................... 27
Figure 4.2: The FP and FN rates with three threshold settings for RSEP and RCQS .............. 38
Figure 4.3: Sample of a participant trajectory across multiple sectors and days ..................... 42
Figure 4.4: The FP and FN rates with three threshold settings for RSEP and DRPC .............. 44
Figure 4.5: The FP and FN rates with three threshold settings for RSEP and DRCS .............. 47
Figure 5.1: The PCT architecture ............................................................................................. 54
Figure 5.2: A crisis map after splitting the area into sectors in each direction ......................... 55
Figure 5.3: The FP and FN rates with three threshold settings for PCT and RSEP ................. 66
Figure 5.4: The Precision and Recall rates with three threshold settings for PCT and RSEP ... 68
Figure 5.5: Multiple maps for the same fire crisis moving toward the east direction .............. 70
Figure 5.6: Diverse heat levels between two crises in the same region .................................. 71
Figure 5.7: Two crises toward each other .................................................................................. 73
Figure 6.1: The CAP architecture ............................................................................................ 79
Figure 6.2: The CAP scheme use case........................................................................................................... 92
Figure 6.3: Data accuracy for three recipient categories based on participant situations......... 94
Figure 6.4: The use case relaxed CAP policy scheme .................................................................................. 95
Figure 6.5: Data accuracy of the original sensitivity parameter attributes on the relaxed policy
version......................................................................................................................................................... 97
Figure 6.6: Data accuracy of the re-classified sensitivity parameter attributes on the original
policy version................................................................................................................................................. 100
Figure 6.7: Data accuracy of the re-classified sensitivity parameter attributes on the relaxed
policy version................................................................................................................................................. 101
Figure 6.8: Data accuracy of all four settings in three participant situations ................................. 103
Figure 7.1: A detailed summary of the framework architecture......................................................... 108
List of Tables

Table 4.1: Sample of participant history repository................................................................. 40
Table 4.2: Sample of contribution history repository ................................................................. 41
Table 6.1: Sensitivity parameter attributes in the two release formats ..................................... 90
Table 6.2: Re-classified sensitivity parameter attributes in the two release formats .................. 99
Chapter 1

Introduction

Participatory Sensing (PS) is an approach that offers individuals and interest groups the opportunity to contribute to an application using their handheld sensor devices such as smartphones and tablets. These sensor devices are able to sense, collect data and use cellular and Internet communication infrastructure such as LTE and WiFi to transmit the data to the application server. The application server processes the collected data and makes them available to the end-users [1].

Smartphones are being gradually equipped with various embedded and/or peripheral sensors such as a camera, microphone, GPS, ambient light, proximity, accelerometer and temperature [2]. These sensors in PS enable a wide range of applications including those related to health, the community, local economy and the environment. These applications are just a few contexts in which PS can be performed by scalable and low-cost hand-held devices.

Similar PS approaches carry similar definitions, requirements and goals. Some researchers use the terms mobile sensing [3], opportunistic sensing [4], public sensing [5] and crowd sensing [4] interchangeably. However, others have differentiated between these terms based on the sensing
1.1 **Motivation**

mode that are at the level of user involvement in taking the sensing action, e.g., manual, automatic and opportunistic.

Crisis situations such as accidents, fires, earthquakes and floods, threaten people’s lives and must be dealt with in a timely manner. Thus, rescue personnel’s immediate response is crucial. In such situations, PS applications can play a major role in reaching optimal performance in setting rescue plans [6]. Participants who are within the close proximity to a crisis use their smartphones to sense the available data that is directly related to the crisis. A Crisis Response System (CRS) receives the collected data from participants in addition to the pre-existing data to make an efficient rescue plan.

Participant contributions consist of sensor data, location, date and time. PS applications usually need to collect extra data about participants such as identity, age, gender, contact, etc. The applications use the extra collected data to verify the credibility of participants and their contributions.

1.1 **Motivation**

A Participatory Sensing System (PSS) consists of participants, an application server and end-users. PS applications have become very popular in smartphone users’ daily life due to the convenient services PS provides to their users and communities. PS applications carry out four major tasks: sensing, sending, analyzing and sharing the results with the end users. In the first two tasks, participants sense their surrounding environment and send the sensor data in addition to their own data to the application server. The application server then analyzes the received data to visualize and share with the end-users.
1.1 Motivation

The two main challenges threaten the success of PSS are data trustworthiness [7, 8] and participant privacy [2, 9]. The data collected from participants’ devices including identity, location, time, age, gender and contact are essential to verify the credibility of participants and the accuracy of their contributions. However, these additional participant data are considered private [10].

On the one hand, an application server needs to verify that the collected data is correct and being sensed at the right location and time by an identified participant. On the other hand, safeguarding participant privacy needs to be guaranteed to make participants feel comfortable and willing to contribute safely.

Ensuring data trustworthiness requires more data about participants to ensure the accuracy of their contributions, which eventually sacrifices the participant privacy. In contrast, safeguarding participant privacy means less data to be provided to the application server, which will be a disadvantage for ensuring data trustworthiness. Therefore, the design of a successful PSS is met with overcoming the challenge of accuracy-privacy trade-off.

In more critical situations when a crisis occurs, the accuracy-privacy trade-off becomes more complex. Adding more weight to one side needing accurate data, over the other, risking breach of privacy, may become essential due to the specific situation. When a participant is at risk, data accuracy becomes more important than participant privacy. In this case, participant privacy should still be active to a level that does not prevent rescue personnel from carrying out the rescue plan. On the contrary, when a participant is in a safe position, privacy becomes a priority to a level that data accuracy is still valid and acceptable.
1.2 Thesis Contributions

Given these challenges and situations, this thesis aims to address the following research questions:

**R1.** How can we evaluate and validate participant contributions to ensure data trustworthiness in a PS application environment?

**R2.** How can we verify the accuracy of contributions in critical situations when a crisis occurs, where every piece of information is crucial?

**R3.** Is it possible to protect participant privacy in critical situations when a crisis occurs while keeping an acceptable level of providing accurate data to the application?

1.2 Thesis Contributions

The proposed research aims to answer the above research questions, as follows:

**R1.** PS applications are usually open to the public and receive sensor data from multiple participants. This openness feature allows inaccurate and corrupted contributions to affect the quality of the application services negatively. Therefore, validating the correctness of contributions is essential for PS applications. A way of evaluating contribution validity is by evaluating participant reputation values. To this end, we propose a Reputation Scheme to Evaluate Participants (RSEP). This will also validate their contributions.

RSEP computes each participant reputation value based on their previous contribution results to help validate their current contribution. At the end of each round, the system rates all contributions and assigns scores to each participant based on their contributions validity.
1.2 Thesis Contributions

R2. When a crisis occurs, immediate response by rescue personnel is crucial. Decisions for a rescue plan are based solely on data about the crisis from the location. Therefore, CRS, on the one hand, requires all available data to reach its optimal performance. On the other hand, the PS applications usually accept sensor data from the public which raises the challenge of participant contribution trust; what data is accurate? And what data is not? Therefore, the PS applications need to verify the accuracy of contributions before sending the data to the CRS. To this end, we propose a Participant Contribution Trust scheme (PCT).

PCT aims to provide trusted sensed data by filtering the inaccurate contributions out from the accurate contributions. PCT compares contributions from different locations at the crisis site to confirm the accuracy of the data collected. It also computes participant reputation values to be used in selecting data from highly reputed participants.

R3. Data collected from participants including location, date, time, contacts, etc. are significant to the CRS and considered private to the participants. Protecting participants’ privacy, on the one hand, is essential to encourage them to contribute in such applications. On the other hand, data accuracy is vital to execute CRS optimal performance. Therefore, balancing the privacy-accuracy trade-off challenge is critical especially since participants may become at risk and lose their lives in such situations. To this end, we propose a Context-Aware Privacy scheme (CAP) for crisis situations.

CAP works on balancing the privacy-accuracy trade-off of participant contributions. CAP aims to provide accurate privacy-preserved data to authorized recipients based on the participants’ situation. Different recipient categories receive a different level of participants’ private data.
1.3 Thesis Organization

In this chapter, we have highlighted the motivations and discussed the major contributions. The remainder of this thesis is organized as follows.

Chapter 2 introduces the required background for this research. This chapter defines the participatory sensing system and classifies its applications and their sensing modes. This chapter differentiates the terms of privacy, security and trust, as well as provides more details about the participatory sensing privacy and participatory sensing trust. In participatory sensing privacy, major related privacy schemes such as anonymization, cryptography and differential privacy are discussed and classified. In participatory sensing trust, the participant and data trust issues are discussed, and related schemes and methods such as reputation systems are reviewed. Finally, this chapter describes the crisis response system, its requirements and how it may benefit by allowing PS applications as an extra source of data.

Chapter 3 reviews the proposed framework architecture. The first part illustrates the major components and entities of the proposed schemes and shows the relations between them. Next, we briefly discuss multiple datasets we use in implementing the proposed schemes. An overview of the evaluation metrics to assess the results of the schemes is presented in the last part of this chapter.

Chapter 4 presents the Reputation Scheme to Evaluate Participant (RSEP) scheme for PS applications. In this chapter, we explain the challenge of validating participant contributions to ensure data trustworthiness in a PS application environment. Next, we propose the scheme architecture including its components and algorithms. The remaining parts of the chapter discuss the experimental results and evaluation metrics.
Chapter 5 introduces the Participant Contribution Trust (PCT) scheme in PS applications for crisis response systems. We clarify the contribution trust challenge in the case of crisis situations. In the first part of this chapter, we illustrate the scheme overview and its features during a crisis. Then, we discuss the evaluation environment and experimental results of the scheme.

Chapter 6 presents the Context-Aware Privacy (CAP) scheme for crisis situations. In this chapter, we explain the importance of the privacy for the participants and how complex it is in critical situations when a crisis occurs. We clarify the challenge of the accuracy-privacy trade-off. Then, we propose the major components of the CAP scheme that consists of context-aware scheme and privacy scheme. The remainder of the chapter discusses the experimental results and the evaluations metrics.

Chapter 7 provides a conclusion of the preceding chapters and a summary of related limitations and future work.
CHAPTER 2

BACKGROUND AND RELATED WORK

In this chapter, we discuss the main background research materials. In addition, we review some work related to this thesis research. In Section 2.1, we describe participatory sensing systems, their application classifications and sensing modes. Section 2.2 differentiates between the three terms: privacy, security and trust. In Section 2.3, we discuss participatory sensing privacy and review the major privacy methodologies that are being used for the participatory sensing applications. In Section 2.4, we describe participatory sensing trust and reputation systems. Finally, Section 2.5 defines crisis and crisis response systems.

2.1 Participatory Sensing Systems

A Participatory Sensing System (PSS) consists of participants, an application server and end-users. Participatory Sensing (PS) allows individuals and communities to contribute to an application by sensing their surrounding environment, collecting available data, sending collected data to a central application server and sharing the results with the end-users [1], as illustrated in Figure 2.1. Each of these steps uses existing technologies. Current sensor devices such as
smartphones and tablets are able to contribute to PS applications by using their embedded sensors to collect data. Cellular and Internet communication infrastructures such as LTE and WiFi facilitate information dissemination.

Smartphones are increasingly equipped with various embedded and/or peripheral sensors such as a camera, microphone, GPS, ambient light, proximity, accelerometer and temperature [2]. These sensors in PS enable a wide range of applications including urban planning [11], environmental monitoring [12], air quality monitoring [13], ambient noise monitoring [14], public health [9], transportation monitoring [15, 16], traffic monitoring [17], price-dispersion monitoring [18], mobile social services [19, 20], domestic eldercare [21] and citizen journalism [22]. These applications are just a few contexts in which PS can be performed by scalable and low-cost consumer devices. In other words, the readily equipped participatory sensing devices with required sensors coupled with these available applications make the deployment cost of a participatory sensing system virtually zero. The above mentioned applications and others can be classified into two main classes: people-centric and environment-centric.
2.1 Participatory Sensing Systems

![Diagram of Participatory Sensing Applications]

*Figure 2.2: Classification of participatory sensing applications*

**People-centric applications** emphasize documenting individual’s behaviour. They are divided into two classes, *health* applications and *economy* applications, as shown in Figure 2.2. Some of these applications are public health [9], domestic eldercare [21], price-dispersion monitoring [18] and mobile social services [19, 20].

**Environment-centric applications** emphasize documenting and collecting environmental parameters. They are divided into two classes, *urban planning* applications and *environment* applications, as illustrated in Figure 2.2. Examples of such applications are transportation monitoring [15], road condition and traffic monitoring [17], environmental monitoring [12], air quality monitoring [13] and ambient noise monitoring [14].

People and environment-centric applications can be run on scalable, hand-held, smart devices. As a result of the above applications, extra information will be collected in addition to the collected data, such as location and time, in each contribution to verify the credibility of the collected data.
2.1 Participatory Sensing Systems

In other words, the application server needs to know the location and time of the participant’s collected data to improve data analysis and to identify cheating of false data [24, 22].

Application properties may require sensor devices to take an action in one of three sensing modes that are at the level of user involvement [2]. The three sensing modes are manual, automatic and opportunistic [25] as shown in Figure 2.3. Manual is where participants need to execute the sensing task for each contribution. Automatic is mainly based on time interval where participants allow sensors to act periodically. Opportunistic is when participants permit sensors to act whenever they receive a task or satisfy applications’ conditions such as entering or exiting a required zone.

Similar PS approaches carry similar definitions, requirements and goals. Mobile sensing [3], opportunistic sensing [4], public sensing [5] and crowd sensing [4] are being used in the field of PS for similar purposes [26, 27]. However, a number of researchers differentiated between these approaches based on the sensing modes mentioned earlier. For instance, Ganti et al. [4] differentiated between participatory and opportunistic sensing, with the former defined as the kind of sensing where individuals are actively involved in contributing sensor data. On the contrary, opportunistic sensing is where the sensing is more autonomous and user involvement is minimal.
2.2 Privacy, Security and Trust

The combination of privacy, security and trust targets to ensure protection of systems, networks, information or individuals. In fact, each of the three terms may have slightly different definitions depending on their field of research. Thus, privacy, security and trust definitions in PS may differ from the respective fields. A brief definition of each term in the content of PS is provided below.

**Privacy** governs the use and access of data in legal and appropriate ways, as well as protecting data. Granting access to data can be controlled by privacy schemes, rules and policies.

**Security** fulfills the primitives of confidentiality, integrity and availability of data. In general, data security and its schemes are mostly covered by the definition of privacy in PS.

**Trust** assures that steps and processes of a system behave as they are expected to act. Additionally, trust may include the trustworthiness of participants or data, and that gives trust a major role in PS.

2.3 Participatory Sensing Privacy

The success of PSS is dependent on participant contributions. Therefore, encouraging individuals to contribute is an essential task and that does not happen without developing solid applications that satisfy participants’ requirements. One of the most important requirements is ensuring participant’s privacy.

Since most PS applications collect extra data, such as location, time and identity, in addition to the collected data through participants’ sensor devices, privacy issues become a concern. Thus, privacy is the main challenge that threatens the success of PSS [28, 29, 2, 22, 9, 10, 30, 31].
2.3 Participatory Sensing Privacy

Privacy is concerned with not disclosing participants’ private data without their permission. To do so, private data should be controlled before they are released. This kind of control could be at either ends (sender or receiver) or at a trusted third party, as shown in Figure 2.4.

Designing a successful PS application is met with overcoming the challenge of Participatory Sensing Privacy (PSP) by safeguarding participants’ privacy [10, 31]. Safeguarding participants’ privacy such as their identity, contacts, location, time, etc. needs to be achieved with the end result so that participants become more comfortable to contribute to an application [10].

Researches have proposed various privacy schemes using different methodologies for PS applications. The majority of the privacy schemes use the methodologies of anonymization through $k$-anonymity, mix-networks, cryptography and differential privacy.

The privacy schemes proposed by researchers in [10, 32, 33, 34] use $k$-anonymity as an anonymization method to preserve participant privacy. $K$-anonymity eliminates the uniqueness of participant data. Thus, a release of data provides $k$-anonymity protection if the data for each participant contained in the release cannot be distinguished from at least $k-1$ other participants whose data also appear in the release.

![Figure 2.4: Participatory sensing privacy through a trusted third party](image-url)
2.4 Participatory Sensing Trust

Some privacy schemes [35, 36, 37, 38] consider mix-network as an anonymization channel. Mix-network consists of multiple nodes (participants), which are assumed to be trusted, to decouple the report producer’s private data from being disclosed before it arrives to the other end. Mix-network is usually located between participants and the application server, and sometimes between participants and a third party especially in the case of non-trusted third party.

A number of privacy schemes [26, 39, 40, 41] use cryptography as a privacy method to protect participant privacy. Cryptography encrypts report content at the sender’s side, sends it encrypted to the application server, then decrypts it at the recipient’s side. Their purpose of using cryptography is to protect the report contents from being disclosed to any unauthorized entity and to maintain data integrity and confidentiality.

Some privacy schemes proposed [42, 43, 44, 45, 46] consider differential privacy as a method of protecting participant privacy. Differential privacy is a concept for dataset privacy that learns as much as possible about a group of participants while learning as little as possible about individuals. Regardless of the background knowledge, an adversary with access to the privacy-preserved data will have an equally likely conclusion whether a participant data is in the dataset or not.

2.4 Participatory Sensing Trust

PS applications are usually open to public and receive sensor data from multiple distinct participants. This openness feature, however, allows inaccurate and corrupted contributions which negatively affect the quality of the application services. Therefore, validating the correctness of contributions is essential for PS applications [7, 47]. Participatory Sensing Trust (PST) can be
2.4 Participatory Sensing Trust

ensured by evaluating the participant reputation values using a reputation system and comparing
the participant contributions with others to keeping only the correct and the most accurate ones.

The issue of contribution trust in PS has been studied in [7, 8]. The trust scheme outlined in [7]
proposes a trust-based framework to measure the accuracy of the contributions. It maintains a list
of participants who are deemed to be trusted and protected from external attacks. Those trusted
participants consistently sense accurate data. When other participants contribute in a task, the trust-
based framework evaluates them by comparing their contributions with the contributions of the
neighboring trusted participants. The trust scheme [8] evaluates participants’ contributions based
on their reputation values. The reputation value computations rely on the participants’ previous
contributions that have been evaluated based on the quality of the sensed data. The scheme assesses
the contribution quality by passing them through a quality evaluator component. The quality
evaluator’s results and participant reputation history are used to calculate the participant’s current
reputation.

A Reputation System (RS) is a way to measure a set of objects such as service providers, sellers,
buyers or services within a domain by computing their reputation values [48]. RS uses a specific
reputation algorithm to compute the reputation value based on the history of the object
dynamically. RS is popular in online markets such as eBay\(^1\), AliBaba\(^2\) and Amazon\(^3\). These e-
markets use RS to allow buyers and sellers to rate each other based on their transaction satisfaction
such as delivery time, quick payments, etc. For example, eBay has an RS where buyers can rate
the sellers, and vice versa, by leaving a feedback rating of positive, neutral or negative after each

\(^1\) http://www.ebay.com/
\(^2\) http://www.alibaba.com/
\(^3\) http://www.amazon.com/
2.5 Crisis Response Systems

transaction. The higher the positive feedback, the higher the reputation value. The eBay method of calculating a customer’s reputation value can be obtained by dividing the positive feedback scores by the number of responded feedbacks in the past 12 months.

The schemes [49, 50] use RS as one of the ways to validate the correctness and accuracy of participant contributions by computing their reputation values. In [49], an RS is compatible with social networks to distribute participatory sensing tasks. The social network members could be requesters of a service or participants. The computations involved, in assessing participant contribution reputations, are influenced by the requester, who is able to add their evaluations to the contribution reputation. The RS in [50] aims to improve data quality by classifying participants before starting the tasks. The requesters set a list of conditions that participants must satisfy. The system ranks participants who meet the requester conditions based on the participant reputation values. Then, requesters select the desired rank level of participants.

2.5 Crisis Response Systems

A crisis situation is defined as an unpredictable critical phase when an urgent action needs to be taken to disrupt or decrease difficulties [6]. Accidents, fires, earthquakes, floods, hurricanes, landslides, etc., threaten people’s lives and must be dealt with in a speedy fashion. A Crisis Response System (CRS) consists of a group of authorities who are trained to deal with such situations [47, 51]. The authorities need accurate data to be able to make appropriate rescue plans and act to resolve the situation. When a crisis happens, some of the data is already known to the authorities such as the location of forests, lakes, mountains, municipal facilities and routes into and out of the crisis site. However, additional data directly related to the crisis would be beneficial to make efficient rescue plans. Social media and social networks are examples of great sources of
2.5 Crisis Response Systems

data that may help rescue authorities make decisions. This data could also be collected by individuals who are within the close proximity to the crisis and gathered by a PS application that delivers the data to the CRS.
3.1 The Framework

In this research, we investigate the following three research problems: (1) ensuring participant contribution data trustworthiness in a PS application, (2) verifying the accuracy of participant contributions in critical situations, and (3) protecting participant privacy in critical situations.

This chapter is organized as follows. In Section 3.1, we present an overview of the proposed framework. We discuss the overall framework architecture that includes the general components and entities of the proposed schemes. In Section 3.2, we discuss multiple datasets that we use in the implementation. Section 3.3 briefly reviews the evaluation metrics to assess the results of the proposed schemes.

3.1 The Framework

The proposed framework involves a set of schemes that co-operate to provide a privacy-preserved accurate data from participants through a PS application. Figure 3.1 shows the major framework architecture components that are required for the proposed schemes.
3.1 The Framework

First, we propose a *Reputation Scheme to Evaluate Participants (RSEP)* that aims to provide accurate participant contributions in a typical environment. This scheme depends on RS that measures the received contributions based on participant reputation values. RSEP consists of two major phases. First, the scheme selects the most accurate contributions by grouping participants based on the similarities of their contributions. The next step of this phase calculates each group value by computing its participants’ reputation values. The highest group value is the winner of the most accurate contribution that will be sent to the next component. In the second phase, the scheme updates participant reputation values by assigning positive scores to the participants with accurate contributions and negative scores to the participants with inaccurate contributions. The second phase, upon completion of assigning the scores, saves the updated participants’ data and contributions into the participant and contribution history repositories. The details of this process are described in Chapter 4.

A *Participant Contribution Trust (PCT) scheme* is proposed that provides accurate participant contributions in crisis situations. Such situations require various considerations. Participant contributions become more important than in other situations due to the risk that they or others could face. PCT consists of three major phases. First, the scheme divides the affected crisis area into multiple sectors. Second, the scheme filters participant contributions to get their most accurate information. The third phase updates participant reputation values by updating their scores (positive or negative) based on the validity of their past contributions. Similar to the previous scheme, PCT saves the updated data at participant and contribution history repositories. Chapter 5 describes this scheme in further detail.
3.2 Datasets

The outputs of the previous two schemes are the input to the context-aware scheme. This scheme acts as the first step required before the initiation of the privacy scheme that protects participants’ privacy. The two schemes combined is called Context-Aware Privacy (CAP) scheme, and it aims to encourage participants to contribute comfortably. CAP is compatible to work in crisis situations taking into consideration of the possible risk to the participant's safety. CAP assesses the privacy level based on the risk state and the type of recipient of the participant data. The context-aware scheme gathers participant data and their contributions to get the participant situations, in addition to recipients’ categories. CAP then applies the policies to decide what participant attributes to release, to what level of privacy and to which recipient categories. Next, the scheme executes the decision of the previous step by clearly releasing participant attributes to the publisher, totally hiding attributes from being released or applying the privacy scheme on the attributes that need to be protected. The publisher entity, then, publishes the privacy-preserved data, which have been filtered, to the PS application server. The details of the CAP scheme are described in Chapter 6.

3.2 Datasets

We evaluated the proposed schemes using two real-world datasets that were modified by generating additional data to match our functionality requirements. The first real-world dataset, called Roma Taxi, is publicly available on Crawdad archive at Dartmouth College [52]. The other real-world dataset, called Canadian Community Health Survey (CCHS), which is also publicly available from Statistics Canada, Health Statistics Division [53].

For the evaluation, we require the dataset to provide data about participants’ locations, date and time. The original Roma Taxi dataset [52] provides these requirements by collecting the
3.2 Datasets

Figure 3.1: The framework architecture overview
3.2 Datasets

GPS position of participants (taxicabs) moving around the city of Rome. Each participant is equipped with an Android OS tablet device running an app that uses the GPS sensor to update their current positions including date and time.

In a typical situation, as in an RSEP scheme, we use the Roma Taxi dataset, in addition to the attached generated dataset (to be discussed further in Chapter 4). We divide the whole area into equal square sectors. Alternatively, in a crisis situation, where data follows a certain trend, we center the crisis and create multiple zones around the crisis. The closer the zone to the crisis, the higher the risk.

For all the presented results, we analyze the available participant contributions over a few days. We split each day into multiple epochs. In every epoch, we have a different number of participants that are randomly selected. Since participants are mobile, participant positions may change in different epochs.

The CCHS dataset [53] is a survey and a source for health research that collects information related to health care for the Canadian population. It relies upon a large sample of respondents and is designed to provide reliable estimates at the health region level (to be discussed further in Chapter 6).

For the implementation, as we explain in Chapter 6, we require the dataset to provide enough data about the participants that includes personal data such as age, gender, height, weight and health condition, which CCHS dataset provides. We select a few hundreds out of thousands of participants in the survey and assign their data randomly to the participants as their metadata. The dataset eventually has one record for each participant.
3.3 Evaluation Metrics

The schemes will be evaluated in two dimensions. The first dimension is to assess the accuracy results of the schemes compared to our pre-known participants’ classifications. The second dimension is to compare and benchmark the schemes against others. To that end, we use the following evaluation metrics:

*False Positive (FP) rate* means that a participant is classified as dishonest before running the scheme, but the results show that its reputation value is above a pre-set threshold (detailed in Chapter 4). The threshold is a percentage that is applied to the participant reputation values to distinguish honest participants from dishonest participants.

*False Negative (FN) rate* means that a participant is classified as honest before running the scheme, but the results show that its reputation value is below the threshold (detailed in Chapter 4).

*Precision rate* is the ratio of the honest participants whose reputation values are above the threshold to all participants whose reputation values are above the threshold (detailed in Chapter 5).

*Recall rate*, as we define, is the ratio of the honest participants whose reputation values are above the threshold to all participants of all classes (detailed in Chapter 5).

*Identification Confidence (IC)* measures the confidence level of re-identifying a participant through its published data (detailed in Chapter 6).
3.3 Evaluation Metrics

*Privacy-Accuracy Impact* measures the impact that a privacy scheme may cause in preventing useful data due to hiding a portion or all of the data rendering the results useless (detailed in Chapter 6).
4.1 Introduction

Participatory sensing (PS) applications are usually open to the public and receive sensor data from multiple participants. This openness characteristic however, allows inaccurate and corrupted contributions which negatively affect the quality of the application services [22, 48]. Therefore, validating the accuracy of contributions is essential for the PS applications. A way of evaluating contribution validity is by evaluating participant reputation values.

In this chapter, we propose a Reputation Scheme to Evaluate Participants (RSEP) and validate their contributions. RSEP computes each participant reputation value based on their previous contribution results to help validate their current contribution. At the end of each round, the scheme rates all contributions and assigns scores to each participant based on their contribution validity.

RSEP consists of two major phases: (1) selecting the most accurate contributions and (2) updating participant reputation values. Each phase must follow multiple steps to complete its tasks including various equations that compute individual and group reputation values.
4.2 The RSEP Scheme

We evaluate RSEP on a real-world application dataset that collects sensor data from multiple participants [54]. They are a fleet of taxicabs in the city of Rome, Italy. They use their sensor devices to collect outside temperatures from different grids at different periods of the day. The application uses the collected temperatures for weather forecasting.

We perform empirical validations that show the efficiency of RSEP in assessing the correctness of the contributions and in evaluating their participants. We compare RSEP to an existing reputation scheme. RSEP will enhance the services of the PS applications. It filters out the inaccurate contributions and passes only the accurate contributions to the application servers.

The remainder of this chapter is organized as follows. Section 4.2 details the proposed reputation scheme and its algorithms. In Section 4.3, we describe the experimental evaluation and setup, and discuss the evaluation results. In Section 4.4, we discuss some participants’ related trajectories, data and methods of calculating reputation values. Section 4.5 summarizes this chapter.

4.2 The RSEP Scheme

In this section, we provide the overview of the proposed reputation scheme for participatory sensing in Section 4.2.1. Sections 4.2.2 and 4.2.3 discuss the algorithms of RSEP and participant reputation value computation, respectively.

4.2.1 The RSEP Overview

Figure 4.1 shows the data flow from participant handheld devices to the application server passing through RSEP. Participants start sensing using their sensor devices and send the collected sensor data to RSEP. It processes the received data and sends only the most accurate contributions
4.2 The RSEP Scheme

The RSEP Scheme consists of two major phases: (1) selecting the most accurate contributions and (2) updating participant reputation values.

In phase one, participant contributions go through three steps to evaluate them and to ease the selection of the most accurate contributions to be sent to the application server (Algorithm 1).

The first step of phase one starts with dividing participants into three groups. Second, it evaluates each group by calculating their values. To calculate a group value, the scheme requires the calculation of each participant reputation (Algorithm 2) in the group and each participant weight among other participants in the same group. Third, it selects the contributions of the highest group value and sends them to the application server.

In phase two, RSEP applies the final step by updating the participant scores based on the accuracy of their contributions. It assigns positive scores to the participants of the selected group (highest group value) and negative scores to the remaining participants.

Figure 4.1: The RSEP architecture
There are two repositories at RSEP to save the information collected from the results of the two phases. One saves participant history and the other saves contribution history. The participant history repository saves each participant’s information. After each contribution, the scheme updates the participant information and computes the new reputation value. The contribution history repository saves all the contributions made by participants. After each contribution, the scheme records the contribution information.

RSEP provides two modes of operations, aging and newcomer, to help make decisions in selecting accurate contributions. Aging allows the scheme to only consider the participant reputation value of the most recent contributions. In addition, it gives an opportunity for disreputable participants to re-establish their reputation status. By using contribution history repository, aging is able to only consider the last $Z$ contributions, days or months in its calculation of participant reputation values.

In the case of a newcomer participant, the scheme assigns an initial reputation value of 0.5. If a newcomer receives a positive score in their first contribution, the reputation value will increase to 1 (100%). On the contrary, if the newcomer receives a negative score, the reputation value will drop to 0. Therefore, RSEP proposes to continue assigning a reputation value of 0.5 for the first $y$ contributions to avoid the fluctuation of the newcomer reputation value. RSEP counts the positive and negative scores that a newcomer receives during the $y$-th contributions to be used in computing the actual reputation value in the $(y+1)$-th contribution.

4.2.2 The RSEP Algorithm

In Algorithm 1, RSEP starts by gathering all participant contributions under certain conditions such as location and time, as scheme inputs. It then selects the most accurate contributions and updates participant scores as scheme outputs.
4.2 The RSEP Scheme

After gathering all contributions, the scheme divides participants into three groups: \( G_x, x = \{1, 2, 3\} \). The grouping is based on the participant sensed data \( (q) \), as shown in Lines 1 to 6. The grouping function compares every \( q \) to the ground truth \( (\mu) \) within a range of grouping parameter \( (gp) \). Thus, similar participant sensed data will be added to the same group.

Next, the scheme calculates each group value \( (V_{G_x}) \). This step requires computing participant reputation values \( (rv_i), i = \{1, ..., m\} \) where \( m \) is the total number of participants, from Algorithm 2. When participant reputation values are computed (Line 7), the scheme calculates each participant’s weight \( (w) \) among other participants in the same group, as discussed in Lines 8 to 12. The absolute total of all participant weights in the same group is one (100%). A participant weight is computed by dividing the reputation value of participant \( i \) \( (rv_i) \) over the summation of all participant reputation values in the same group \( G_x \) as follows:

\[
    w_i = \frac{rv_i}{\sum_{i \in G_x} rv_i}
\]  

(4.1)

Line 13 shows the last step of computing \( V_{G_x} \) that depends on Eq. 4.1.

\[
    V_{G_x} = \sum_{i \in G_x} w_i \times rv_i
\]  

(4.2)

The previous steps are applied on each of the three groups to get their \( V_{G_x} \). Next step compares between the three group values and selects the Highest Group Value \( (HGV) V_{G_x} \) as the winner group,
4.2 The RSEP Scheme

Algorithm 1 - Reputation Scheme to Evaluate Participants (RSEP)

Input: Periodic Participants Contributions

Output: Accurate Contributions; Scores Update

Participants Grouping ($G_x$)
1. for $i \leftarrow 1$ to $m$ do
2. 
3. if $(\mu - (\mu \times gp)) \leq (q_i) \leq (\mu + (\mu \times gp))$
4. then Add $q_i$ to $G_1$
5. else if $(q_i) < (\mu - (\mu \times gp))$
6. then Add $q_i$ to $G_2$
7. else Add $q_i$ to $G_3$

Group Values Calculation ($V_{G_x}$)
8. Get participant reputation values ($rv$) // Call Algorithm 2
9. for $x \leftarrow 1$ to $3$ do
10. 
11. for $i \leftarrow 1$ to $|G_x|$ do
12. $RV_x \leftarrow \sum rv_i$
13. $w_i \leftarrow \frac{rv_i}{RV_x}$
14. $V_{G_x} \leftarrow \sum w_i \times rv_i$

Highest Group Value Selection ($HGV$)
15. if $V_{G_2} \leq V_{G_1} \geq V_{G_3}$
16. then $HGV \leftarrow V_{G_1}$
17. else if $(V_{G_2} \geq V_{G_3})$
18. then $HGV \leftarrow V_{G_2}$
19. else $HGV \leftarrow V_{G_3}$

Send $q_i$ of $HGV$ to the Application Server

Positive ($ps$) and Negative ($ns$) Scores Updating
20. for $x \leftarrow 1$ to $3$ do
21. 
22. if $V_{G_x} = HGV$
23. then
24. for $i \leftarrow 1$ to $|G_x|$ do
25. $ps_i \leftarrow ps_i + 1$
26. else
27. for $i \leftarrow 1$ to $|G_x|$ do
28. $ns_i \leftarrow ns_i + 1$
4.2 The RSEP Scheme

as shown in Lines 14 to 18. To this point, the scheme is able to send the contributions of the winner $G_x$ to the application server as the most accurate contributions.

Finally, RSEP updates the reputation values of the participants for their contributions. Lines 19 to 26 show the steps of the updating task by assigning positive scores ($ps$) and negative scores ($ns$) to the participants based on their group values. Thus, each participant in the winner group receives a $ps$ as an award for their accurate contributions. On the contrary, each participant in the other two groups receives an $ns$ for their inaccurate contribution. These new $ps$ and $ns$ change the reputation value of each participant either up or down based on the assigned score as in Eq. 4.3. Let the reputation value of participant $i$ ($rv_i$) be 75% from a total of 30 positive scores ($ps_i$) and 10 negative scores ($ns_i$) from its previous contributions. If it receives a $ps$ in a new contribution, $rv_i$ becomes 75.6%. In contrast, if it receives an $ns$ in a new contribution, $rv_i$ becomes 73.2%.

4.2.3 Reputation Value Computation Algorithm

Participant reputation values reflect their trustworthiness which plays a major role in allowing the scheme to make a selection decision. Algorithm 2 shows the steps to calculate a participant reputation value ($rv$). It can be calculated under the following two conditions. (1) If a participant is a newcomer ($nc$) (Lines 2 and 3), the scheme assigns an initial $rv = nc$, $nc = 0.50$ (50%) as starting value, then the participant builds its reputation value through the future contributions. (2) If a participant is not a newcomer (Lines 4 to 9), the scheme compares and takes the minimum number of contributions of $X$ or $Z$, where $X$ is the participant’s total number of contributions and $Z$ is the number of contributions that need to be considered for aging mode. If $X$ is the minimum number of contributions (Lines 4 to 6), the Total Positive Score of participant $i$ ($TPS_i$) equals the total positive
4.3 Experimental evaluation

scores in the previous contributions. On the contrary, if $Z$ is the minimum number of contributions (Lines 7 to 9), $TPS_i$ is the total positive scores in the last $Z$ contributions only.

Finally, Line 10 computes the reputation value of participant $i$ ($rv_i$) using the previous inputs of $TPS_i$ and $Y_i$ as follows:

$$rv_i = \frac{TPS_i}{Y_i}$$  \hfill (4.3)

Algorithm 2 - Participant Reputation Values Computation

**Input**: Participants ID

**Output**: Participant Reputation Values ($rv$)

1. for $i \leftarrow 1$ to $m$ do
2. if $X_i < y$ \quad // Newcomers mode
3. then $rv_i \leftarrow nc$  
4. else if $X_i < Z$ \quad // Aging mode
5. then $TPS_i \leftarrow \sum ps_i$  
6. $Y_i \leftarrow X_i$  
7. else for $t \leftarrow X_i - (Z - 1)$ to $X_i$ do
8. $TPS_i \leftarrow \sum ps_t$  
9. $Y_i \leftarrow Z$  
10. $rv_i \leftarrow \frac{TPS_i}{Y_i}$  

4.3 Experimental evaluation

In this section, we discuss the experimental evaluation results of RSEP. In Section 4.3.1, we review the implementation setup and evaluation environment. Section 4.3.2 explains the dataset we use in the implementation. The evaluation metrics to assess the accuracy of the RSEP results are discussed in Section 4.3.3.
4.3 Experimental evaluation

4.3.1 Evaluation Environment

The implementation is evaluated using a real-world dataset that consists of a fleet of taxicabs as participants (see Section 4.3.2 for details). The participant collects sensor data, attaches date, time and location, and then sends the report to RSEP. It continues receiving contributions from the participants for each grid until the end of the current period. RSEP then starts processing all the contributions from that period as discussed in Section 4.2. It selects the most accurate contributions and sends them to the application server. Finally, RSEP updates the participant scores and saves them for the next participation.

4.3.2 Dataset

We adapt a real-world dataset that is publicly available on Crawdad archive\(^4\) [54] at Dartmouth College. The original dataset [52] collects the GPS position of taxicabs moving around the city of Rome, Italy. Each driver is equipped with an Android OS tablet device running an app that uses the GPS sensor to update their current position.

We limit the analysis to cover a large area of the center of Rome, where the density of taxicabs is high. We consider an area of approximately 22.5\(\text{x}\)22.5 [km \(\times\) km] whose bounds are given by the coordinate pairs (41.9951, 12.3648) and (41.7887, 12.6283). The area has been analyzed using 3x3 grids. A grid cell covers a square area of approximately 7.5\(\text{x}\)7.5 [km \(\times\) km].

For all the presented results, we analyze the sensing of 289 taxicabs over 4 days. We split each day into four periods, six hours each. The periods are as follows: early morning [00:00 – 05:59], late morning [06:00 – 11:59], afternoon [12:00 – 17:59] and evening [18:00 – 23:59].

\(^4\) http://crawdad.org/queensu/crowd_temperature/20151120
4.3 Experimental evaluation

We modify the original data by assuming that each taxicab is equipped with a peripheral temperature sensor. When the taxicab is moving, the sensor collects the outside temperature of its current grid and records the period of day. In each grid, we assume that each taxicab is allowed to participate once during each period of a day.

We generate a temperature value for every active taxicab in a certain period by applying Gaussian distribution. To fill out the parameters of Gaussian function, we assign a mean ($\mu$) and standard deviation ($\delta$) for every run. The mean value ($\mu$) corresponds to the ground truth temperature for every period in every grid on every day. We use The Weather Network\(^5\) statistics to assign the correct value ground truth to the specific period and grid location. For every taxicab, we assign a fixed error range ($\delta$) that remains the same in all of its contributions. To do so, we randomly classify participant taxicabs into three classes. First class, called “honest,” consists of taxicabs that usually sense accurate temperatures within a 10% error range from the ground truth. The population of honest class is 145 taxicabs (50% of all participant taxicabs). Second class, called “dishonest,” consists of taxicabs that usually sense inaccurate temperatures between 10% and 30% error range from the ground truth. The population of the dishonest class is 72 taxicabs (25%). Third class, called “misleading,” consists of the remainder of the 72 participant taxicabs (25%) that can report accurate or inaccurate temperatures. The data generator function makes a random decision to generate accurate or inaccurate temperatures for each taxicab among the misleading class. The latter class plays a major role in the results of the reputation scheme since the accuracy of their contributions is not consistent. The dataset assigns for each taxicab a sensed temperature contribution based on its fixed error range and the ground truth of the day, period and grid of its location.

\(^5\) http://www.theweathernetwork.com/
4.3 Experimental evaluation

4.3.3 Experiment Results

Collecting sensor data by the participants and sending this data to the application server are major tasks for participatory sensing. However, assessing those participants and selecting the accurate contributions are essential tasks for the application services. Hence, RSEP aims to apply these essential tasks efficiently. To evaluate the RSEP results, we apply two metrics: False Positive (FP) and False Negative (FN) rates.

FP rate is the ratio of the participants whose reputation values are above the threshold while they are originally classified as dishonest. FN rate is the ratio of the participants whose reputation values are below the threshold while they are originally classified as honest. The threshold is a percentage that is applied to the participant reputation values to distinguish honest participants from dishonest participants. Threshold value can be set based on the application requirements. FP and FN have an inverse correlation that depends on the threshold. The higher the threshold, the lower the FP, and the higher the FN.

The FP and FN rates are to measure the accuracy of RSEP in assessing participants. As discussed in Section 4.3.2, we randomly classified participant taxicabs into honest, dishonest and misleading. We generated the temperature degrees for the participant taxicabs with given error range based on their classes. Now, after running the scheme on all valid contributions and rewarding the accurate contributions with positive scores and the inaccurate contributions with negative scores, we check how accurate RSEP is in assessing participants.

To evaluate the RSEP results based on the FP and FN rates, we create three sets of participants: set_1 and set_2 consist of 50 and 150 randomly selected participant taxicabs, respectively, while set_3 consists of all 289 participant taxicabs. We set the metrics to three different thresholds: 60%, 70% and 80% to show the accuracy rates of assessing participants in different settings. Next, we apply
4.3 Experimental evaluation

each threshold on the three sets and get the FP and FN rates. To compute the FP and FN rates, we apply the following:

\[
FP rate_c = \frac{D_c}{|\text{subset}_c|} \quad (4.4)
\]

\[
FN rate_c = \frac{H_c}{set_c - |\text{subset}_c|} \quad (4.5)
\]

Here, \(D_c\) (a.k.a. FP number) is the total number of dishonest participants whose reputation values are above the threshold in \(\text{subset}_c\), \(c = \{1, 2, 3\}\). \(H_c\) (a.k.a. FN number) is the total number of honest participants whose reputation values are below the threshold in the rest of \(set_c\). The \(\text{subset}_c\) is the total number of participants whose reputation values are above the threshold in \(set_c\).

With a threshold of 60%, \(set_1\) has a \(\text{subset}_1\) of 37 participant taxicabs above the threshold and 13 participant taxicabs below the threshold. By executing the FP and FN rates in Eq. 4.4 and Eq. 4.5, we find that the FP rate is 3% and FN rate is 0%. The FP rate of 3% is due to one participant taxicab that has a reputation value above the threshold after running the scheme, while it was classified among the dishonest class before running the scheme. On the contrary, no single participant taxicab is classified as honest and the scheme shows that it is dishonest. In \(set_2\), we get a \(\text{subset}_2\) of 110 participant taxicabs above the threshold and 40 participant taxicabs below the threshold. The FP rate is 6% and FN rate is 2%. In \(set_3\), a \(\text{subset}_3\) of 211 participant taxicabs above the threshold with the FP and FN rates of 7% and 1%, respectively.

With the threshold of 70%, we get subsets of 35, 101 and 195 participant taxicabs above the threshold with the FP rates of 3%, 4% and 5%, and FN rates of 7%, 2% and 1%, for \(set_1\), \(set_2\) and \(set_3\), respectively.
4.3 Experimental evaluation

With the threshold of 80%, we get subsets of 28, 84 and 168 participant taxicabs above the
threshold with the FP rates of 0%, 0% and 2%, and FN rates of 9%, 5% and 5%, for set\textsubscript{1}, set\textsubscript{2} and
set\textsubscript{3}, respectively.

In order to understand the advantage that PS applications gain from using RSEP, we implement
Reputation and Contribution Quality Scheme (RCQS) [8] to compare our scheme to another
existing scheme. We focus on this particular scheme because it mainly depends on the current and
previous participant contributions quality when it computes the reputation value, unlike other
schemes where they give the service requesters or users leverage to affect the reputation value
computation. We evaluate the RCQS using our dataset to get a reasonable comparison.

For the RCQS scheme, we measure the steps of assessing participants and evaluating their
reputations. The inputs for the scheme in a period are a prediction value that is derived from the
participant contribution and a ground truth value that is received from the end user. These inputs
pass through three main components that analyze the possible data errors, evaluate the contribution
quality and finally evaluate participant reputation as the scheme output. The last component
computes the reputation value based on two factors, data quality level that is received from the
previous component and participant history. Next, we apply the FP and FN rate metrics on those
final participant reputation values (outputs) to evaluate the scheme accuracy in assessing
participants.

Figure 4.2 illustrates the FP and FN rates for RSEP and RCQS based on the thresholds of 60%,
70% and 80%. The lower the rate, the better the accuracy in assessing participants. Therefore, the
results in all three thresholds show that RSEP has a better performance than RCQS in both metrics.
In Figure 4.2(a), for example, the FP rates in RSEP is 3%, 6% and 7%, while they are 13%, 14%
and 13% in RCQS for set\textsubscript{1}, set\textsubscript{2} and set\textsubscript{3}, respectively.
4.3 Experimental evaluation

Figure 4.2: The FP and FN rates with three threshold settings for RSEP and RCQS
4.4 Discussion

The FN rates are 0%, 2% and 1% in RSEP and 7%, 11% and 8% in RCQS for \( \text{set}_1, \text{set}_2 \) and \( \text{set}_3 \), respectively.

The different factors used in RCQS during the reputation computation causes having higher rates. Combining the two factors, data quality level and reputation history, in the computation without assigning a reward mechanism produces a fluctuation of reputation values during a few periods. Consequently, some honest participants may have lower reputation values than what they deserve because of a few inaccurate contributions, and vice versa.

4.4 Discussion

We review data repositories and participants’ trajectories in Section 4.4.1. We discuss additional instances of computing participant reputation values in Section 4.4.2 and Section 4.4.3.

4.4.1 Data Repositories and Trajectories

Participant history is one repository that saves taxicab history and updates that taxicab's file after every contribution. Table 4.1 shows a sample of 10 out of 289 total participant taxicabs including their identities, total number of positive scores, total number of negative scores and current reputation value. For example, taxicab number 135 has 49 ps out of 53 contributions. These values lead to its \( rv \) of 0.92 using Eq. 4.3.

Contribution history is the other repository that saves all individual contributions of each participatory taxicab. After each complete round, the contribution history repository saves all the contributions information of the period including identity, sensing date, time, location, sensed data, positive or negative score (received from the current contribution) and reputation value. Table 4.2
4.4 Discussion

shows a sample of 10 out of 5,082 total contributions. For example, we can extract the contribution information of taxicab number 239. It collected sensor data in grid 5 (latitude 41.8990, longitude 12.4905) at noon on February 3, 2014 with a sensed temperature of 13.4 Celsius. The contribution was not selected as an accurate temperature and, therefore, received a negative score.

To show the trajectories of a participant taxicab, we analyze its records that are saved in the participant history and contribution history repositories. For example, taxicab number 135 has been active during the four analyzed days in multiple grids and in different periods. Figure 4.3 shows the trajectories of the taxicab number 135 over the four day period (February 1-4, 2014). It is interesting to note in its trajectory that the taxicab received four negative scores, as shown in Table 4.1.

<table>
<thead>
<tr>
<th>Participant ID</th>
<th>Positive Score</th>
<th>Negative Score</th>
<th>Reputation Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
<td>49</td>
<td>4</td>
<td>0.92</td>
</tr>
<tr>
<td>12</td>
<td>32</td>
<td>3</td>
<td>0.91</td>
</tr>
<tr>
<td>68</td>
<td>20</td>
<td>2</td>
<td>0.91</td>
</tr>
<tr>
<td>269</td>
<td>26</td>
<td>2</td>
<td>0.93</td>
</tr>
<tr>
<td>305</td>
<td>16</td>
<td>3</td>
<td>0.84</td>
</tr>
<tr>
<td>13</td>
<td>29</td>
<td>4</td>
<td>0.88</td>
</tr>
<tr>
<td>61</td>
<td>17</td>
<td>6</td>
<td>0.74</td>
</tr>
<tr>
<td>288</td>
<td>28</td>
<td>1</td>
<td>0.97</td>
</tr>
<tr>
<td>179</td>
<td>9</td>
<td>7</td>
<td>0.56</td>
</tr>
<tr>
<td>293</td>
<td>11</td>
<td>18</td>
<td>0.38</td>
</tr>
</tbody>
</table>

Table 4.1: Sample of participant history repository

(Sample of 10 participant history shows their total positive and negative scores and current reputation value)
4.4 Discussion

The taxicab received the ns in the early morning (in grid 4) and in the evening (in grids 3 and 6) on February 1. Moreover, it received the fourth ns in the afternoon (in grid 2) on February 3. The reason for receiving negative scores in grids 4, 6 and 2 was due to the inaccurate contributions the taxicab made. On the contrary, from the contributions analysis of the taxicab number 135, we find that it collected accurate sensor data in grid 3 but its group value was low due to the low reputation values of other members in the same group.

4.4.2 Double Recent Positive Contributions Method (DRPC)

As discussed earlier in Section 4.2.3, RSEP provides aging mode when computing participant reputation value. Aging considers the last Z contributions to reflect the recent participant behavior.

<table>
<thead>
<tr>
<th>Participant ID</th>
<th>Sensing Date</th>
<th>Sensing Time</th>
<th>Sensing Location</th>
<th>Sensed Data</th>
<th>Positive/Negative</th>
<th>Reputation Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>239</td>
<td>03/02/2014</td>
<td>12:00:04</td>
<td>41.8990, 12.4905</td>
<td>13.4</td>
<td>0</td>
<td>0.67</td>
</tr>
<tr>
<td>243</td>
<td>03/02/2014</td>
<td>14:50:12</td>
<td>41.8580, 12.4779</td>
<td>16.1</td>
<td>1</td>
<td>0.92</td>
</tr>
<tr>
<td>248</td>
<td>03/02/2014</td>
<td>13:33:15</td>
<td>41.8621, 12.4528</td>
<td>16.3</td>
<td>1</td>
<td>0.43</td>
</tr>
<tr>
<td>249</td>
<td>03/02/2014</td>
<td>12:11:12</td>
<td>41.8965, 12.4776</td>
<td>16.1</td>
<td>1</td>
<td>0.80</td>
</tr>
<tr>
<td>252</td>
<td>03/02/2014</td>
<td>17:05:59</td>
<td>41.8579, 12.4709</td>
<td>15.1</td>
<td>1</td>
<td>0.85</td>
</tr>
<tr>
<td>262</td>
<td>03/02/2014</td>
<td>17:59:45</td>
<td>41.9013, 12.5012</td>
<td>16.8</td>
<td>1</td>
<td>0.83</td>
</tr>
<tr>
<td>274</td>
<td>03/02/2014</td>
<td>12:00:10</td>
<td>41.9003, 12.4727</td>
<td>14.8</td>
<td>1</td>
<td>0.77</td>
</tr>
<tr>
<td>281</td>
<td>03/02/2014</td>
<td>12:32:25</td>
<td>41.8998, 12.4542</td>
<td>16.1</td>
<td>1</td>
<td>0.67</td>
</tr>
<tr>
<td>287</td>
<td>03/02/2014</td>
<td>15:25:15</td>
<td>41.9064, 12.5386</td>
<td>16.3</td>
<td>1</td>
<td>0.50</td>
</tr>
<tr>
<td>309</td>
<td>03/02/2014</td>
<td>12:00:11</td>
<td>41.9207, 12.4801</td>
<td>14.2</td>
<td>0</td>
<td>0.73</td>
</tr>
</tbody>
</table>

Table 4.2: Sample of contribution history repository

(Sample of 10 contribution history that were collected for grid 5, in the afternoon, on February 3, 2014)
4.4 Discussion

and trustworthiness. In this section, we propose an additional instance of the aging mode to compute the reputation value by Doubling Recent Positive Contribution (DRPC). DRPC instance doubles only the positive scores in the last \( v \) contributions of the last \( Z \) contributions. In other words, the positive scores of the last \( v \) contributions are counted twice, one is with the rest of the contributions and the other count is for those within the last \( v \) contributions only. DRPC aims to offer an extra

---

**Figure 4.3: Sample of a participant trajectory across multiple sectors and days**

(Participant ID 135 trajectory on February 1 through 4)
4.4 Discussion

advantage of enhancing the reputation value participants who provided accurate contributions and received positive scores recently.

Algorithm 3 is a modified version of Algorithm 2 which is the original method of computing reputation values. DRPC is not practical in the case of newcomer’s mode where the number of participant contributions is less than \( y \) due to the fluctuation of the newcomer reputation value. Algorithm 3 shows that DRPC is applied in both cases when the number of contributions is less than \( Z \) (Lines 4 to 8), as long as they are more than \( y \), and more than \( Z \) (Lines 9 to 13).

We re-implement RSEP with the new DRPC method of computing participants’ reputation values. In the new implementation, we use the same reputation scheme and dataset as in the original RSEP. Next, we assess the experiment results using the same metrics (the FP and FN rates), the three set sizes (50, 150 and 289) and the three thresholds (60%, 70% and 80%).

In order to measure the differences between the two methods of computing reputation values, we compare the assessment results of the original RSEP with the results of DRPC. Figure 4.4 shows the FP and FN rates for RSEP and DRPC with the three thresholds of 60%, 70% and 80%. The lower the rate, the better the accuracy in assessing participants.

The overall results show that DRPC has an increase in all the FP rates in the three thresholds except for two cases in set1 with the thresholds of 70% and 80% (Figure 4.4(b) and Figure 4.4(c)), where DRPC has equal FP rates with the original RSEP. On the other hand, DRPC has better FN rates than RSEP in most cases of set1 and set3 in the three thresholds, while both methods have equal FN rates with set2.

Focusing on doubling only the participant positive scores in the last \( v \) contributions causes an increase in the reputation values, with no negative effects on decreasing them. This eventually raises
4.4 Discussion

The number of participants whose reputation values are above the thresholds, in both classes

- Threshold of 60%
- Threshold of 70%
- Threshold of 80%

Figure 4.4: The FP and FN rates with three threshold settings for RSEP and DRPC
4.4 Discussion

**Algorithm 3 - Participant Reputation Values Computation - Double Recent Positive Contributions**

**Input:** Participants ID

**Output:** Participant Reputation Values ($rv$)

1. for $i \leftarrow 1$ to $m$ do
2. \hspace{1cm} if $X_i < y$ \hspace{1cm} // Newcomers mode
3. \hspace{1cm} then $rv_i \leftarrow nc$
4. \hspace{1cm} else if $X_i < Z$ \hspace{1cm} // Aging mode
5. \hspace{1cm} then $TPS_i \leftarrow \sum p_{si}$
6. \hspace{1.5cm} for $o \leftarrow X_i - (v - 1)$ to $X_i$ do
7. \hspace{2.5cm} $TPS_i \leftarrow (\sum pso) + TPS_i$
8. \hspace{1.5cm} $Y_i \leftarrow X_i + |\sum pso|$  
9. \hspace{1.5cm} else for $t \leftarrow X_i - (Z - 1)$ to $X_i$ do
10. \hspace{2.5cm} $TPS_i \leftarrow \sum p_{ti}$
11. \hspace{1.5cm} for $o \leftarrow X_i - (v - 1)$ to $X_i$ do
12. \hspace{2.5cm} $TPS_i \leftarrow (\sum pso) + TPS_i$
13. \hspace{1.5cm} $Y_i \leftarrow Z + |\sum pso|$  
14. \hspace{1cm} $rv_i \leftarrow \frac{TPS_i}{Y_i}$

the number of participants whose reputation values are above the thresholds, in both classes of honest and dishonest. As a result, DRPC has more dishonest participants, who received positive scores recently, are above the threshold ($D$) than RSEP, which is the main reason of the increase in the FP rates. Since DRPC does not cause any decrease in the reputation values, the results do not show any increase in the FN rates compared to RSEP.

**4.4.3 Double Recent Contribution Scores Method (DRCS)**

From the previous section, we find that DRPC instance causes only an increase in the reputation values by considering only the positive scores in the last $v$ contributions. This, as a result, causes an increase in the FP rates and a decrease in the FN rates in most cases of the three sets and thresholds.
Therefore, in this section, we propose an enhanced instance of the aging mode to compute the participant reputation value by Doubling Recent Contribution Scores (DRCS). Unlike DRPC, DRCS method doubles the last $v$ contribution scores of the last $Z$ contributions regardless of the form of the score. Similar to DRPC, DRCS is not practical in the case of newcomer’s mode where the number of participant contributions is less than $y$. Algorithm 4 shows that DRCS is applied in both cases when the number of contributions is less than $Z$ (Lines 4 to 8), as long as they are more than $y$, and more than $Z$ (Lines 9 to 13). The purpose of proposing DRCS is to give a fair influence of the last $v$ contributions on the computation of the participant reputation values.

We implement DRCS by using the same reputation scheme and dataset as in the original RSEP. As well, we assess the experiment results based on the FP and FN rates, the three set sizes and the three thresholds.

Figure 4.5 shows the assessment result comparisons of the original RSEP and DRCS. The overall results show that doubling the most recent contribution scores provides similar FP rates to the original RSEP results. The FN rates, however, are better in RSEP than in DRCS in all cases of set$_2$ and set$_3$ of the three thresholds. In contrary, two cases in set$_1$ with the thresholds of 60% and 80% (Figure 4.5(a) and 4.5(c)), have equal FN rates in both methods. A single case in set$_1$ with the threshold of 70% (Figure 4.5(b)), has a lower FN rate in DRCS than in RSEP. The differences between RSEP and DRCS FN are due to the increase of honest participants whose reputation values are below the thresholds ($H$) in set$_2$ and set$_3$. This increase of the $H$ value is due to the increase of the negative scores caused by doubling the last $v$ contributions, especially for the participants in the honest class.
4.4 Discussion

**Figure 4.5:** The FP and FN rates with three threshold settings for RSEP and DRCS
4.5 Summary

Participatory sensing applications need to verify participant contributions to select useful collected sensor data and enhance the application services. We propose a Reputation Scheme to Evaluate Participants (RSEP), to achieve the participatory sensing needs. RSEP goes through two phases. One selects the most accurate contributions and the other updates participant reputation values. We showed the steps of the first phase by dividing participants into three groups based on their collected sensor data. Then, RSEP evaluates each group using its participant reputation values and selects the contributions of the highest group value. The second phase assigned positive and negative scores to participants based on the accuracy of their contributions. These new scores change the reputation values of the participants in the next contribution.
4.5 Summary

We proposed two additional instances of the aging mode to compute the participant reputation values. The first instance doubles the recent positive scores and the other instance doubles the recent contribution scores whether that score is positive or negative. Both instances aim to give more weight for the most recent contributions in the computation of the reputation value.

The evaluations, based on a real-world dataset, showed that the accuracy level of assessing participants using RSEP is high, as compared to an existing reputation scheme. We used the false positive and false negative rate metrics to evaluate the schemes with three threshold settings on three sets of random participants.

RSEP ensures contribution data trustworthiness by evaluating participant reputation values in a typical participatory sensing environment. When a crisis occurs, however, validating participant contributions becomes crucial and follows the crisis environment nature. Thus, in the next work, we discuss a scheme that verifies the accuracy of a participant’s contributions in crisis situations.
5.1 Introduction

A crisis, by definition, is a situation that has reached an unpredictable critical phase, and an urgent action needs to be taken to disrupt or decrease difficulties [6]. Accidents, fires, earthquakes and floods are examples of crises. They threaten people’s lives and must be dealt with in a timely manner.

A Crisis Response System (CRS) consists of a group of authorities who are trained to deal with such situations [55]. The authorities need accurate data to be able to make appropriate rescue plans and act to resolve the situation. When a crisis happens, some of the data needed pre-exist with the authorities such as the location of forests, lakes, mountains, municipal facilities and routes into and out of the crisis site. However, additional data directly related to the crisis would be beneficial to make rescue plans. This data could be generated by individuals who are within the close proximity to the crisis and gathered by an application that can deliver this data to the CRS.
5.1 Introduction

Since participatory sensing consists of participants, an application server and a receiver [1], participants sense their surrounding environment using their handheld sensor devices, then send the sensor data to an application server. The server analyzes the received data and shares the final results with the CRS [56].

CRS, on the one hand, requires all available data to reach its optimal performance. On the other hand, the participatory sensing application usually accepts sensor data from the public which raises the challenge of participant contribution trust; what data is accurate and what data is not. Therefore, the participatory sensing application needs to verify the accuracy of contributions before sending the data to the CRS.

To overcome this challenge, we propose a Participant Contribution Trust scheme (PCT). PCT aims to provide trusted sensed data by filtering the inaccurate contributions out from the accurate contributions. PCT compares contributions from different locations at the crisis site to confirm the accuracy of one another. It also computes participant reputation values to be used in selecting the highly reputed participants.

PCT consists of three major stages: (1) dividing the affected crisis area into multiple sectors, (2) filtering participant contributions and (3) updating participant reputation values. As well PCT is a viable CRS solution for various environmental conditions such as fire disaster, radiation measurement, wind speed, humidity and air quality.

Contribution trust is essential for participatory sensing applications to provide better services. Trust can be verified by measuring the accuracy of a participant’s contributions using reputation systems and contributions confirmation, that can be done by comparing theirs with the contributions made by other participants.
5.1 Introduction

Contribution trust has been studied in the CRS [51, 47, 57]. Tundjungsari and Yugaswara [51] proposed a scheme to collect data and distribute information among the CRS authorities. The scheme distinguishes the good sensor data by applying a reputation system on their participants. The scheme distributes the information of the reputed participants to minimize the time wasted downloading the poor quality information. Tan et al. [47] proposed a trust model to evaluate participants in emergency communications. By using a filtering algorithm, the trust model avoids the untrusted participants by rejecting their contributions to improve the service performance. Conrado et al. [57] produced a data quality measurement framework that is compatible with social networks. This framework manages the uncertainty collected data by participants. It aims to support the CRS authorities with the best available contributions for the rescue plan decision-making process.

In Chapter 4, we proposed the Reputation System to Evaluate Participant (RSEP) scheme [58]. It validates participant contributions using their reputation values. It starts by dividing participants based on the similarities of the contribution values. Then, the system evaluates each group of the participants based on their reputation weights using their members’ reputation values. The highest group weight is the winner, and its participant contributions are the most accurate. At the end of the process, RSEP rewards the winner participants and penalizes the losers. RSEP has similarities to and differences from PCT, which we discuss in Section 5.3.

In this work, we evaluate the proposed PCT on a fire crisis dataset. Around the crisis, multiple participants use their handheld sensor devices to sense the air temperature in degrees during different periods of time and from several locations. The data follows a certain trend. Thus, different locations will have different temperature readings indicating the direction of the fire and its intensity. Then, participants send the collected data to PCT. In addition to the temperature, the
collected data includes metadata such as the participant’s location, date and time. The CRS uses the output of PCT to measure the severity of the disaster and with that information authorities make an efficient rescue plan.

We perform experimental evaluations to assess the accuracy of the proposed PCT, and compare PCT to our previous work (Chapter 4), the RSEP scheme. We show the results of the comparison between the PCT and RSEP schemes.

The remainder of this chapter is organized as follows. Section 5.2 details the proposed participant contribution trust scheme and its related algorithms. In Section 5.3, we describe the experimental evaluation and setup, and discuss the evaluation results. In Section 5.4, we discuss some practical settings and specific considerations of the work. In Section 5.5, we summarize the work.

5.2 The PCT Scheme

In this section, we overview the proposed PCT scheme in Section 5.2.1. Section 5.2.2 details the PCT algorithm. In Section 5.2.3, we briefly discuss the participant reputation value computation. Then, we end this section by explaining the way of dividing the crisis area into sectors in Section 5.2.4.

5.2.1 The PCT Overview

PCT aims to provide trusted contributions by selecting the most accurate sensed data. Then, it sends the accurate data to the CRS. Figure 5.1 shows the data flow starting from the participants’ data collection passing through PCT then onto the CRS. At every epoch, a period of time, participants start the process by sensing the required data using their devices with embedded
sensors. Participants send the sensed data to PCT to filter the data and obtain the most accurately sensed data. Then, PCT sends the accurate sensed data to the CRS. The cycle of PCT goes through three major stages: (1) dividing the entire affected area into smaller sectors, (2) filtering participant contributions and (3) updating participant reputation values.

In stage one, PCT splits the area into multiple sectors by creating multiple zones and four cardinal directions (north, east, south and west) as explained in Section 5.2.4. Each sector belongs to a specific zone and direction, as shown in Figure 5.2. By creating these multiple sectors, the next stage can treat each direction separately.

In stage two, PCT runs a filtration steps in one cardinal direction at a time as outlined in Algorithm 5, Section 5.2.2. Filtering participant contributions passes through two steps: (1) from the outermost sector to the innermost sector, then (2) from the innermost sector to the outermost sector. The order of these two major steps depends on the crisis environment and rescue crew requirements. Through these two steps, PCT computes the Average Sensed Data (ASD) of the High Participant Reputation Values (HPRV) in every sector it passes through. Computing the reputation...
value depends on the participant’s contributions history, as in Section 5.2.3. PCT compares the computed ASD with other contributions of either the same sector (intra-sector) or a different sector (inter-sector). The comparison phase allows the scheme to decouple the Inaccurate Sensed data (IS) from the Accurate Sensed data (AS).

Stage three updates participant reputation values at the end of the filtration task of each direction. When PCT decouples the IS from the AS, it assigns a negative score (ns) to every participant in IS and a positive score (ps) to every participant in AS. These new assignments will
change the participant reputation value either up or down in the next contribution in a different epoch.

5.2.2 The PCT Algorithm

PCT collects contributions from participants in an affected area in every epoch. In Algorithm 5, PCT filters the sensed data in one cardinal direction \((d)\) at a time. The filtration step of one cardinal direction in Algorithm 5 starts from the outermost sector, \(\text{Sector}_{n,d}\), to the innermost sector, \(\text{Sector}_{1,d}\) as in Figure 5.2, to compare participant contributions and keep the accurately sensed data. Then, it reverses the steps from the innermost sector, \(\text{Sector}_{1,d}\), to the outermost sector, \(\text{Sector}_{n,d}\) as in Figure 5.2, to apply extra filtration steps of the remaining participant contributions and gain the most accurate contributions as a final result. PCT, then, updates the participants’ scores for their next contributions.

In the first section of Algorithm 5, the scheme computes \(\text{ASD}_j\) of \(\text{HPRV}_j\) of \(\text{Sector}_{j,d}\) and compares it with all participants in \(\text{Sector}_{j-1,d}\), where \(j = \{n, \ldots, 1\}\). This inter-sector comparison filters out some of the inaccurate contributions in \(\text{Sector}_{j-1,d}\) by checking if the sensed data of \(i\)-th participant \((S_i)\) is greater than or equal to \(\text{ASD}_j\). Any contribution which passes the condition is added to the Filtered Sensed data group of \(\text{Sector}_{j-1,d}\) \((\text{FS}_{j-1})\), Line 8. On the contrary, any contribution which does not pass the condition is added to the Inaccurate Sensed data group of \(\text{Sector}_{j-1,d}\) \((\text{IS}_{j-1})\), Line 9. In the next sector \((\text{Sector}_{j-1,d})\), the scheme computes \(\text{ASD}_{j-1}\) of \(\text{HPRV}_{j-1}\) of only those who were added to \(\text{FS}_{j-1}\) in the previous comparison. PCT keeps applying the same steps to all the sectors until it reaches the innermost sector.

At the innermost sector, \(\text{Sector}_{1,d}\), the scheme compares \(\text{ASD}_i\) of \(\text{HPRV}_i\) with all participants in \(\text{FS}_i\) (Line 26). The condition (Line 27) of this intra-sector comparison accepts the sensed data
5.2 The PCT Scheme

Algorithm 5 - Participant Contribution Trust (PCT)

Input: Participant Contributions

Output: Trusted Contributions

1. Get $P$ Reputation Value // Section 5.2.3
2. Get $P$ Sector // Section 5.2.4

From Outermost Sector to Innermost Sector
3. for $j \leftarrow n$ to 1 do
4. compute $ASD_j$ of $HPRV_j$

Compare $ASD_j$ with each $q$ of $Sector_{j-1,d}$ // inter-sector
5. if $j > 1$,
6. then for $i \leftarrow 1$ to $|Sector_{j-1,d}|$ do
7. if $q_i \geq ASD_j$
8. then add $q_i$ to $FS_{j-1}$
9. else add $q_i$ to $IS_{j-1}$
10. $Sector_{j-1,d} \leftarrow FS_{j-1}$
11. else $a \leftarrow 1$ and Call Intra-sectora Comparison Function

From Innermost Sector to Outermost Sector
12. for $j \leftarrow 1$ to $n$ do
13. compute $ASD_j$ of $AS_j$

Compare $ASD_j$ with each $q$ of $FS_{j+1}$ // inter-sector
14. if $j < n$
15. then for $i \leftarrow 1$ to $|FS_{j+1}|$ do
16. if $q_i \leq ASD_j$
17. then add $q_i$ to $AS_{j+1}$
18. else add $q_i$ to $IS_{j+1}$
19. Send $q_i$ of $AS_{j+1}$ to the CRS
20. else $a \leftarrow n$ and Call Intra-sectora Comparison Function

Update Participants Reputation Scores
21. for $j \leftarrow 1$ to $n$ do
22. for $i \leftarrow 1$ to $|AS_j|$ do
23. $p_{si} \leftarrow p_{si} + 1$
24. for $i \leftarrow 1$ to $|IS_j|$ do
25. $n_{si} \leftarrow n_{si} + 1$
5.2 The PCT Scheme

**Intra-sector Comparison Function**

Compare \( ASD_a \) with each \( q \) in \( FS_a \)  

\[
\text{for } i \leftarrow 1 \text{ to } |FS_a| \text{ do}
\]

26. if \((ASD_a + (ASD_a \times u)) \geq q_i \geq (ASD_a - (ASD_a \times u))\) then 
27. add \( q_i \) to \( AS_a \)
28. else add \( q_i \) to \( IS_a \)
29. Send \( q_i \) of \( AS_a \) to the CRS

within an upper and lower percentage \( u \) of \( ASD_i \). Those who pass the condition are added to \( AS_i \) (Line 28). On the contrary, those who do not pass the condition are added to \( IS_i \) (Line 29).

In the second section of Algorithm 5 (Line 12), the scheme applies the same steps as in the first section with minor differences. Unlike the first section, the scheme computes \( ASD_j \) of the contributions in \( AS_j \) that reflects the accurate contributions of \( Sector_{j,d} \). The main purpose of this section is to apply an extra filtration step by applying the opposite condition of the first section (Line 16). As a result of applying the condition in Line 16, the scheme gets \( AS_j \) and \( IS_j \) of all sectors until it reaches the outermost sector.

At the outermost sector, \( Sector_{n,d} \), the scheme applies the \textit{intra-sector} comparison function to filter out the inaccurate contributions within the \( Sector_{n,d} \) and gets \( AS_n \) and \( IS_n \).

The scheme sends all the sensed data in \( AS_j \) of each epoch to the CRS (Lines 19 and 30) as the most trusted contributions by PCT.

Finally, the PCT algorithm updates participant reputation values based on the accuracy of their contributions (Lines 21 to 25). Every accurate participant’s contribution belongs to \( AS_j \) receives an extra \( ps \) (Lines 22 and 23). On the contrary, the rest of the participants that belong to \( IS_j \) receive an extra \( ns \) (Lines 24 and 25). Those new \( ps \) and \( ns \) scores affect the participant reputation value in the next contribution either positively or negatively based on the extra score it receives.
5.3 Experimental evaluation

5.2.3 Reputation Value Computation

Participant reputation values ($r_v$) reflect their trustworthiness which plays a major role in allowing the scheme to make a selection decision of $HPRV$. Computing the reputation value depends on the participant’s contributions history. We, in this section, use the same method used in Chapter 4 by applying the steps of Algorithm 2 to compute participant reputation values.

5.2.4 Crisis Area Sectors Division

Dividing the crisis area into multiple sectors allows PCT to have a more accurate measurement. In Algorithm 6, the scheme determines a Participant Location ($PL_i$, $i = \{1, ..., m\}$ by checking its position to the zones. The scheme centers the crisis location, $R_0$, and creates $n$ zones by considering radius $R_j, j = \{1, ..., n\}$, that takes on a shape of nested circles (Lines 2 to 4) as shown in Figure 5.2.

The innermost zone, $Zone_1$, is the closest to the crisis and the outermost zone, $Zone_n$, is the closest to the nature condition. Next, the scheme splits the map into the four cardinal directions by creating two ordinal direction lines from the northwest to the southeast and from the northeast to the southwest. The main purpose of splitting the area into the four cardinal directions is to allow the CRS to better estimate the movement direction of the crisis. As a result, the scheme creates $n$ sectors in each direction and determines the participants of each sector (Lines 5 to 8), where $Sector_{j,d}$ refers to the sector in $Zone_j$ and $direction_d$.

5.3 Experimental evaluation

In this section, we discuss PCT experimental evaluation results. We review the implementation setup and evaluation environment in Section 5.3.1. Section 5.3.2 explains the dataset we use in the
5.3 Experimental evaluation

Algorithm 6 - Crisis Area Sectors Division

**Input**: Participant Location and Time

**Output**: Participant Sector

**Get Participant Zone**
1. for $i \leftarrow 1$ to $m$ do
2. \hspace{1em} for $j \leftarrow 1$ to $n$ do
3. \hspace{2em} if $R_{j-1} < PL_i \leq R_j$ \hspace{1em} \// $R_0$: Crisis (Centre)
4. \hspace{2em} then Add $P_i$ to Zone$_j$

**Determine Participants in Sectors**
5. for $j \leftarrow 1$ to $n$ do
6. \hspace{1em} for $i \leftarrow 1$ to $|\text{Zone}_j|$ do
7. \hspace{2em} if $PL_i \in \text{Sector}_{j,d}$
8. \hspace{2em} then Add $P_i$ to Sector$_{j,d}$

implementation. Section 5.3.3 discusses the evaluation metrics to assess the accuracy and precision of the PCT results.

5.3.1 Evaluation Environment

The PCT scheme is intended to use on a dataset collected by a group of participants who are within the vicinity of the crisis (dataset detail is in Section 5.3.2). Each record in the dataset represents a contribution of a participant. The participant collects sensor data, includes its metadata such as participant location, date and time, and sends them to PCT. This action continues by participants from all sectors to the end of the collection epoch. PCT receives all the contributions by the end of the epoch and then applies the steps of locating participants and filtering their contributions as described in Section 5.2. The objective of the scheme is to filter the data to only have the most accurate contributions to send to the CRS. As the last step of the evaluation
5.3 Experimental evaluation

environment of PCT, it applies a reward/penalty mechanism to all participants based on their contribution accuracy.

5.3.2 Dataset

Due to the lack of real-world data collected from handheld sensor devices of an actual crisis, we generated our dataset. In the dataset, we assume a crisis at a randomly selected location and generate random dynamic participants located within a certain distance from the crisis. Participants use their smartphones’ sensors to collect sensor data in addition to spatiotemporal data such as location, date and time.

A fire crisis is our use case. We center the crisis and generate a heat map by creating four heat levels around the crisis. In such situations, data follows a certain trend. Therefore, the closer the level to the crisis, the higher the temperature range. We consider an area of a radius of 1.5 km from the crisis. The dataset consists of 500 participants contributing for eight days. The data collector operates 24 hours a day and collects data every 30 minutes (epoch). In every epoch, we have a different number of participants that are randomly selected. Since participants are mobile, participant positions may change in different epochs. The sensing temperature values range between 10 and 90 degrees Celsius\textsuperscript{6} that depends on the participant’s heat level.

Participants are randomly distributed in the considered area. We generate a temperature value for every participant in a certain epoch by applying Gaussian distribution\textsuperscript{7}. In every run, we assign a mean ($\mu$) and standard deviation ($\sigma$) as required parameters for Gaussian Function. The mean value ($\mu$) corresponds to the ground truth temperature for every level in every epoch. For every

\textsuperscript{6} Typical smartphones cannot function in temperatures above 90 degree Celsius.

\textsuperscript{7} We followed the temperature value generator function in Chapter 4.
5.3 Experimental evaluation

participant, we assign a fixed error range ($\delta$) that remains the same in all of its contributions. For the sake of measuring the success of the scheme, we randomly classify participants into three groups: (1) honest, (2) dishonest and (3) misleading. Honest participants usually sense accurate temperatures with a 10% error range from the ground truth. Honest group consists of 50% of all participants. Dishonest participants usually sense inaccurate temperatures with error range between 10% and 30% from the ground truth. This group consists of 25% of all participants. Misleading participants, the last 25% of all participants, sense accurate or inaccurate temperatures based on the data generator function decision. In the results of the scheme, this group plays a major role because of the inconsistency of its contribution accuracy.

5.3.3 Experiment Results

Since we have generated the dataset and predetermined honest and dishonest participants, we can take advantage of this and measure the accuracy and precision of PCT. In addition to filtering participant contributions, PCT evaluates participants by rewarding the accurate contributions with positive scores and the inaccurate contributions with negative scores, which will impact the reputation value of the participants. Hence, we measure the results of PCT using the two metrics discussed in Chapter 4 that are False Positive (FP) and False Negative (FN) rates in addition to precision and recall rates.

FP rate is the ratio of the participants whose reputation values are above the threshold while they are originally classified as dishonest. FN rate is the ratio of the participants whose reputation values are below the threshold while they are originally classified as honest. The threshold is the percentage that is applied to the participant reputation values to distinguish honest from dishonest participants. Thus, low FP and FN rates mean that the PCT scheme assessment is highly accurate.
5.3 Experimental evaluation

On the other hand, precision rate is the ratio of the honest participants whose reputation values are above the threshold to all the participants whose reputation values are above the threshold. We define the recall rate as the ratio of the honest participants whose reputation values are above the threshold to all the participants of all the classes. Thus, high precision rate means that the PCT scheme assessment returns significantly more relevant honest participants than dishonest participants, while high recall rate means that the PCT scheme assessment returns most of the relevant honest participants.

We set the threshold into three values: 70%, 80% and 90% to assess PCT results accuracy and precision. We produce three sets with different sizes of participants to evaluate PCT using the proposed metrics. \( \text{set}_1 \) and \( \text{set}_2 \) consist of 100 and 250 randomly selected participants, respectively, while \( \text{set}_3 \) consists of all 500 participants. To evaluate the PCT results, we measure FP, FN, precision and recall rates by applying each threshold on the three sets as in Eq. 4.4, Eq. 4.5 (in Chapter 4), Eq. 5.1 and Eq. 5.2, respectively:

\[
\text{Precision}_c = \frac{T_c}{|\text{subset}_c|} \quad (5.1)
\]

\[
\text{Recall}_c = \frac{T_c}{|\text{set}_c|} \quad (5.2)
\]

where, \( T_c \) (a.k.a. True Positives (TP) number), \( c = \{1, 2, 3\} \), is the total number of honest participants whose reputation values are above the threshold in a set. \( \text{subset}_c \) is the total number of participants whose reputation values are above the threshold in \( \text{set}_c \).
5.3 Experimental evaluation

From the analysis of the PCT results, we find that the total number of participants whose reputation values are above the threshold \((\text{subset}_c)\) in set\(_1\), set\(_2\) and set\(_3\) are 62, 167 and 318, respectively, with a threshold of 70%. The FP rates are 3%, 7% and 5%, and the FN rates are 3%, 2% and 1% for the three sets, respectively. The FP rate of set\(_1\) is 3% because of two participants who have been classified as dishonest and their reputation values are above the threshold. On the contrary, the FN rate of set\(_2\) is 2% because of two participants who have been classified as honest and their reputation values are below the threshold. In addition, the precision rates are 97%, 93% and 95%, and the recall rates are 60%, 62% and 61% for set\(_1\), set\(_2\) and set\(_3\), respectively. The precision and the recall rates of set\(_3\) are 95% and 61%, respectively, due to 303 true positive participants (out of 318) for precision and 500 for recall, who have been classified as honest and their reputation values are above the threshold of 70%.

With a threshold of 80%, the FP rate are 2%, 4% and 3%, and the FN rates are 7%, 5% and 2%, for set\(_1\), set\(_2\) and set\(_3\), respectively. The precision rates are 98%, 96% and 97%, and the recall rates are 58%, 61% and 60% for the three sets, respectively.

With a threshold of 90%, the FP rate are 0%, 2% and 1%, the FN rates are 9%, 8% and 6%, the precision rates are 100%, 98% and 99%, and the recall rates are 57%, 59% and 58% for set\(_1\), set\(_2\) and set\(_3\), respectively, as shown in Figure 5.3 and Figure 5.4.

We compare PCT with our previous work RSEP (see Chapter 4), to distinguish the accuracy and precision levels of their results. We implement RSEP on the dataset of this chapter to get reasonable results and fair comparison. Then, we analyze the results based on FP, FN, precision and recall rates to evaluate the accuracy and precision of the scheme results. The selection of RSEP for the comparison is due to the similarities in its features with PCT. However, the methodology that RSEP uses to reach the target results is different, in addition to the environments that it can be applied for.
5.3 Experimental evaluation

RSEP aims to provide accurate contributions to end users. It is designed to deal with participant contributions participating for an application service. RSEP evaluates those contributions using their participant reputation values. It then sends the accurate contributions to the application service. At the last step, RSEP rewards/penalizes participants based on their contribution accuracy.

The two major differences between PCT and RSEP are: (1) the process of evaluating the contributions and (2) the RSEP limitation of receiving the contributions from one sector at a time.

Relating to the former difference, when RSEP receives the contributions from participants, it divides the participants into multiple groups based on the similarities of their contribution values. Then, it evaluates each group by computing the total reputation value - derived from the group’s individuals’ reputation value. The highest group value is the winner to send its contributions to the application service. Unlike RSEP, PCT compares participant contributions across other sectors to filter contributions due to the crisis nature where data follows a certain trend.

Relating to the second difference, RSEP can only treat the contributions that originate from a single sector at a time. This limitation could lower the accuracy of the contribution evaluations due to the lack of comparing existing contributions with others from neighboring sectors.

We applied the same settings to RSEP by creating the same three set sizes (100, 250 and 500) and three threshold values (70%, 80% and 90%). In the comparison, the lower the FP and FN rates, the better the accuracy. In Figure 5.3(a), for example, when the threshold is 70%, the FP rates in PCT are 3%, 7% and 5%, and the FN rates are 3%, 2% and 1%, for set1, set2 and set3, respectively. On the contrary, the FP rates in RSEP are 5%, 8% and 8%, and the FN rates are 6%, 2% and 3%, for set1, set2 and set3, respectively. The RSEP higher FP rates are due to the higher $D_C$ number of...
5.3 Experimental evaluation

Figure 5.3: The FP and FN rates with three threshold settings for PCT and RSEP
participants who have been classified as dishonest and their reputation values are above the threshold. For example, the RSEP FP rate of set_3 is 8% is due to 26 $D_3$ participants among 334 participants, while the PCT FP rate is 5% due to 15 $D_3$ participants among 318 participants. Similarly, FN rates are higher in RSEP due to the higher $H_c$ number of participants who have been classified as honest and their reputation values are below the threshold.

Furthermore, the higher the precision and recall rates, the better the precision in assessing participants. For instance, in Figure 5.4(b), the threshold is 80%, the precision rates in PCT are 98%, 96% and 97%, and the recall rates are 58%, 61% and 60% for set_1, set_2 and set_3, respectively. On the other hand, the precision rates in RSEP are 98%, 94% and 94%, and the recall rates are 60%, 61% and 60% for set_1, set_2 and set_3, respectively. The RSEP lower precision rates are due to the lower $T_c$ number of participants. For example, the RSEP precision rate of set_3 is 94% due to 302 $T_c$ participants among 321 participants, while the PCT precision rate is 97% due to 300 $T_c$ participants among 310 participants.

Considering participant contributions from one sector at a time limits RSEP to assess these contributions by using participant reputation values only. This limitation decreases the evaluation accuracy and precision; thus, it causes higher FP and FN rates and lower precision rates in most cases of the comparison with PCT. In contrast, assessing participant contributions by comparing them with other intra and inter-sector contributions gives PCT an advantage of better evaluation accuracy and precision. The contributions comparisons are applied in two directions, from the outermost to the innermost sectors and vice versa. Consequently, the results of the comparison (Figure 5.3 and Figure 5.4) show that PCT has a better performance than RSEP with respect to FP, FN and precision rates.
5.3 Experimental evaluation

Figure 5.4: The Precision and Recall rates with three threshold settings for PCT and RSEP
5.4 Practical Settings

In this section, we discuss the practical settings and considerations of this work. In Section 5.4.1, we discuss the case when a crisis moves from one position to another. Section 5.4.2 reviews the case when multiple crises occur close to each other and at the same time.

5.4.1 Crisis Move

The crisis area is divided into multiple sectors and split into the four cardinal directions by creating two ordinal direction lines from the northwest to the southeast and from the northeast to the southwest. By collecting participant contributions from all sectors around the crisis and applying the PCT scheme to get the accurate contributions, the analysis of the sensed data can provide the information of each direction and the most affected directions by the crisis. Thus, one of the main purposes of splitting the area into the four cardinal directions is to allow the CRS to better estimate the direction the crisis is moving towards, which can be caused by winds, land slopes, roads, etc. PCT is able to adapt its map when the crisis moves by creating new zones and sectors through the PCT sector division function. The map adaptation can be applied with every epoch run.

In the case of fire crisis, as in our case study, the CRS can estimate the fire direction move, if applicable, from the analysis of the temperature degrees collected by the participants. The highest heat areas may indicate the direction the crisis is moving to. The possible reasons for the fire to move can be one or a combination of many sources such as winds, forest, a chain of houses and vehicles, flammable materials, etc.

Figure 5.5 shows an instance of a fire moving in an easterly direction and how the PCT scheme adjusts its zones and sectors to follow the crisis and give better estimations of the affected areas.
5.4 Practical Settings

5.4.2 Multiple Crises

In the case of multiple crises occurring in a region, PCT can treat each crisis situation separately. The CRS is able to measure the overall situation by receiving the PCT scheme results for each crisis. The PCT sectors division function (Section 5.2.4) centers each crisis location and draws its map by creating multiple sectors and directions. This will allow PCT to control the filtration steps and extract the most accurate contributions of each crisis situation separately.

Figure 5.5: Multiple maps for the same fire crisis moving toward the east direction
5.4 Practical Settings

In the fire crisis use case, when a participant travels from one area of a crisis, say A, towards another crisis, say B, the participant sensed data will vary. The sensed data will change, for instance, from severe, in the case of being close to the center of the crisis A, to cool, then back to severe when the participant becomes closer to the center of the crisis B. Figure 5.6 shows an instance of two fire crises occurring next to each other with a traveling participant from one crisis to the other through different heat levels.

When the Average Sensed Data (ASD) values of the High Participant Reputation Values (HPRV) of the outer sectors are gradually increasing, this could be an indication of overlapping

![Figure 5.6: Diverse heat levels between two crises in the same region](image-url)
5.5 Summary

sectors of another fire crisis in that direction, as shown in Figure 5.7(b). In such a case, the PCT scheme can decrease the zones radii of the crisis situation A to avoid the overlapping sectors with crisis B, as shown in Figure 5.7(c). The same steps apply to the crisis situation B. Avoiding overlapping sectors by minimizing zones radii will allow PCT to better control the filtration steps of each crisis separately.

In the case of two crises becoming very close to each other, sectors will definitely overlap. The PCT scheme may not provide the expected results especially when the number of contributions will gradually decrease in the areas between the crises. In this case, PCT maximizes the zones radii to be one larger crisis, as shown in Figure 5.7(d).

As discussed earlier, at the end of each epoch run, the PCT scheme sends the accurate contributions to the CRS. By receiving contributions for multiple crises, the CRS can measure the severity of the crises, how close or far away they are from each other and into what direction each crisis is heading.

5.5 Summary

Allowing individuals to contribute to crisis response systems is essential for better understanding the crisis and making rescue plans. Since those contributions are received from distinct participants, we proposed the PCT scheme. The goal of PCT is to provide trusted sensed data by eliminating the inaccurate ones, and keeping only the accurate contributions. PCT goes through three stages to achieve this: dividing the crisis area into multiple sectors, filtering participant contributions, and updating participant reputation values. Dividing the area into sectors addresses the fact that different sectors have different sensing levels. This allows the scheme to have a better assessment in treating those distinct contributions. Filtering participant contributions
5.5 Summary

Figure 5.7: Two crises toward each other

takes place by comparing contributions with other *intra* and *inter-sector* contributions to confirm the accuracy of the sensed data. Through this step, the scheme eliminates the inaccurate contributions during the comparison. Participant reputation values are updated by assigning positive and negative scores to participants based on their contribution accuracy. These new scores change the reputation values of the participants in the next contribution.

To evaluate PCT, we compared it to RSEP based on false positive, false negative, precision and recall rates. The experimental results showed that PCT provides a higher detection rate for
5.5 Summary

eliminating inaccurate contributions resulting in the delivery of the most accurate data to the crisis response system.

During the implementation of the PCT scheme, we took into consideration two practical settings that we discussed in this chapter. In the case of the crisis move, PCT adjusts the crisis map in every epoch to fit the scheme’s requirements. The multiple crisis occurrences in the same region can be solved by minimizing the radii of the zones and treating each crisis separately; or merging the multiple crises into one bigger crisis.

Participants are the data producers in the participatory sensing applications. The participants’ data such as identity and location, in addition to the sensed data, are essential to the PCT scheme to validate participant contributions. Participants, however, may not be comfortable to share those data publicly for their privacy. In crisis situations, the case becomes more complicated when participants are at risk. Therefore, the next work proposes a scheme that provides levels of privacy and categories of recipients based on the status of participants.
6.1 Introduction

In recent years, devices such as smartphones and tablets are increasingly being equipped with various embedded sensors such as camera, microphone, GPS, proximity, accelerometer, temperature and humidity \[1\]. These sensors enable a wide range of applications in Participatory Sensing (PS). PS allows the users of these devices to participate by sensing and collecting data from their surrounding environment and sending them to the application server.

Participants’ contributions enhance the PS application services for the end users. These contributions become crucial when the application collects data about a crisis. A crisis such as fires, earthquakes and floods needs an urgent action to be taken to disturb its difficulties. A crisis PS application can be a major source of information for a Crisis Response System (CRS). CRS consists of a group of authorities who are trained to deal with such situations \[55\]. In addition to the basic pre-existing data at CRS, authorities need data, through the PS applications, that are directly related to the crisis and individuals who are within close proximity to the crisis to make rescue plans.
6.1 Introduction

Data collected from participants including location, time, contacts, etc. are significant to the CRS and are considered private to the participants. Protecting participant privacy, on the one hand, is essential to encourage them to contribute in such applications. On the other hand, data accuracy is vital to execute CRS optimal performance. Therefore, balancing the privacy-accuracy trade-off is challenging especially that participants may become at risk and lose their lives.

To overcome this challenge, we propose a Context-Aware Privacy (CAP) scheme. CAP aims to provide privacy-preserved data to authorized recipients based on the status of participants. Different recipient categories receive a different level of participants’ private data.

CAP consists of two major components: (1) context-aware scheme and (2) privacy scheme. The context-aware scheme decides what and how much private data to release to recipients. The privacy scheme protects participants’ private data to a certain level based on the context-aware scheme decisions. It applies a manipulated Differential Privacy (DP) function [42] before sending the data to recipients.

CAP is a viable CRS solution for various environmental conditions such as fire disaster, radiation measurement and air quality. As well, it is compatible with multiple types of private data and recipient categories.

We evaluate the proposed CAP scheme on a fire crisis dataset. Participants, who are around the crisis, sense the air temperature using their sensor devices from different locations and epochs (time periods). Afterwards, participants send the collected data including the metadata such as the participant’s location, date, time and some personal data to CAP. It then applies its functions to protect participant privacy and sends its output to the application server. Recipients, including CRS, use the available output to measure the severity of the disaster and make an efficient rescue plan.
6.2 Related work

We perform experimental evaluations to assess the success of the proposed CAP scheme in controlling the privacy-accuracy trade-off. The results show that CAP scheme achieves a high level of privacy protection in safe areas. In risk areas/situations, the scheme achieves a higher level of data accuracy than existing privacy schemes.

The remainder of this paper is organized as follows. In Section 6.2, we discuss several related works. Section 6.3 details the proposed context-aware privacy scheme and its related algorithms. In Section 6.4, we describe the experimental evaluation, setup and the evaluation results. Section 6.5 provides more discussions about other possible settings of the scheme. Section 6.6 summaries the work.

6.2 Related work

Protecting participant privacy is important to encourage them to contribute to PS applications. Participant data can be privacy-preserved before being published to the end users. Due to the lack of research discussing privacy schemes in crises, we, in this section, primarily discuss the related work that is proposing privacy schemes including DP in various PS applications.

Participant trajectory and position data in PS applications have been privacy-preserved by DP [43, 44]. Li et al. [43] proposed a differentially private trajectory data publishing scheme to protect the privacy of sensitive areas. The scheme is based on partition-based models to partition the original location universe at each time point into multiple groups. The scheme follows an algorithm to select optimal partitions to apply DP to protect the trajectory privacy. To et al. [44] proposed a scheme to protect the privacy of participant locations in PS applications. They assumed that a trusted third party has access to data sanitized by DP. Thus, the trusted third party can release participant locations to the PS applications in noisy form, according to DP.
6.3 The CAP Scheme

Jin et al. [45] proposed a differentially private incentive scheme that preserves the privacy of each participant’s bid against others including curious participants within the same application. Some PS applications offer a reward to the participant to do a required task as an encouraging step. To win the reward, participants submit their bids that contain some private and sensitive data to be protected by DP.

Chen and Ma [46] proposed a privacy-preserving aggregation scheme to limit PS applications of learning participants’ sensitive data. The scheme applies the concept of DP by adding noise to the sensitive data. Then, it encrypts the noisy data and sends them to the application server. The application server can only learn the sum of the noisy data.

Existing schemes work on satisfying privacy-preserving PS applications. These schemes do not consider crisis situations in protecting participant privacy. As a result, they do not provide different privacy levels in critical situations when data accuracy is more of a concern.

6.3 The CAP Scheme

In this section, we overview the proposed CAP scheme in Section 6.3.1. Sections 6.3.2 and Section 6.3.3 detail the context-aware scheme and the privacy scheme algorithms, respectively.

6.3.1 The CAP Overview

CAP is a scheme that works in critical situations when crises occur. It aims to balance the privacy-accuracy trade-off challenge based on the status of participants. When a participant is at risk, more accuracy and less privacy will be released to recipients, and vice versa. Different recipient categories receive a different level of participants’ private data.
Figure 6.1: The CAP architecture

Figure 6.1 shows the data flow starting from the participants’ data collection passing through the CAP scheme then onto the PS application server. Participants start the process by sensing the required data using their sensor devices. They send the sensed data to CAP to decide what data to release and apply privacy scheme. Then, CAP releases the privacy-preserved data to the PS application server.

In this work, we protect privacy based on both policy and technology protections. Policy protection is by enforcing rules through “rules entity” in the context-aware scheme. Technology protection is by enforcing the privacy scheme on the data that is considered private. Thus, the course of the CAP scheme goes through two major components: (1) context-aware scheme and (2) privacy scheme.
6.3 The CAP Scheme

In the first component, the context-aware scheme decides what participant’s data to release to whom and to what level of privacy protection, as discussed in Section 6.3.2. The context-aware scheme inputs are the participant contribution data and their metadata. Its decision depends on multiple contexts, i.e., participant situations, recipients of the data and a set of policies.

The second component performs three steps on participant data based on the decisions of the first component. Step one removes some data that the first component decides to hide from recipients. This step prevents the selected recipients from accessing that specific participant data. Step two publishes certain data that the first component decides to release in its original format. This step allows the selected recipients to receive those certain data clearly. Lastly, step three applies the privacy scheme on the data that are selected to be privacy-preserved before they reach recipients, as explained in Section 6.3.3.

6.3.2 The Context-Aware Scheme

In Algorithm 7, participant situations, recipient categories and policies are defined based on the application requirements. In every epoch, the context-aware scheme receives contributions from participants in an affected area. Participants’ contributions consist of multiple attributes describing their surrounding environment and themselves.

The context-aware scheme divides the crisis area map into multiple sectors, as shown in Figure 5.2. It centers the crisis location, $R_0$, and creates $n$ nested circle zones by considering radius $R_j$, where $j = \{1, \ldots, n\}$. Then, the scheme splits the map into four cardinal directions (north, east, south and west) to facilitate following crisis directions and locating participants. We follow the sector division methodology as described in Chapter 5. As a result, the scheme acquires $n$ situations ($S_j$). The closer the sector to the crisis, the higher the risk.
6.3 The CAP Scheme

The decision maker entity, within the context-aware scheme (see Figure 6.1), determines participants’ situations based on their proximity to the crisis that can be derived from their location data. The entity forms situation groups by adding a Participant_i (P_i), where i = {1, ..., m}, to its relevant S_j. Then, the decision maker entity applies the predefined rules (Rule_j) onto S_j. Each of these rules considers participant data attributes, participant situations and recipient categories. For example, the j-th set of rules applies to the j-th situation that decides what participant attributes to hide, release or privacy-preserve before sending them to recipients. Each recipient category may receive different types of participant attributes and different level of privacy.

In the end, the context-aware scheme formulates three output decisions of participant data attributes, i.e., totally hide, clearly release and privacy-preserve. It forwards these decisions to the privacy scheme component.

Algorithm 7 - Context-Aware Scheme

**Input:** Participant Contributions

**Output:** Decisions of What to Release to Who

31. Get Participant Situations
32. Get Recipient Categories
33. Get Administrator Policies
34. Get P Attributes

**Decision Maker Entity**

35. for i ← 1 to m do
36. for j ← 1 to n do
37. if PL_i ∈ S_j (radius R_j) then add P_i to S_j
38. for j ← 1 to n do
39. apply Rule_j to S_j
40. Decide “what (participants’) attributes to release to who (recipients)”
6.3 The CAP Scheme

6.3.3 The Privacy Scheme

The privacy scheme component receives the context-aware scheme output decisions to apply them. It applies the three steps of hiding, releasing and privacy-preserving to each situation at a time. Then, it treats recipient\(_k\) (\(C_k\)), where \(k = \{1, ..., h\}\), by checking each participant attribute \((P_{i.a})\) decision, as shown in Algorithm 8. If \(P_{i.a}\) decision is to hide, then the attribute is removed from the published list. If \(P_{i.a}\) decision is to release, the attribute is forwarded to the publisher. If \(P_{i.a}\) decision is to privacy-preserve, a manipulated Differential Privacy (DP) function is applied on the attribute and the privacy-preserved attribute is sent to the publisher. As a result, the scheme sends the publishable attributes to \(C_k\).

In the case \(P_{i.a}\) requires privacy preservation, the privacy scheme applies a manipulated DP function. DP is a promising approach to privacy-preserving data analysis. It is a concept for dataset privacy that learns as much as possible about a group of participants while learning as little as possible about individuals. If an algorithm analyzes a dataset, it can be differentially private if by looking at the output, one cannot tell whether any individual's data was included in the original dataset or not. Thus, regardless of the background knowledge, an adversary with access to the privacy-preserved data will have an equally likely conclusion whether a participant data is in the dataset or not. DP provides strong worst-case guarantees about the harm that a user could suffer from participating in a differentially private data analysis, but is also flexible enough to allow for a wide variety of data analyses to be performed with a high degree of utility [42].

\[
Pr[f(D) \in S] \leq e^\epsilon. Pr[f(D') \in S]
\]  
(6.1)
6.3 The CAP Scheme

A randomized function \( f \) gives \( \varepsilon \)-differential privacy if for all adjacent datasets \( D \) and \( D' \) differing on at most one participant, and all events \( S \subseteq \text{Range}(f) \) [42].

DP requires computing multiple factors, i.e., sensitivity level, maximum difference in an attribute and privacy level, to compute the noise level properly.

**Algorithm 8 - Privacy Scheme**

**Input:** Context-Aware Scheme Decision  
**Output:** Privacy_Preserved Data

1. for \( j \leftarrow 1 \) to \( n \) do  
2.   for \( k \leftarrow 1 \) to \( h \) do  
3.     for \( i \leftarrow 1 \) to \( |S_j| \) do  
4.       if \( P_i.A = \text{Hide} \) then Remove \( P_i.A \) from list  
5.       else  
6.       if \( P_i.A = \text{Release} \) then Send \( P_i.A \) to Publisher  
7.       else Apply DP on \( P_i.A \) and Call Differential Privacy  
8.         Send PP.P_i.A to Publisher  
9.         Send \( P_i \) attributes in Publisher to \( C_k \)

**Manipulated Differential Privacy Function**

**Compute** sensitivity level (\( \Delta f \))

12. \( \Delta f = \max_{D,D'} |f(D) - f(D')| \)

**Compute** maximum difference between two elements (\( E \)) of the same attribute (\( \alpha \))

13. \( \alpha = \max_{1 \leq i \leq m} |(E_i) - (E_j)| \)

**Compute** privacy level (\( \varepsilon_i \))

14. \( \varepsilon_i = \left\lfloor \ln \frac{m \cdot \beta_i \cdot \gamma}{1 - \beta_i} \right\rfloor / \alpha \)

**Compute** noise level (\( b_i \))

15. \( b_i = \frac{\Delta f}{\varepsilon_i} \)

**Compute** LaPlace mechanism

16. \( \text{Lap} (\lambda, b_i) \)
One of the factors is sensitivity level ($\Delta f$). Sensitivity level is the maximum amount of all possible datasets by which the present or absent of a participant can change the outcome [42].

$$\Delta f = \max_{D,D'} |f(D) - f(D')|$$ (6.2)

Another factor is the maximum difference between two participants’ element ($E$) of the same attribute ($\alpha$).

$$\alpha = \max_{1 \leq i \leq m} |(E_i) - (E_l)|, \quad i \neq l$$ (6.3)

The privacy scheme cannot use the same noise level for all attributes due to the differences in the nature of the attribute types. Therefore, the purpose of computing $\alpha$ is to relate the noise level to the attribute range values when applying the distribution function.

Privacy level ($\varepsilon_i$), a.k.a. privacy budget and privacy loss, is a key factor in computing how much noise the scheme needs to add to an attribute to protect participant data privacy. The privacy level is not an absolute measure of privacy but is rather a relative measure. The scheme computes $\varepsilon_i$ as the natural logarithm of the ratio of Eq. 6.1. It is the inverse of the exponential function $e^\varepsilon$ divided by $\alpha$.

$$\varepsilon_i = \left| \ln \frac{m \cdot \beta_i \cdot \gamma_j}{1 - \beta_i} \right| / \alpha$$ (6.4)

where $m$ is the total number of participants in a situation $S_j$ in one epoch. $\beta_i$ is the probability of participant $P_i$ to occur in a certain sector in the current contribution. $\gamma_j$ is a situation degree of danger.
6.3 The CAP Scheme

γ is an assigned value set by the administrator. The purpose of γ is to adjust the privacy level to match the situation critical condition that differs from one to another. Thus, each situation has a same value of γ.

By computing the sensitivity level (Eq. 6.2) and privacy level (Eq. 6.4), the scheme computes the noise level \( b_i \). It is a real number that will be added to the true participant data to achieve privacy.

\[
b_i = \frac{\Delta f}{\varepsilon_i}
\]  
(6.5)

\( \varepsilon_i \) and \( b_i \) have an inverse correlation. The higher the \( \varepsilon_i \), the lower the privacy and the higher the accuracy, which leads to lower noise level \( b_i \). In contrast, the lower the \( \varepsilon_i \), the higher the privacy and the lower the accuracy, which means the higher the \( b_i \).

To add \( b_i \) to the original data, the scheme applies Laplace distribution. It is mainly how wide is the noise to be added to protect privacy.

\[
Lap = (\lambda, b_i)
\]  
(6.6)

where \( \lambda \) is the position that depends on the original data that needs to be privacy-preserved. \( b_i \) is the scale factor that depends on \( \Delta f \) and \( \varepsilon_i \), not on the dataset. The higher the \( b_i \), the flatter the scale, and the lower the \( b_i \), the sharper the scale.
6.4 Experimental evaluation

In this section, we discuss the experimental evaluation of the CAP scheme. Section 6.4.1 reviews the implementation setup and evaluation environment. In Section 6.4.2, we describe the dataset we use for the evaluation. Finally, we discuss the implementation results and the evaluation metrics to assess the success of the scheme in Section 6.4.3.

6.4.1 Evaluation Environment

The evaluation of the CAP scheme uses a dataset by a group of participants who are within the vicinity of a crisis (see Section 6.4.2 for details). The participant contributes by collecting sensor data, location, date and time. In each participant contribution, metadata, i.e., age, gender, height, weight and health condition are included. Participants send their contributions to CAP periodically. Then, CAP applies the steps of the context-aware scheme and the privacy scheme as discussed earlier. Based on the CAP decisions of what data to release and to what level of privacy protection, the publisher component sends the privacy-preserved data to the application server.

6.4.2 Dataset

The overall dataset consists of two parts: sensor dataset and participant dataset. Sensor dataset considers the crisis environment and sensor data, i.e., location, date and time. Participant dataset deliberates participants’ personal data, i.e., age, gender, height, weight and health condition. Our dataset is publicly available on Scholars Portal Dataverse\(^8\) [59].

\(^8\) https://dataverse.scholarsportal.info/dataset.xhtml?persistentId=doi:10.5683/SP2/DIDFP9
6.4 Experimental evaluation

i. Sensors Dataset

Due to the lack of data collected from sensor devices of an actual crisis, we generated the dataset following some of the early steps as discussed in Chapter 5 [60]. In our generated dataset, we randomly assigned the crisis location and the participants located within the vicinity of the crisis.

Our use case is a fire crisis. We generated a heat map by creating three heat levels in a radius of 2 km from the crisis. The dataset contains 250 participants contributing for six days. The data collector gathers the data every 2 minutes (epoch). In every epoch, participants use their smartphones’ temperature sensors to collect sensor data in addition to their location, date and time. In our use case, the temperature is an instance. Participants freely travel from one position to another. Therefore, the number of participants in any given zone differs from one epoch to another due to the absence of some of the participants who are out of the crisis considered range.

We apply a Gaussian distribution to generate a temperature value for every participant in every epoch. In the Gaussian distribution, we assign a mean ($\mu$) that corresponds to the ground truth temperature for every heat level and a standard deviation ($\delta$) that corresponds to the limited possible error of the participant contribution.

ii. Participants Dataset

Metadata, in this work, is the data about participants that do not change frequently. To have such data, we searched for a real-world dataset that contains data about actual people collected by official organizations. Statistics Canada has collected a dataset “Canadian Community Health Survey” (CCHS) in 2014 and published it in 2016 [53]. The CCHS is a survey that collects information related to health status, health care utilization and health determinants for the Canadian population. It relies upon a large sample of respondents and is designed to provide reliable estimates at the health region level [53]. We selected specific attributes to describe the
6.4 Experimental evaluation

participants. These are age, gender, height, weight and health condition. We selected 250 out of thousands of participants in the survey and assigned their data randomly to our 250 participants. The participant dataset eventually has one record to each participant.

To make the dataset more challenging to privacy, we applied two steps that make some participant contributions distinct from others that may cause, with some effort, to re-identify the participants. Re-identifying a participant means that an adversary discloses a participant’s personal data such as identity, location, age, gender, health condition, etc. that meant to be hidden from public.

In the first step, we chose 80 uncommon characteristic participants in the survey (among the selected 250) that are either underweight or obese. We computed the Body Mass Index (BMI) values to obtain the two uncommon characteristics. BMI is a simple index of weight-for-height that is commonly used to classify underweight and obesity in adults. It is defined as the weight in kilograms divided by the square of the height in metres (kg/m$^2$). Based on the World Health Organization (WHO) classification [61], the BMI value of 18.5 and under is underweight and the value of 30 and over is obese. As a result, we had 33 underweight and 47 obese participants in the dataset.

In the second step, for each participant, we assigned a probability of visiting each sector in the map. We allocated random adjacent sectors to each participant and random probability to each sector. In other words, this step attempts to say a participant $P_i$ for example, has 50% probability to be in sector 3N where its home is, and 33% in sector 2N where its work is, etc. This example is to link this step to the real-world participant practices. In the work experiment, however, the scheme uses those probabilities to be a part of computing the privacy level as discussed earlier.
As a result, participants, selected by these two steps, are more vulnerable to be re-identified than others due to their uncommon characteristics and appearance probability in some sectors.

### 6.4.3 Experiment Results

At the end of the CAP process, every publishable data will be sent in either its clearly released (original) or privacy-preserved format. Therefore, we need to consider the consequences that those publishable data may cause regarding protecting participant privacy and rescuing victims. Hence, we evaluate the success of the scheme by measuring: (1) the possibility of re-identifying participants due to releasing some of their data in the original format, and (2) the impact that the privacy scheme may cause to prevent rescuing victims due to hiding full or part of the original data.

*Identification Confidence (IC)* is a metric to measure the confidence level of re-identifying a participant through its published data.

To apply IC, we need to classify all the participant attributes and measure how sensitive each attribute is in the two possible release formats, clearly released and privacy-preserved. As a result, we understand the *quasi-identifier* attributes that may lead to re-identify the participant. A quasi-identifier attribute is an attribute that can be used to probabilistically identify a participant either by that attribute or in a combination with other attributes. Table 6.1 shows all the attributes in the use case and their sensitivity parameters in the two release formats. The proposed sensitivity parameters are high, medium and low. For example, if combining a high sensitive attribute with another high sensitive attribute, the result can lead to a high probability of re-identifying the participant.
6.4 Experimental evaluation

Sweeney\(^9\) et al. [62] found that the probability of re-identifying an individual by combining the quasi-identifiers of the date of birth, gender and full postal code is 87%. By making either the date of birth or full postal code less specific, the probability drops to 44%. Hence, decreasing the number and/or the details of the quasi-identifiers will result in decreasing the probability of re-identifying individuals. Thus, we assign the values of 80, 40 and 10 to the attribute parameters high, medium and low, respectively. These assigned values are used to compute IC that measures the confidence level of re-identifying a participant.

We set two thresholds, 30% and 60%, to decide the probability of re-identifying participants. In this case, a small IC value means good privacy and poor accuracy level, and vice versa. If the IC

<table>
<thead>
<tr>
<th>Data Format</th>
<th>Original</th>
<th>Privacy-preserving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant ID</td>
<td>Hi</td>
<td>Med</td>
</tr>
<tr>
<td>Sensed Data</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Contact</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Location</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Time</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Date</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Age</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Gender</td>
<td>Hi</td>
<td>Med</td>
</tr>
<tr>
<td>Weight</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Height</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Health Condition</td>
<td>Med</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 6.1: Sensitivity parameter attributes in the two release formats

---

9 Latanya Sweeney has made several discoveries and contributions related to identifiability and privacy technologies. Her well known academic work is on the theory of k-anonymity.
6.4 Experimental evaluation

value is equal or below 30% (IC ≤ 30%), then the probability of re-identifying a participant is low, which means the privacy protection is good. If the value is above 60% (IC > 60%), the probability to re-identify a participant is high, which means the accuracy is good. Finally, if the value is between the two thresholds, the probability to re-identify a participant is medium, the privacy and accuracy are fair. Hence, through the evaluation, we consider the IC value as the data accuracy level that is affected by the injected privacy to the attributes.

To compute IC, we take the average parameter values of all publishable attributes for each recipient category in every situation, as shown in Eq. 6.7:

\[
IC_{jk} = \frac{\sum \text{publishable attribute sensitivity parameters}}{\text{total number of publishable attributes}}
\]  

(6.7)

where \(j = \{1, 2, 3\}\) referring to the number of situations that are \(S_1\): high risk situation, \(S_2\): moderate risk situation and \(S_3\): safe situation. \(k = \{1, 2, 3\}\) refers to the number of recipient categories that are \(C_1\): family and friends, \(C_2\): authorities and \(C_3\): journalists and public. Authorities in \(C_2\) are the most important recipient category due to their responsibility for setting rescue plans regardless of the participant situations. Therefore, the application administrator allows more data to be released to this category than others. Family and friends in \(C_1\) come next in releasing data due to the close relationship, then journalists and the public in \(C_3\).

Figure 6.2 shows the use case through the CAP scheme. It presents eleven participant attributes, participant situations, recipient categories and a set of policies. The participant attributes, \(A_1, \ldots, A_{11}\) include the sensor data and the participant metadata. The set of policies is predefined by the application administrator to help the decision maker decide about what data to release and to what
level of privacy protection. Through the set of policies, A represents the clearly release attribute policy, and PA represents the privacy-preserved attribute policy.

Figure 6.3 shows the data accuracy, that is derived from the IC values, for the three recipient categories based on the participant situations. At $S_1$, $C_1$ and $C_2$ receive more accurate data than $C_3$ and the probabilities of the re-identification rates are high at 63%, 63% and medium at 41%, respectively. The medium probability of re-identifying participants for $C_3$ is due to applying the privacy scheme on many of the published attributes.

At $S_2$, the results show that all recipient categories receive less accurate data than in $S_1$ because participants’ status are more comfortable; however, $C_2$ receives more data than the other categories in the same situation. The IC values are medium at 45%, 57% and low at 24% for $C_1$, $C_2$ and $C_3$.

Figure 6.2: The CAP scheme use case
respectively. The reduction of the accuracy is due to the fewer number of attributes that are allowed to be published in both release formats.

Finally, $S_3$ is the most comfortable and safe situation for participants, and the results show that $C_2$ receives more accurate data than the other categories due to the need for data to measure the crisis severity even if the participants are in a safe position. The IC values are the lowest at 33%, 52% and 10% for $C_1$, $C_2$ and $C_3$, respectively, as shown in Figure 6.3, and the privacy level increases due to the lower risk on participants.

From the IC values, we can measure the impact that the privacy scheme may cause to prevent rescuing victims due to hiding full or part of the original data. We can notice that the impact is very low in $S_1$, where the most critical situation is. The probability of re-identifying participants is as high as 63% for $C_1$ and $C_2$, which means that the published data is critically managed to provide more accurate data besides privacy.

In $S_2$, risk reduces to a level that rescuing participants becomes less important. As a result, the published data becomes less accurate and more private than in the previous situation. Consequently, rescuing plans can be affected by this higher attributes privacy level. The IC values become less than 60% to all recipient categories.

When the participants are in $S_3$, safe situation, the published attributes are in their maximum level of privacy. Accordingly, this may cause a negative impact on rescuing victims than in $S_2$. Authorities ($C_2$) including CRS, however, still receives a higher level of data accuracy than the other categories due to the importance of receiving more data about the crisis and possible victims.

As a result, the impact that the privacy scheme may cause to prevent rescuing victims depends on the status of the participants during the contributions. When the participant is in high risk
situation, the impact is low because of releasing many of the participant attributes. In the contrary, when the participant is in a safer situation, the impact becomes higher due to hiding and/or privacy-preserving additional participant attributes.

### 6.5 Discussion

Policies of what data to release, hide or privacy-preserve are predefined by the application administrator. In the use case we consider, a set of policies is applied during the execution of the CAP scheme. Next, in Section 6.5.1, we relax those policies by allowing the recipients to receive more data about the participants due to the critical situations of the environment that we apply our scheme in. In addition, we re-classify the sensitivity parameters of the participant attributes as described in Section 6.5.2. The purpose of these two steps (Sections 6.5.1 and Section 6.5.2) is to

---

Figure 6.3: Data accuracy for three recipient categories based on participant situations
6.5 Discussion

measure how much they may affect on the level of re-identifying participants, and how they may improve the received data about the crisis to help in rescuing possible victims. In Section 6.5.3, we discuss and compare the results of the proposed settings.

6.5.1 Predefine New Policies at The Context-Aware Scheme

Relaxing policies allows more data about the participant to be published in either release formats. This step may add more attributes to be released to recipients, remove attributes from the released data list, change attributes’ rules from clearly release to privacy-preserve, and change the privacy-preserved attributes’ rules to be clearly released to recipients. Any of these conditions may be applied to any category in any situation. Figure 6.4 shows the new relaxed policies in the use case of the CAP scheme.

![Figure 6.4: The use case relaxed CAP policy scheme](image-url)
6.5 Discussion

When an attribute is added to the list of policies of a recipient category, the Identification Confidence (IC) value increases or decreases based on the sensitivity parameter values of the added attribute. The same applies to the other steps of removing or changing the release format of an attribute. Thus, the attribute policy and attribute sensitivity parameter are the main factors at play in changing the data accuracy level by the change of the IC value.

The experimental results of the relaxed polices show similar trends as the original policies (Section 6.4.3) in the IC values with all recipient categories in all crisis situations. Figure 6.5 shows the data accuracy of the original sensitivity parameter attributes on the relaxed policy version of all three participant situations and recipient categories.

In the high risk situation ($S_1$), the probabilities of the re-identification rates do not change for the recipient categories of family and friends ($C_1$) and authorities ($C_2$) because they carry the same rights to receive all the participant attributes in both policy versions, the original and relaxed versions. The probability of the re-identification rate for the recipient category of journalists and the public ($C_3$), however, increases from 41% to 48%. This increase in the IC value is due to the changes of the release format from privacy-preserve to clearly release for two attributes, which causes an increase in the sensitivity parameters of these attributes.

In the moderate risk situation ($S_2$), the policies of publishing the participant attributes change for all three categories. The release format is changed from privacy-preserve to clearly release of one attribute for $C_1$, two attributes for $C_2$ and two other attributes for $C_3$. As well, two additional attributes are added to $C_2$ and $C_3$. Consequently, the probabilities of the re-identification rates are increased from 45%, 57% and 24% in the original policies version to 57%, 62% and 40% for $C_1$, $C_2$ and $C_3$, respectively.
6.5 Discussion

Due to the safe situation in $S_3$, the original policy version is careful in releasing accurate data to the recipient categories. Hence, relaxed policy version adds more attributes to the three recipient categories to allow more data about the crisis and participants. The relaxed policies change two attributes from privacy-preserve to clearly release format for $C_2$. Moreover, three addition attributes are allowed for $C_1$ and $C_3$, and one additional attribute for $C_2$. As a result, the additional attributes for $C_1$ decrease the IC value from 33% in the original policies version to 22%, as shown in Figure 6.5, because they are published in privacy-preserved release format, which carry the lowest sensitivity parameter. The relaxed policies, however, increase the IC value for $C_2$ from 52% to 60%. The additional attributes for $C_3$ do not change the IC values because the attributes are released in privacy-preserved format that have the same sensitivity parameters values of the original version.

As a result of the relaxed policy version, all categories receive higher data accuracy when the situation is in higher risk. $C_2$ still receives the highest data accuracy about the crisis and participants.

![Image](image.png)

**Figure 6.5**: Data accuracy of the original sensitivity parameter attributes on the relaxed policy version

(for three recipient categories based on participant situations)
6.5 Discussion

than the other categories in all different situations. Consequently, the probabilities of the re-
identification rates increase for recipient categories when the situation is in a higher risk. Thus, the
impact that the privacy scheme may cause to prevent rescuing victims is limited to the participant
situation. The higher the risk situations on the participant, the lower the impact; and the safer the
situation, the higher the impact.

6.5.2 Re-classifying Attribute Sensitivity Parameters

Previously, we classified the participant attributes and measured how sensitive each attribute is
in the two possible release formats, clearly released and privacy-preserved. The classification of
the attribute sensitivity parameters depend on the quasi-identifier attributes. Here, we re-classify
some of the participant attributes, as shown in Table 6.2, and compute the new accuracy levels
through the values of IC.

The purpose of the re-classification step is to discover how the sensitivity parameters make
differences in the data accuracy level by the computation of the probability of re-identifying
participants. This step decreases the sensitivity parameters of some attributes from high to medium
sensitivity or from medium to low sensitivity. Lowering a sensitivity parameter of an attribute
means that the attribute has less sensitivity of re-identifying the participant. The new sensitivity
parameters cause a decrease in the IC values of the affected recipient category. In this section, we
apply the new re-classified sensitivity parameters on both versions of the policies, the original and
the relaxed policy versions.

i. The re-classification sensitivity parameters on the original policies version

Figure 6.6 shows the data accuracy level of the new re-classified sensitivity parameter attributes
on the original policy version. In $S_1$, all recipient categories are effected by the re-calssified
attributes. Thus, the probabilities of re-identifying the participant rates are lower than the original attribute classification. The IC values of the re-classified attributes are 52%, 52% and 30% compared to 63%, 63% and 41% of the original attribute sensitivity parameters for \( C_1 \), \( C_2 \) and \( C_3 \), respectively.

In \( S_2 \), two of the categories have lower IC values while one retains the same value as in the original version. \( C_1 \) and \( C_2 \) have the IC values of 38% and 43%, while they are 45% and 57% with the original classification. The policies of \( C_3 \) are not effected by the re-classification step, therefore, the IC value remains the same in both versions.

Normally, the accuracy level is at its lowest level in the safe situation, \( S_3 \). With the re-classified sensitivity parameters, however, the accuracy level becomes lower than the normal cases. This low

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Original</th>
<th>Privacy-preserving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant ID</td>
<td>Hi</td>
<td>Med</td>
</tr>
<tr>
<td>Sensed Data</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Contact</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Location</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Time</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Date</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Age</td>
<td>Hi</td>
<td>Low</td>
</tr>
<tr>
<td>Gender</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Weight</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Height</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Health Condition</td>
<td>Med</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 6.2: Re-classified sensitivity parameter attributes in the two release formats
value applies to $C_2$, as shown in Figure 6.6, because it is the only effected category by the new sensitivity parameters. The IC value of $C_2$ decreases from 52% in the original classification to 36% in this case. The other two categories are not effected by the re-classified parameters; thus, $C_1$ and $C_3$ have the same values as in the original version.

**ii. The re-classification sensitivity parameters on the relaxed policies version**

In this section, we apply the re-classified sensitivity parameters on the relaxed policy version. As discussed earlier in Section 6.5.1, the relaxed policy version has higher IC values than in the original version due to the allowance of more data to be released to the recipient categories. Thus, the relaxed policy version has higher accuracy level. With the re-classified attribute sensitivity parameters, however, the IC values of the affected categories are decreased due to lowering some
6.5 Discussion

of the sensitivity parameters. Figure 6.7 shows the data accuracy of the new re-classified sensitivity parameter attributes on the relaxed policy version.

In the high risk situation, $S_1$, the IC values of the relaxed policy version with the new re-classified sensitivity parameters are 52%, 52% and 36%, while with the original sensitivity parameters are 63%, 63% and 48% for $C_1$, $C_2$ and $C_3$, respectively.

In $S_2$, the probabilities of re-identifying participants, that is the data accuracy level, turn out to be lower than the same probabilities in $S_1$ due to the lower risks in the $S_2$ situation. An additional decrease to the re-identification probabilities happens because of the new re-classification sensitivity parameters. Thus, the IC values in this case are 43%, 49% and 29%, while with the original sensitivity parameters the IC values are 57%, 62% and 40% for $C_1$, $C_2$ and $C_3$, respectively.

![Figure 6.7: Data accuracy of the re-classified sensitivity parameter attributes on the relaxed policy version](image)

(for three recipient categories based on participant situations)
6.5 Discussion

In the last and safest situation, $S_3$, the IC values are 22%, 48% and 10%, while with the original sensitivity parameters the IC values are 22%, 60% and 10% for $C_1$, $C_2$ and $C_3$, respectively, as shown in Figure 6.7. In $S_3$, the only effected recipient category is $C_2$ by two attributes that are transferred from high to medium sensitivity. The other categories retain the same IC values because they do not carry the effected attributes through their policies.

6.5.3 Comparison of the four settings

To measure the data accuracy level by computing the IC values and measure the impact that the privacy scheme may have on successfully rescuing victims, we discussed four different settings, as follows:

1. The original policy version with the original attribute sensitivity parameters, Section 6.4.3.
2. The relaxed policy version with the original attribute sensitivity parameters, Section 6.5.1.
3. The original policy version with the re-classified attribute sensitivity parameters, Section 6.5.2.i.
4. The relaxed policy version with the re-classified attribute sensitivity parameters, Section 6.5.2.ii.

Figure 6.8 shows the comparison results of the data accuracy of all four settings in three participant situations. Since $C_2$, authorities, is the most significant category due to its tasks of creating and controlling rescue plans, the application’s administrator gives $C_2$ more access to the crisis and accurate participant data. Thus, the data accuracy level of $C_2$ are always higher than the other categories in the four different settings. $C_1$, family and friends, comes next in receiving accurate attributes. Then, $C_3$, journalists and public, is the least of receiving accurate data about the participants in the four settings.
6.5 Discussion

On the one hand, lowering the sensitivity parameters of some attributes causes lower IC values, a. High Risk Situation ($S_1$)

b. Moderate Risk Situation ($S_2$)

c. Safe Situation ($S_3$)

Figure 6.8: Data accuracy of all four settings in three participant situations
where IC values depend on the sensitivity parameters of the assigned attributes. Consequently, the IC values in settings 3 and 4 are lower than the IC values in settings 1 and 2, respectively. On the other hand, less strict policies with respect to releasing some data causes higher IC values, which leads to publishing more data about the crisis and participants. As a result, the IC values in settings 2 and 4 are higher than the IC values in settings 1 and 3, respectively.

In some cases, such as $C_j$ in $S_3$ with setting 1 and setting 3, the IC values of a category in one setting are equal to their peers in another setting. This event occurs when the category’s policies of releasing data do not include the affected attributes in both settings.

The differences between the results in the four settings are mainly based on the policies and sensitivity parameters. The stricter the policies, the less the probability of re-identifying participants, and the greater the chance of failure to rescue victims and vice versa. On the other hand, the higher the sensitivity parameters, the higher the probability of re-identifying participants, and the less chance of failure to rescue victims and vice versa.

### 6.6 Summary

Protecting participant privacy is essential to encourage them to contribute in crisis PS applications. Also, data accuracy is necessary to set finest plans by rescue personnel. Therefore, balancing the privacy-accuracy trade-off is challenging especially that participants may become at risk in some situations. We proposed the CAP scheme that aims to provide privacy-preserved data to authorized recipients based on the status of participants. Different recipient categories receive a different level of participants’ private data.

We evaluated the proposed CAP scheme on a use case of a fire crisis. We projected a dataset that includes sensor data and participant profiles. We experimented fours settings of the use case
6.6 Summary

to show different possible results of the proposed scheme. Experimental results showed that the CAP scheme achieves a high level of privacy protection in safe situations, and a higher level of data accuracy than existing privacy schemes in risky situations.
CHAPTER 7

CONCLUSION

In this chapter, we summarise the overall contributions of this thesis, discuss the limitations and assumptions, and present some open problems that can be used as a basis for advancing this research area.

7.1 Summary and Concluding Remarks

The goal of this thesis work was to develop a framework that overcomes the challenge of the privacy-accuracy trade-off for participatory sensing. On the one hand, the participatory sensing application needs to verify that the collected data is accurate, that it is being sensed correctly at the right location and time by the exact participant. On the other hand, safeguarding participant privacy needs to be guaranteed to encourage participants and make them comfortable and willing to contribute.

As an environmental challenge, we considered critical situations in our work. When a crisis occurs, the accuracy-privacy trade-off becomes more complex. In one component of the framework, we managed to filter out the inaccurate contributions and send the remainder to another component where it controlled the accuracy-privacy trade-off.
To reach this goal, we solved three research concerns: (1) ensuring participant contribution data trustworthiness in a PS application, (2) verifying the accuracy of participant contributions in critical situations, and (3) protecting participant privacy in critical situations. The proposed framework (Chapter 3), involved a set of schemes that co-operated to provide a privacy-preserved accurate data for PS applications. Figure 7.1 shows a detailed summary of the framework architecture components and subcomponents.

In Chapter 4, we proposed the Reputation Scheme to Evaluate Participants (RSEP). It showed the ability to provide accurate participant contributions to a PS application in a typical environment. RSEP groups participants based on their contribution similarities, then assesses each group value by computing its participants’ reputation values. The highest group value is the winner of the most accurate contributions that will be sent to the application server. Through the reputation value computation, we considered newcomer participants who do not have a reputation history. We also enabled a function of considering the most recent contributions, called aging, in a participant reputation value computation to reflect the recent behaviour of the participant. As an enhancement of the aging function, we proposed Doubling Recent Contribution Scores (DRCS), a method to give the recent contribution scores higher influence in the reputation value computation. We evaluated RSEP in a manipulated real-world dataset. We then assessed the results by computing the false positive and false negative rates to measure how accurate the scheme is in assessing participants. The scheme showed better rates in assessing honest and dishonest participants than a comparable existing work. From the results, we conclude that the relation between reputation values computation and recent contributions is vital. Since RSEP depends on reputation values in selecting accurate contributions, we found that focusing on the most recent contributions and doubling those scores in the reputation values computation provides better
Figure 7.1: A detailed summary of the framework architecture
results because it reflects the current participant behaviour. In addition, we conclude from the comparison of RSEP with an existing work, which does not apply reward mechanism in its process, that a reward mechanism is an essential factor in controlling the reputation value fluctuation.

In view of a more challenging environment, we considered several crisis situations in the framework. A Crisis Response System (CRS) that is usually controlled by authorities needs accurate data about the crisis to make efficient rescue plans. Therefore, in Chapter 5, we developed a Participant Contribution Trust (PCT) scheme to provide only accurate contributions to the CRS. The PCT scheme splits the affected crisis area into multiple sectors to ease creating rescue plans and assessing the severity of the crisis. In addition to the reputation value computation, the filtration step depends on the contribution comparison from the same sector (intra-sector) and/or different sectors (inter-sectors) to filter out inaccurate contributions from the whole set. The possibility of facing multiple crises and a crisis expanding and moving to a different location were considered in the scheme. We compared the PCT scheme to our previous scheme RSEP. We measured the results of the PCT scheme with respect to the precision and recall rates, in addition to the false positive and false negative rates. The experimental results showed that PCT provides a higher detection rate for eliminating inaccurate contributions resulting in the delivery of only the most accurate data to the CRS. The features of the reputation system, the contribution comparison and the fact that data follows a certain trend in crisis situations give PCT a better opportunity in evaluating the result accuracy and precision.

After we addressed the challenge of selecting the most accurate participant contributions, we worked on safeguarding participant privacy. In Chapter 6, we proposed the Context-Aware Privacy (CAP) scheme. CAP is compatible to work in crisis situations and consists of two sub-
schemes, context-aware and privacy schemes. All inputs into the CAP scheme are assumed to be accurate contributions from the previous components. We showed how the context-aware scheme decides what participant attributes to release, to whom and what privacy level. It depends on participant situations, recipient categories, and lists of policies. It assesses the privacy level based on the risk state of the participant and the type of recipient of the participant data. Thus, the output decisions have three forms: clearly releasing, privacy-preserving or totally hiding the participant attributes. Next, we discussed the modified Differential Privacy (DP) scheme that provides an adapted DP function based on the decisions of the context-aware scheme. Privacy scheme applies the privacy-preserving function on selected participant attributes before sending them to the publisher. We evaluated CAP in a modified dataset that carries two parts, participant personal data and participant contributions about a crisis. We assessed the results by calculating the probability of re-identifying participants by their released data, and the impact that privacy-preserving function may have on preventing rescuing victims due to hiding all or part of the original data. In showing different results for different settings, we relaxed the attribute sensitivity levels and lists of policies. We conclude that the probability of re-identifying participants has a direct relation to the attribute policies and attribute sensitivity parameters, as they are the main two factors involved in allowing sensitive data to be released or saved. Thus, the evaluation results of the four proposed settings showed reasonable differences based on how strict or relaxed their policies and attribute sensitivity parameters were set.

7.2 Limitations and Assumptions

Although we proposed multiple schemes to reach the objective of our research work, some limitations and assumptions exist. For instance, running the proposed schemes in an independent
7.3 Future Work

entity means that no other entities such as participants and application servers have an influence on the processes and results of the schemes. The schemes, however, can be run on either participants or application server machines if the site of running the schemes is secured, trusted and independent. In some cases, in a real-world setting, those features may be available when the application servers are operated by governments, banks, telecom companies, etc.

Another limitation occurred due to lack of a suitable dataset that matched our research characteristics. The required dataset is to carry sensor data in addition to metadata and participants’ data. We overcome this limitation by manipulating a real-world dataset that carries a part of the required data and injecting formally generated data to end up with datasets that satisfy our research requirements.

During crisis situations, we assumed that participant devices are capable to perform their tasks of sensing in any environment. This assumption in real-world crisis situations, however, may not be applicable due to multiple reasons depending on the crisis, such as extreme temperatures and radiation.

Regarding participant contributions, we assume that inaccurate contributions could be caused by multiple factors such as a device sensor malfunction, a participant simulating the sensed data, and an environmental influence. The proposed schemes eliminate the inaccurate contributions regardless of the reason for the poor results.

7.3 Future Work

In this section, we briefly discuss some of the potential future research directions with respect to the core components of this thesis research.
7.3 Future Work

Computing participant reputation values is a major part of the schemes to select the most accurate contributions. Existing methods can be enhanced by adding other factors into the computation formula. Other factors, such as receiving reputation values from other participants/applications who had dealt with existing participants, may provide a more accurate assessment of the participant behaviors. Consequently, this addition into the reputation value computation will enhance the overall performance of trust schemes to validate participant contributions.

In crisis situations, developing a decentralized system for collecting contributions is feasible as a solution to the centralized servers’ availability challenge. Regarding the contribution validation, an area where our work primarily focused on, other methodologies of computing reputation values are required. Thus, implementing an existing decentralized reputation system can be a viable solution in crisis situations by collecting a participant reputation value through other participants. A participant, who is receiving a contribution from another participant, can validate the contribution and assess the reputation value of the sender by asking other neighboring participants who had previous experiences with the sender. The decentralized reputation system will be able to address other issues; therefore, the reputation system can be an alternative solution in the case of the unavailability of servers which may occur in crisis situations.

Different applications may have different reputation systems to compute participant reputation values. In addition, a participant may contribute to different applications, therefore, the participant will have different reputation values. Thus, a universal concept to transmit participant reputation values between applications/reputation systems is required. This concept will face multiple challenges to balance the weights of the reputation values from different applications/systems to
7.3 Future Work

come up with a universal reputation value. Overcoming the challenges of the universal concept will require more cooperation between applications that depend on participant reputation values.

As discussed earlier in the thesis, data accuracy is essential to applications to provide a good quality of service. On the contrary, maintaining privacy can sacrifice data accuracy. For example, some voice-recording-based or photo-based applications may reveal other surrounding people, sounds or faces. Although these applications may have considered participants’ privacy, surrounding people have the right to be protected. As a result, this kind of consideration may add an extra negative impact on data accuracy. Therefore, the privacy-accuracy trade-off needs to be further researched to achieve optimum level of service as an application.


**BIBLIOGRAPHY**


7.3 Future Work


7.3 Future Work


7.3 Future Work


7.3 Future Work


7.3 Future Work


7.3 Future Work


121
7.3 Future Work


7.3 Future Work