Trust Management and Reputation Systems in Mobile Participatory Sensing Applications: A Survey

Hayam Mousa[a,b], Sonia Ben Mokhtar[a], Omar Hasan[a], Osama Younes[b], Mohiy Hadhoud[b], Lionel Brunie[a]

[a] *LIRIS, INSA de Lyon, France, hayam910@gmail.com; {Omar.Hasan; Sonia.Benmokhtar; Lionel.Brunie}@insa-lyon.fr*
[b] *Faculty of Computers & Information, Menoufia University, Egypt, {osama.younes; mmhadhoud}@ci.menofia.edu.eg*

Abstract

Participatory sensing is an emerging paradigm in which citizens everywhere voluntarily use their mobile phones to capture and share sensed data from their surrounding environment in order to monitor and analyze some phenomena (e.g., weather, road traffic, pollution). Interest in participatory sensing systems has arisen from their low deployment cost. However, relying on citizens who share their contributions arises many challenges. Participants can disrupt the system by contributing corrupted, fabricated, or erroneous data. Consequently, monitoring participants' behaviors in order to estimate their honesty is an essential need. This enables to evaluate the veracity and accuracy of participants' contributions and therefore to build robust and reliable participatory systems. Recently, several trust and reputation systems have been proposed to trace participants' behaviors in these systems. This survey presents a study and analysis of existing trust systems in participatory sensing applications. First, we study the nature of participatory sensing applications by surveying existing systems and outlining their common features. Then, we analyze the main vulnerabilities and attacks that can be launched in these systems. Furthermore, we discuss the concept of trust and we introduce a classification of existing trust systems. The two main classes of trust assessment methods (e.g. TPM and reputation) are discussed. In addition, we investigate the adequacy of existing trust systems for participatory sensing applications. Subsequently, we analyze the merits as well as the limitations of each of them, from which we derive an intensive comparative study of these systems. From this study, we clarify that many trust problems have not been solved and many attacks have not been addressed yet in the literature. Finally, we draw the main lines of a research agenda concerning trust management in participatory sensing systems.

Keywords: Participatory sensing, vulnerabilities, trust systems, TPM, reputation

1. Introduction

Everyday, millions of people move around the world carrying a variety of handheld devices equipped with sensing, computing and networking capabilities (e.g., smartphones, tablets, GPS watches) [1]. Both the advancement and widespread of such devices help for the emergence of a new kind of applications called *participatory sensing* [2]. These applications exploit both the mobility of participants and the sensing capabilities of their devices [3]. Consequently, a large mobile sensor network can be opportunistically constructed with much less cost and efforts than it was the case a decade ago.

In participatory sensing, participants capture sensed data from their surrounding environment using a variety of sensors (e.g., GPS, dual camera, microphone, accelerometer, gyroscope, digital compass) embedded in their own devices (e.g., smartphones, smart gears, tablets, music players and in-vehicle sensors). Then, participants share their collected observations with a backend server, which processes the received data to monitor, map, or analyze some incidents or phenomena of common interest.

Participatory sensing applications can be applied to serve many of our daily life needs, including health monitoring (e.g., [4, 5, 6, 7, 8]), traffic monitoring (e.g., [9, 10, 11, 12]), noise monitoring (e.g., [6, 13, 14]), weather monitoring (e.g., [15, 6]), monitoring activities [16, 17, 18, 19, 20], commerce [21, 22], monitoring sports [23], and many other applications [24]. In these applications, participants control the sensing process and take over the responsibility to capture and report their observations to a backend server. However, no restrictions are usually imposed about the participants' experience, concern, trustworthiness, and interest. As a consequence, participatory sensing applications are vulnerable to *erroneous* and *malicious* participants. By erroneous and malicious participants, we mean those who mislead and disrupt the system measurements by reporting false, corrupted or fabricated contributions. Hence, the need arises for protocols that try to detect erroneous participants and deter or mitigate malicious ones.

Among the classical solutions to deal with malicious users is the notion of *trust* [25]. For assessing trust, these systems often aggregate the *reputation* value of individual participants, which is the general opinion of the community about actions performed by the latter [26]. Trust systems have been first studied and applied in different domains such as peer-to-peer networks (e.g., [27]), ad hoc networks (e.g., [28, 29, 30]), wireless sensor networks (e.g., [31, 32, 33]). More recently, trust systems have been applied in participatory sensing. In this context, researchers seek to estimate the trustworthiness of participants' behaviors in order to assess the quality of their contributions [34, 35]. Complementary to reputation-based trust sys-

tems, researchers suggested to equip smartphone sensors with an embedded Trusted Platform Module (*TPM*) [36, 37]. Such module ensures the authenticity of participants' contributions. Furthermore, some TPM based systems can protect data from unauthorized access through applying some authentication and hardware cryptography mechanisms.

In this paper we survey existing research efforts for trust assessment in participatory sensing applications, belonging the the two major categories above, i.e., reputation-based trust systems and TPM-based trust systems.

1.1. Contribution

The contributions of this paper can be summarized in the following points:

- First, we present an overview of participatory sensing, recall a classification of its applications and a classical architecture for sensing campaigns.
- We then analyze the vulnerabilities of these systems and list a set of attacks that were previously defined in the literature. We further propose a threat model that classifies these attacks.
- We recall the definition of trust in the context of participatory sensing and propose a classification of trust systems in this context.
- We thoroughly survey state-of-the-art trust systems for participatory sensing and carry out a multi-criteria comparative study of these systems. We perform this comparison according to different features such as the methodology adopted, the goals reached and the robustness of these systems against attacks.
- Finally, we draw the main lines of a research agenda in trust assessment for participatory sensing applications.

The remainder of this paper is organized as follows. First, we present a study of existing participatory sensing systems and a generic architecture in Section 2. Then, we discuss different threats and define attacks on these systems in Section 3. In Sections 4, we discuss the notion of trust and propose a classification of existing trust systems. In Sections 5 and 6, we present a detailed discussion of the two main classes of trust systems, i.e., TPM and reputation based trust systems respectively. In addition, different classes of the state-of-the-art trust systems are surveyed in Section 7. We then present a comparative analysis of the surveyed systems in Section 8. Finally, we explain open research challenges in Section 9 and conclude this paper in Section 11.

2. Participatory Sensing

Applications. Khan et. al. in [24] classify participatory sensing applications into three main categories: *public*, *personal* and *social* centric participatory sensing. In public sensing application, participants use their mobile phone to collect data and observations about their surrounding environment such as noise, traffic, pollution, etc [38, 6, 9, 39, 40]. Personal sensing applications are those in which the sensing is based on monitoring the participants themselves such as their health status, activities, etc [41, 42, 43, 44, 45]. In social participatory sensing, participants share sensed data with their friends [46], which can provide them higher motivation for contributing their resources to participatory sensing.

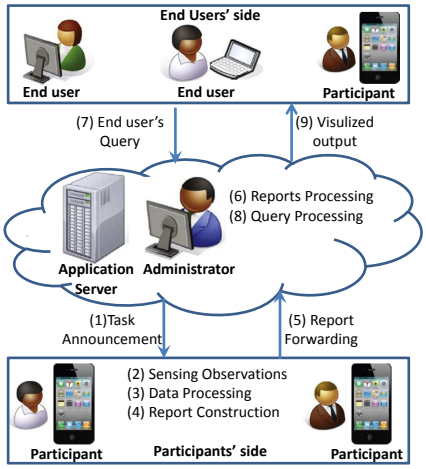

Figure 1: Typical architecture of participatory sensing system

Campaign Architecture. Most of participatory sensing systems mentioned above share the client server architecture presented earlier in [47] and depicted in Figure 1. In this architecture, we can distinguish three main parties: participants (depicted at the bottom of the figure), a campaign administrator (depicted in the middle of the figure) and end users (depicted at the top of the figure). In the following steps, we show how different parties interact to accomplish a sensing campaign according to the architecture in [47]:

1. ***Task announcement*:** The campaign administrator initiates the participatory sensing campaign, manages the campaign and setups the application server. Tasks are then announced to the participants through the application server (step 1).
2. ***Sensing observation*:** Each participant selects one or more tasks and uses his own mobile phone to capture his observations (step 2).
3. ***Reports preparation*:** Once the participant finalizes capturing the required samples, local processing module is carried out on the sensed data (step 3). Local processing summarizes sensed data, extracts some high level information from the data, and/or applies some privacy protection mechanisms. Next, one or more sensing reports are constructed (step 4). Finally, the participant's mobile phone uses the available communication network to send these reports to the application server (step 5).
4. ***Report Processing*:** The received reports are maintained by the application server. Reports received from different participants for the same task are stored in the related

database. Subsequently, reports are processed and analyzed in order to extract the required features and measurements (step 6).

5. ***End user query*:** The end user sends a query to the server (step 7). The server processes the query (step 8), and returns the result to the user (step 9).

3. Vulnerabilities of Participatory Sensing Applications

One of the major limitations of participatory sensing systems is the uncertainty of participants' behaviors. These systems are vulnerable to erroneous contributions as well as to contributions from malicious participants. In the following, we discuss different attacks faced by participatory sensing applications. Then, we propose a threat model to describe how these vulnerabilities may affect the system.

3.1. Attacks on Participatory Sensing Applications

In this section, we present a set of well known attacks in networked applications (e.g, [27, 48, 49, 50, 51]) and discuss how they apply to participatory sensing applications.

- ***Corruption attack***: This attack may arise as a result of a malfunctioning sensor of a participant's device. Adversary can deliberately contribute corrupted or forged data. A local processing module is used by the adversary for modifying the sensed data before sharing it. In addition, an adversary can initiate sensing actions which may corrupt the sensed data by putting his/her phone in non appropriate position.

- ***On-off attack***: In this attack, the adversary alternates between normal and abnormal behaviors. Specifically, the adversary provides false data randomly and irregularly with a probability p, which makes it difficult to be detected. [52, 53, 54].

- ***Re-entry attack***: An adversary who has a low trust level decides to leave the system and to rejoin it using different identification parameters. This attack enables an adversary to contribute low quality or corrupted data and to avoid the consequences for such bad behaviors. This attack is also referred to as *Newcomer* or *White Washing* attack [51, 55, 56].

- ***Discrimination***: This happens when the adversary has two types of behaviors. The adversary provides high quality contribution to one system, and low quality contribution to other systems.

- ***Collusion***: Multiple malicious participants acting together can cause more damage than each acting independently. This attack is referred to as a collusion attack. Malicious colluding participants would provide false, corrupted contributions, and/or false feedback [57]. If the majority of participants collude they can mislead the system measurements and decisions.

- ***Sybil attack***: Some participatory sensing systems apply some authentication mechanisms. However, they can be hacked unless a strong biometric based authentication mechanism is adopted. Thus, a single participant would have the ability to generate multiple pseudonymous identities [58, 35]. Subsequently, an adversary has the ability to submit multiple reports for the same task or to submit many feedback reports for the same participant [59, 58, 35]. This shuffles the system measurements and mislead the trust system decisions. Sybil attack studied earlier in [60, 61, 62, 63]. The difference between Sybil and re-entry attack is that multiple pseudonyms are synchronized to login into the system.

- ***Reputation lag exploitation***: There is usually a time lag between the instant when a sensing report is submitted and the instant when the evolution of this report is reflected on the corresponding trust rating of a participant. Consequently, malicious participants have the chance to contribute corrupted data by exploiting this lag. For instance, a malicious participant initially provides good quality contributions for some period of time in order to gain a high trust rate. Then, participant misuses this trust by injecting the system with corrupted reports [50].

Another set of attack was defined in [64]. These attacks target to tamper with the sensing campaign through reporting inaccurate location information. These attacks refereed to as *GPS spoofing* attacks. The adversaries spoof their locations on the phone by using some applications (e.g. FakeLocate). Then, they report false information by letting the participatory sensing application know that they are in the sensing area, when in reality they are not [65, 66].

- ***No-knowlege (NK) attack***: The adversary has no knowledge about the sensing area. Thus, the adversary submits random data beside a fabricated GPS location data.

- ***Partial knowledge (PK) attack***: The adversary has some information about the sensing area. For each task, the adversary submits incorrect data with probability p beside a fabricated GPS data.

- ***Seesaw attack***: The adversary also has a partial knowledge about the sensing area. First, the adversary starts by submitting correct data to get high reputation score. Then, she submits incorrect data for a period of time T_i and then correct data for a period of time T_{i+1}. The adversary repeats this scenario to keep his reputation score within acceptable level.

The previous attacks can all be implemented to affect either the application or the reputation system. The following attacks target only the reputation system. Thus, they usually have an indirect effect on the application measurements:

- ***Unfair ratings***: The adversary rater does not report the actual feedback which reflects his genuine opinion about the participant [50, 67, 68, 69, 70].

- ***Bad mouthing attack***: This attack arises when the rater provides a negative feedback rating for a trusted participant. This attack is also referred to as *false accusation* attack [71, 72].
- ***Ballot stuffing attack***: The adversary may assign a positive feedback to badly behaving participants. This attack is also referred to as *false praise* attack [32, 73].

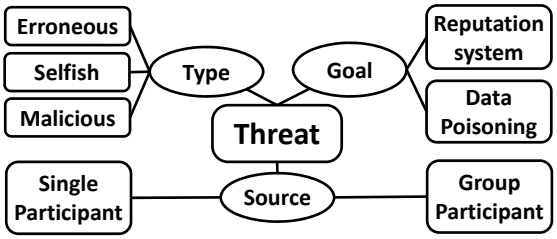

Figure 2: Threat model of the participatory sensing attacks.

3.2. Threat Model

We propose the threat model presented in Figure 2 to describe the different forms of vulnerabilities and attacks in participatory sensing systems. We propose to analyze attacks along the following dimensions:

Type. A threat can be originated from different types of participants: *erroneous*, *selfish*, and *malicious* participants. Erroneous contributions may be the result of a malfunctioning hardware or software held by a participant. Selfish participants are those who may not participate actively to the sensing campaign in order to save their mobile phone battery, or computational, and networking capabilities. If a large number of participants start to behave selfishly, the quantity, quality, and accuracy of the sensed data might be affected. Finally, malicious participant may deliberately report false, corrupted, or forged sensed data in order to disrupt the application analysis and measurements. Furthermore, participatory sensing systems may allow the participants to login anonymously. This enables malicious participants to launch attacks while escaping from any consequences.

Source. An attack can be initiated either from a *single* participant or from a *group* of participants. Although, a single source attack can disrupt the application measurements, it is, of course, more difficult to detect and treat attacks where multiple participants coordinate their behaviors to achieve some malicious goals.

Goal. An attack may disrupt the system by sharing erroneous, corrupted, and fabricated data (i.e., *data poisoning attack* in the figure). Instead, other attacks try to disrupt the reputation system by providing unfair ratings of other participants (i.e., *reputation system attack* in the figure). Reputation based attacks make a trust system assigns low trust score for honest participants and high scores for dishonest ones. Thus, contributions of honest participants are less considered and vice versa. Subsequently, data poisoning attacks directly affect the system, while reputation based attacks indirectly affect measurements of the application.

In Table 1, we classify the attacks discussed at the beginning of this section according to the dimensions of our proposed threat model.

Recently, trust systems have been adopted to resist or mitigate the effect of the existence of such attacks. In the following, we present the notion of trust.

4. Trust and Classification of Trust Systems in PS.

4.1. Definition and Characteristics of Trust

In participatory sensing, participants' honesty and veracity determine the reliability of their contributions. Participants can use different ways to tamper with their observations before submission, e.g. the corruption attack (Section 3.1). Thus, assessing the expected behavior of a participant can help to assess the reliability of his/her contributions.

In [74], we discussed and compared different definitions of trust. Gambetta [76] defines the term *trust* as:" the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends". Through this definition, trust can quantify the trustworthiness of participant's expected behaviors as a probability and subsequently the reliability of their Contributions.

In a previous work, we inferred the main characteristics of a trust relation between two entities [77]. We recall some characteristics of trust as follows:

- ***Binary, Directed relation*:** Trust is a binary directed relation linking two entities. It is considered as the confidence of an entity called *trustor* towards another entity referred to as *trustee*.
- ***Asymmetry*:** If entity A trusts entity B, it doesn't imply that entity B trusts entity A. Trust is not necessarily reciprocal between a pair of entities.
- ***Contextual*:** Trust is considered in the context of a particular actions which the target entity may perform.
- ***Subjectivity*:** Trust is the level of the subjective probability with which the trustor assesses that the trustee entity will perform a particular action.
- ***Non-transitivity*:** If entity A trusts entity B, and B trusts C, it does not necessarily imply that entity A trusts entity C.
- ***Composability*:** Trust relations can be constructed between not directly connected entities. Entity A may query for trust of entity B. Many entities in the community can provide different ratings i.e. reputation scores of trust for B. Thereafter, entity A can aggregate the received information to assign a trust level for B based on its own trust assessment method.

Table 1: Attacks classification according to the proposed threat model.

Dimensions / Attacks	Type			Source		Goal	
	Erroneous	Selfish	Malicious	Single	Group	Reputation System	Data Poisoning
Corruption	√	-	√	√	-	-	√
On/Of	-	-	√	√	-	-	√
Re-Entry	-	√	√	√	-	-	√
Discrimination	-	-	√	√	-	√	√
Collusion	-	-	√	-	√	√	√
Sybil	-	√	√	√	-	√	√
Reputation Lag	-	-	√	√	-	-	√
GPS Spoofing	-	-	√	√	-	-	√
Unfair rating	-	√	√	√	-	√	-
Bad Mouthing	-	√	√	√	-	√	-
Ballot stuffing	-	√	√	√	-	√	-

- ***Self-reinforcing*:** Entity tends to act honestly with trusted entities and to abstain with untrusted ones. Thus, this behavior reinforces the trust relation among trusted entities along the time.

- ***Dynamicity*:** The trust score of an entity may change over time. It may increase or decrease depending on the current performance of the entity. If its current interaction has a better quality than the last ones, its trust level could increase, and vice versa.

4.2. Classification of Trust Systems

Different trust systems have been proposed to resist and/or mitigate the effect of the attacks discussed in Section 3.1. We can classify these systems according to three dimensions, i.e. the *distribution* of the architecture, the *methodology* employed, and the *anonymity* assumed for the participants, as depicted in Figure 3.

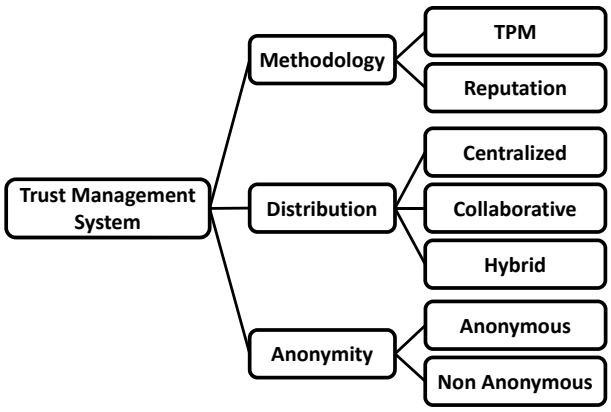

Figure 3: Classification of trust systems in participatory sensing.

4.2.1. Distribution

A trust system can be constructed as centralized, collaborative, or hybrid. Some trust systems exploit the existence of a trusted central third party referred to as *trust server* (*trust manager*). This type of system is called *centralized* trust system. In these systems, trust scores are maintained and stored by a trust server. The trust server receives both the participants' contributions and users' feedback. It then evaluates the contributions and aggregates the feedback to calculate a trust score for each participant. It also disseminates these scores to the users. A number of centralized trust systems have been proposed in the literature (e.g. [78]). A detailed discussion of these systems are presented in Section 7.1.

In some cases participatory sensing application allows a node to act as a source and a sink at the same time, i.e., each node receives the others' contributions while sharing its own ones. In such systems, trust maintenance and storage are equally distributed over all the nodes in the system; these systems are referred to as *collaborative* trust systems. In these systems, there is no central trusted authority. Every entity receives the other participants' contributions, evaluates these contributions, aggregates the neighbors' opinion about the target entity, and calculates a trust score for the target entity. Each node then disseminates the calculated trust scores to be exploited by the others. An example of collaborative trust system is presented in [79]. A detailed discussion of collaborative trust systems is presented in Section 7.2.

In some other systems, the application server is responsible for trust assessment. In these systems, there is no central trusted third party. The application server itself uses its own evaluation of participants' contributions and/or users' feedback to assign trust scores to those participants. Each application server manages the trust scores of the participants involved in its own campaigns. We refer to these systems as *hybrid* trust systems. In hybrid systems, the application server hybridizes/incorporates the role of both trust and application manager. One of these systems is presented in [80]. In this system, the application server measures the consistency of the participant's contribution compared with the other contributions for the same task. It then assigns a trust score to each participant. In Section 7.3, we discuss various hybrid trust systems.

4.2.2. Methodology

Trust systems can be classified according to the methodology used for trust assessment. Some systems depend on the existence of a Trusted Platform Module (*TPM*) while other systems try to assess the trust based on the *reputation* of the participant. The TPM is a hardware chip that ensures the authenticity of

participant's contribution by signing it. The system presented in [36] is an example for TPM based trust systems. More details about how a TPM manages trust is presented in Section 5. In addition, a detailed discussion of TPM based trust systems is presented in Section 7.3.2.

Alternatively, in reputation based trust systems, participants' behaviors are the primary measure of their trust. Participants who have good behavior are assigned higher reputation and trust scores. An example of reputation based trust system is presented in [81]. In this system, each participant is assigned a reputation score which reflects the quality of his/her current contribution. Additionally, the reputation score and the old trust score, which were previously assigned to a participant, are integrated to compute a new trust score for this participant. The details of reputation based trust assessment are presented in Section 6.

4.2.3. Anonymity

Trust systems that preserve participants' anonymity can be constructed. Preserving the participants' anonymity encourages them to share their personal information without being afraid of identity leakage (e.g., [58, 82]). In [58], Wang et.al. adopt blind signatures for anonymity preservation. In [82], Huang et.al. suggest using multiple pseudonyms for the same participant such that the participant uses a new unlinkable pseudonym each time. In this system, the server is responsible for pseudonym management.

In the following sections, we discuss both TPM and reputation based trust systems in more details.

5. Trusted Platform Module (TPM)

5.1. TPM Definition

Trusted Platform Modules (TPMs) are hardware chips that reside on participants' devices. Among other goals, TPMs ensure that the data sensed by the mobile sensors and reported to an application server are indeed captured by authentic and authorized sensor devices within the system. Thus, TPMs assure data authenticity [83, 84]. Some TPM trust systems for participatory sensing are presented in [85, 86, 36, 37].

5.2. TPM Goals

TPMs seek to satisfy one or more of the following goals:

- ***Attesting integrity:*** Integrity attestation is the main goal of TPMs. This property assures the authenticity of participants' contributions. It confirms that the data received from a participant is captured by a legitimate sensor that resides on the participant's mobile phone. Hence, it enables the application server to trust the reported data as authentic. This property is sometimes referred to as *remote attestation* [36, 37].
- ***Data protection, sealed storage:*** This property assures that the data is protected from unauthorized access. This implies that only authorized users and software can access the data [86].
- ***Secure boot:*** This property ensures that a mobile device can boot only the authorized trusted hardware and software configuration. This guarantees that the sensed data is processed only through the trusted hardware and software [87].
- ***Participant privacy :*** A sensing report usually contains personal and sensitive information about the participant, e.g., his location. This information can be exploited for participant re-identification. Although, preserving participants' privacy is not a primary goal of TPM trust systems in general, some of these systems have considered this issue for participatory sensing [86, 87].

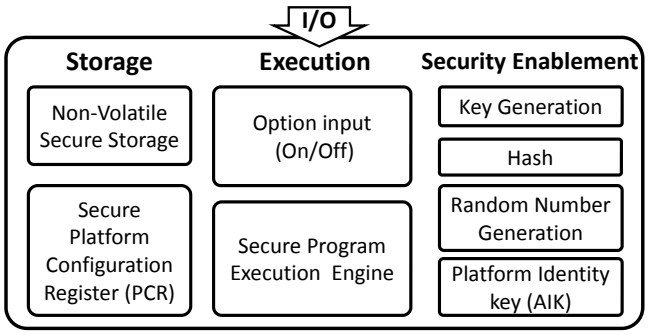

Figure 4: TPM module

5.3. TPM Components

As depicted in Figure 4[1], a TPM comprises several components [83, 84]. These components include:

- ***Nonvolatile secure storage :*** A TPM stores the information required for authentication such as passwords, certificates and/or encryption keys. This information needs to be stored securely over long periods of time. Therefore, such information is stored in nonvolatile secure storage.
- ***Secure platform configuration registers :*** Platform Configuration Registers (PCR) is the storage in which the sensed data is stored.
- ***Hash :*** A cryptographic hash module is used to measure the data that are going to be loaded in the PCR.
- ***Platform identity key :*** The private key of the TPM is stored in a separate storage. It is referred to as Attestation Identity Key (AIK).
- ***Secure program :*** The execution engine of the TPM which executes one or more of the TPM required functions.
- ***Key and random number generator components :*** A TPM can include components for generating keys and random numbers. Both keys and random numbers are exploited by the TPM to perform the different functions carried out through the secure program.

[1] http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

- ***Option input (On/Off) :*** The TPM is enabled or disabled according to an optional input (On/Off). The default value of this input is Off.

5.4. TPM Functions

To achieve the previously mentioned goals, a TPM has to run a secure program, which performs one or more of the following functions:

Digital signature. The most important concern of the TPM is to ensure the authenticity of a participant's contribution. This is referred to as attesting integrity. A TPM uses the stored information required for authentication such as passwords, certificates and/or keys for signing the sensed data. This enables the data to be verified by the server. Additionally, a TPM can generate anonymous contributions by signing them with the AIK besides using some certificates which are granted by a trusted third party for verification. The TPM can thus help to preserve the participant's anonymity [36, 37].

Hardware based cryptography. A TPM has the ability to encrypt the data before storing it. It uses the keys generated by the key generator module and/or the AIK for data encryption. This mechanism is used to ensure that the data stored are protected from unauthorized software access. Therefore, this function makes it much harder to access the stored information without proper authorization. This achieves the data protection goal [86].

Recording software run time configuration. Although a TPM is a hardware solution for trust, it is not only concerned with the hardware that capture the data, but also with the application software which carries out the local data processing on the participants' mobile devices. However, a TPM doesn't have the ability to control which software is launched on the participant's device. Nevertheless, it has the ability to store the run time configurations of the software. Thus, a TPM can send these data with the participant's contribution to the server. The server is then able to verify that only authorized software configurations are adopted for data processing. If the reported configurations differ from the required ones, it means that the software has been attacked. Consequently, the received contributions will not be trusted by the server. In summary, storing the software run time configurations assures the secure boot goal [87].

A TPM has the ability to achieve a high level of security and integrity. Most of TPM trust systems assure the goals discussed above (e.g integrity attestation, data protection, Secure boot,etc) (Section 5.2). However, these systems suffer from many limitations. One of these limitations is that they can't detect badly behaved participants. A detailed study for both TPM merits and limitations is presented in Section 8.1.1.

6. Trust based on Reputation

Reputation is the general opinion of the community about the trustworthiness of an individual or an entity. A person who needs to interact with a stranger, often considers her reputation to determine the amount of trust that he can place in her.

In recent years, reputation systems have gained popularity as a solution for securing distributed applications from misuse by dishonest entities. A reputation system computes the reputation scores of the entities in the system based on the feedback provided by fellow entities. A reputation system makes an entity accountable for its behavior by creating the possibility of losing good reputation and eventual exclusion by the community. Reputation systems make certain that users are able to gauge the trustworthiness of an entity based on the history of its behavior. The expectation that people will consider one another's pasts in future interactions constrains their behavior in the present [26, 74].

6.1. Properties of Reputation based Trust Systems

One can identify the main properties of reputation based trust systems as follows:

- ***Traceability*** **:** It is more probable for the participant who used to be honest to have a good behavior in the future. Similarly, a participant who previously behaved maliciously is expected to provide untrusted contributions. Thus, participant's past behavior should reflect his/her current reputation score.

- ***Freshness*** **:** The reputation score assigned to a participant should increase or decrease to demonstrate the most recent trustworthiness qualities of this participant, as a function of his/her latest interactions.

- ***Separability*** **:** Participants should not have control on the update process of their reputation scores. They shouldn't have the ability either to maliciously interfere to update their scores or to demonstrate a forged or erroneous reputation score.

- ***Exposure*** **:** Malicious participants should be exposed. Having committed a malicious behavior, participant should be identified as malicious and potentially evicted or at minimum his/her malicious contributions should be excluded.

Anonymous reputation based trust systems seek to achieve the previous goals while maintaining the anonymity of the participants' identity. The anonymity of a participant can be preserved by the satisfaction of the following goals as well. Some of these properties have been previously mentioned in [58].

- ***Anonymous login***: A participant should have the ability to login and to submit his/her reports anonymously. Participants' real identities shoudn't be revealed.

- ***Non-associative***: A sensing report should include neither the participant's real identity nor a reference to his/her real identity. Hence, the server will not be able to relate the sensing report to a specific participant by any way.

- ***MSR unlinkabelity***: The server shouldn't have the ability to link Multiple Sensing Reports (*MSR*) from the same participant.
- ***Anonymous demonstration***: Participants should have the ability to demonstrate their reputation scores to the server without revealing their real identities.

Both the satisfaction of these goals and the resistance against the previously mentioned attacks mainly depend on the strength of the trust system. In the following section, we will present how reputation is used to assess trust in participatory sensing applications.

6.2. Reputation based Trust System

The reputation based trust systems usually have four main phases [51]: (1) information collection; (2) information mapping to trust score; (3) dissemination and (4) decision making.

We depict a typical architecture of reputation based trust systems in Figure 5. In the following subsections, the details of this figure are discussed.

In a participatory sensing campaign, the server publishes a set of tasks that participants decide to join. When a given participant, e.g., participant P_i in the figure, captures his observations for a specific task $Task_j$, he/she constructs one or more sensing reports R_{P_i} for this task, and sends these reports to the application server. Then, the server gathers observations from different participants to carry out the required analysis. In addition, a trust system is applied to assess the trust of participants and their provided contributions.

6.2.1. Information Collection

Different information sources have been used to assess the trust of a participant. These sources include a Watchdog Module (*WDM*), users' feedback, community trust, and the history data of the target participant's .

WDM. WDM evaluates participant's current contribution (e.g., [34]). Sensing reports that belong to the same task are grouped together. Then, some consensus and outlier detection algorithms [89, 90, 91] are then used to evaluate the quality of a participant's contribution. These algorithms measure the similarity and consistency of each contribution compared with the other contributions provided by other participants. The higher the similarity of a contribution the more reliable it is. It is commonly assumed that the system is free of collusion or Sybil attacks. Otherwise, this measure can be biased. The result of a WDM is referred to as *Report Evaluation* (*RE*) and is depicted in Figure 5 (steps 1, 2, and 3).

Users' Feedback. A user x may assign a feedback for a contribution R_{P_i} of participant P_i referred to as *End user Feedback* (EuF_x), as depicted in Figure 5 (step4) [78].

Users should share both positive and negative feedback. Indeed, sharing only positive or only negative feedback exposes trust systems to different types of attacks (e.g. bad mouthing and ballot stuffing attacks) discussed in Section 3.1. Consequently, a feedback EuF_x should be evaluated. In Section 6.2.2, we explain how EuF_x is evaluated.

Community Trust. A trust manager may query his neighbors about their trust of a target participant. We refer to this type of information as the Community Trust CT as shown in the (step 6) of Figure 5. The trust data provided by the community members should also be verified against different rating attacks, Section 6.2.2 discusses this step.

History. Another type of information is the old trust scores stored at trust databases. Old trust score of a participant P_i is noted as $OldT_{P_i}$ in the (step 5) of Figure 5.

Following the different sources of information described above, we can deduce that, the collected information is created either *manually* or *automatically*. On the one hand, manual information is usually created as an evaluation of participant's current contribution (e.g., the output of WDM *RE*). On the other hand, automatic information is an available trust data either stored at trust databases (i.e. direct information) or received as a feedback and responses to the trust queries (i.e. indirect information).

Thereafter, the collected information is used to assign a trust score to the participant through the trust mapping phase as shown in Figure 5 (steps 7, 8, and 9). In the following section, we discuss the details of this phase.

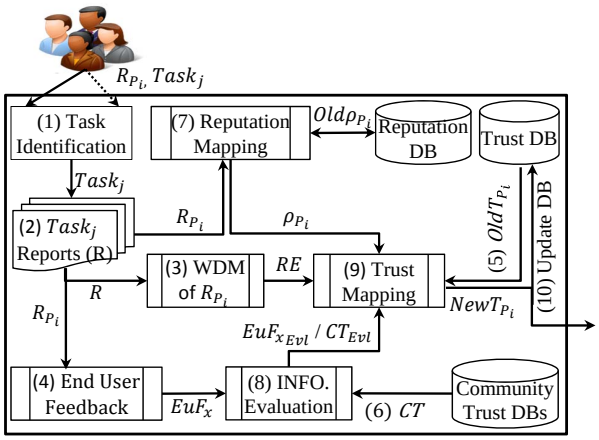

Figure 5: Typical reputation based trust system

6.2.2. Information Mapping into Trust Score

The mapping process is carried out either in a centralized or a distributed way. In centralized mapping, participants' contributions and end users' ratings are exploited by a single entity in the trust system to calculate the new scores. This entity calculates a new reputation ρ_{P_i} and/or trust score $NewT_{P_i}$ for each participant, and updates the participants' record in the related database. A centralized mapping trust system is presented in [78]. Instead, in distributed mapping systems, the mapping process is distributed on more than one entity in the system. For example, in [82], both end user and the server map a new reputation score for each participant.

Reputation Mapping. In this phase, the first objective is to assign a new reputation score ρ_{P_i} to the participant. Here, a reputation mapping function is adopted as depicted in Figure 5 (step

7). According to the literature [51], such reputation mapping function is either *deterministic* or *probabilistic*. In deterministic mapping, the output is computed according to a set of well defined input values. Oppositely, probabilistic mapping functions have possibility of an error (within some known bounds) and an unpredictable output due to some randomness in their input values. Various approaches have been applied to compute reputation scores of participants [92, 25].

Due to the novelty of incorporation of trust management solutions into participatory sensing applications, not all the reputation computation methods that have been used in other domains have been investigated yet. Most of the current trust systems rely on either Bayesian reputation as a probabilistic approach [93] or the Gompertz function as a deterministic approach [94] for reputation mapping. The characteristics of these functions are very suitable for trust construction within participatory sensing environments. This is because the output of these functions dynamically reflects the changes in the participant's behavior along time. Thus, participants' behaviors can be effectively traced using one of these functions. Additional characteristics are discussed as part of the definition of these function hereafter.

Bayesian Model Beta distribution is a statistical distribution which is defined according to the two parameters α and β. Its probability density function f for $0 \leq x \geq 1$ is formulated in Equation 1 as follows:

$$f(x/\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \times x^{(\alpha-1)} \times (1-x)^{(\beta-1)} \quad (1)$$

where, Γ is the gamma function, α and β represent the number of good and bad interactions of the participant respectively. The distribution domain is $[0, 1]$. The reputation is calculated by finding the expectation $E(\alpha,\beta)$ of the beta distribution according to Equation 2.

$$E(\alpha,\beta) = \alpha/(\beta+\alpha) \quad (2)$$

In [95], an example of Bayesian reputation plot generated for three participants is depicted in Figure 6, while (α, β, $E(\alpha,\beta)$): (2, 10, 0.16), (4, 6, 0.40), (20, 5, 0.80) and 0.1 is used as the acceptable level of error. It is clear that, participants with close values of α and β are assigned low reputation scores. In addition, the displacement of the model output along x axis reflects the type of participant's behavior (e.g. good or bad). Consequently, this model has the ability to measure the participant's deviation rate from the good behavior. The considered level of error fits the uncertainty of participants' behaviors in participatory sensing.

Furthermore, reputation should be calculated based on the most current information while keeping the effect of some historical data. The Beta aging parameter w_{age} supports the ability to consider discounting of old information. The new values of α and β are calculated according to the following equations.

$$\alpha_{new} = w_{age} * \alpha_{old} + \alpha_{current} \quad (3)$$

$$\beta_{new} = w_{age} * \beta_{old} + \beta_{current} \quad (4)$$

In this equation, w_{age} ranges from 1.0 which means keeping the entire history to 0.0 which means that no history was taken into consideration.

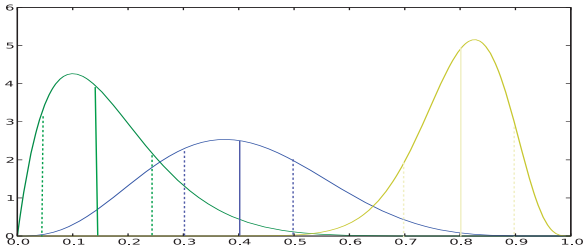

Figure 6: The beta output for various types of participants.

Gompertz Function Gompertz output gradually increases to reach its asymptote during a specific period of time. This behavior is reflective of trust construction in participatory sensing systems. For example, in such participatory sensing environments, trust is built gradually after a period of trustworthy behavior. It can also resemble some social parameters which positively affect trust (e.g. friendship duration, the number of interactions between entities). For example, long lasting relations are stronger than recent ones and subsequently are more trusted. Similarly, it is implied that the stronger the relation between entities, the higher the number of interactions between them during a given period of time. These properties are well resembled by the output of Gompertz function. Gompertz is defined according to Equation 5.

$$f(t) = a \times e^{-be^{-ct}} \quad (5)$$

In this equation, a is the upper asymptote, b controls the displacement of the output along the x axis and c adjusts the growth rate of the function. The output of Gompertz belongs to the range $[0, 1]$. In [79], the output of Gompertz function for c = 1.5, 2.5, and 5 where b = 10 is depicted in Figure 7 (left).

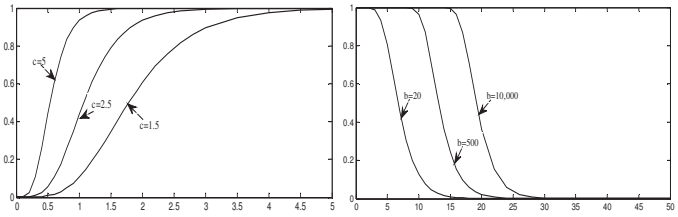

Figure 7: Gompertz and Inv Gompertz output

Inverse Gompertz Function The output of inverse Gompertz function is used to resemble the parameters which negatively affect trust (e.g. timeliness which represent the delay of participant responses). It is implied that, the more the delay of a participant respond to a task, the less concern he pays for it. Subsequently, late responses are usually assigned less trust scores and vice versa. Inverse Gompertz is defined in Equation

6. The output of the inverse Gompertz function for different values of b is depicted in Figure 7 (right).

$$f(t) = 1 - a \times e^{-be^{-ct}} \quad (6)$$

Both Gompertz and inverse Gompertz have the ability to integrate both some aging and reward/penalty mechanisms.

Information Evaluation. The second objective of this phase is to verify the received information such as users feedback EuF and the trust scores received from the community CT against different rating attacks discussed in Section 3. Most trust systems in participatory sensing use the reputation ρ_x stored in the database of the rater x as a weight for his/her provided rating. Consequently, low weight is assigned to the rating provided by a user or entity with poor reputation, and vice versa. The output of this module is referred to as Evaluated end User Feedback EuF_{xEvl} and Evaluated Community Trust CT_{Evl}, Figure 5 (step 8). However, this action doesn't solve the problem of different rating attacks; it only seeks to mitigate the effect of such attacks.

Trust Mapping. The last issue, in this phase, is to assign a new trust level $NewT_{P_i}$ to the participant as depicted in Figure 5 (step 9). In this phase, not only the current reputation score ρ_{P_i} is considered but also other parameters. These parameters include the current report evaluation RE evaluated by the WDM, the old trust level assigned to the participant $OldT_{P_i}$, the trust provided by the community CT_{Evl} and/or the users' feedback about the participant EuF_{xEvl}. Each trust system selects one or more of these parameters and aggregates them to calculate a new trust $NewT_{P_i}$ score of the participant. Finally, this new score is used to update the participant's record in the related databases as depicted in Figure 5 (step 10).

6.2.3. Dissemination

This phase is realized either in a centralized or a distributed manner. In centralized dissemination, the reputation scores are stored in and propagated from a single entity. Additionally, the regularity of the dissemination process comes in one of two forms; *proactive* and *reactive* dissemination. In the proactive mode, the dissemination is performed periodically at a fixed rate. In the reactive mode, the dissemination is performed according to some triggers, events or when some threshold is reached. In other systems, a query message is required for obtaining trust scores [79].

6.2.4. Decision Making

The final phase in reputation based trust systems is the decision making. The decision mainly depends on the trust score assigned to the participant. Trust scores are either *discrete* or *continuous* values. Discrete trust scores use a set of discrete qualitative values such as (Very Untrustworthy, Untrustworthy, Trustworthy, Very Trustworthy). Continuous trust scores come in a range of values such as $[0, 1]$. If the trust score for a participant is greater than a predefined threshold, the participant's contribution is accepted. Moreover, the participant is then rewarded if the trust system applies an incentive/reward mechanism. Oppositely, if the trust score is below the threshold, the participant's contribution may be rejected and the participant may be penalized (if a penalty mechanism is adopted). This type of decision is referred to as a binary decision. However, some systems are designed to accept all received contributions. In these systems, the current trust score of the participant is used as a weight for his/her contribution. We called this type of decision as fusion.

In Figure 8, the reputation based trust systems' phases, functions and parameters are summarized.

In the next section, we present the state-of-the-art trust systems in participatory sensing applications.

7. State-of-the-Art Analysis of Trust-based Systems

7.1. Centralized Trust Systems

Centralized trust systems are those systems where trust scores of participants are maintained and stored by a trusted central third party. In the following, we discuss examples of these systems.

Manzoor et. al., in [81, 98], seek to compute the trustworthiness of participants' predictions about bus arrival times in a bus watch participatory sensing application. The trust server measures the deviation of a participant's prediction compared with others' predictions. This measure is fed into a Gaussian membership function to define the quality of each contribution. The output of the Gaussian function is combined with the old trust of a participant to estimate the instantaneous trustworthiness of this participant.

A centralized trust framework for social participatory sensing systems is introduced in [96]. This framework estimates a score of the *Trust of Contribution* (ToC). This score assesses both the *Quality of Contribution* (QoC) and the *Trustworthiness of Participant* (ToP). Some methods are adopted to evaluate QoC (e.g. [91, 90]). In addition, ToP is used to measure both the participants' capabilities and the strength of their relation with the requester (e.g. expertise, timeliness, locality, friendship duration, and interaction time gap). To calculate a TOC score of a participant, the system combines both of the QoC and the ToP of a participant via a fuzzy inference system [96].

An improved version of the previous system is presented in [78, 99]. A reputation and a subjective rating modules are incorporated. The reputation module utilizes the *PageRank* algorithm [100] to calculate and update the reputation scores of participants. This algorithm relies on the difference between the numbers of nodes that trust the participant compared with the total number of his/her relations; the most trusted participants are assigned higher reputation scores. In addition, the subjective evaluation enables the requester to assign a rate to the participant. The reputation score of the requester is used as a weight for his/her provided rating. The new trust score of a participant is calculated based on ToC, the requester evaluation and its weight. Badly behaved participants are penalized by decreasing their trust scores. This system has the ability to

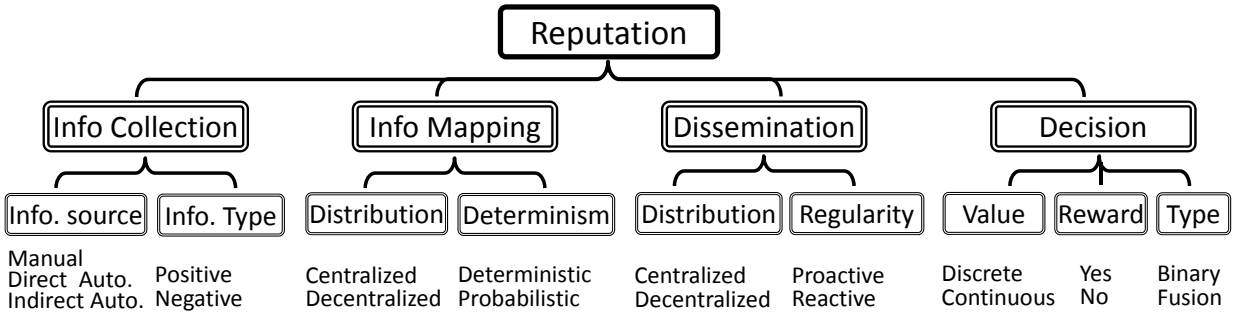

Figure 8: Mapping trust in reputation based trust system

trace and detect the participant's behavior through the continuous update of the reputation scores. It also reflects the change of the participant's behavior. Additionally, early detection and penalty of misbehaved participants act as a deterrent for malicious behavior.

In [101], authors propose a system to select the most appropriate and trustworthy participants among friends and friends of friends in a social participatory sensing network. The most trusted paths to those participants are defined. First, the selection process depends on the compatibility between both the task requirements' parameters and participants' attributes. Participants who achieve an acceptable levels of homogeneity with the task requirements are selected to attend the campaign. In such social sensing network, routes from a requester to the selected participants can include other intermediate nodes. Thus, a depth first search is applied to define the most trusted route to those participants. The route trust score is calculated as a combination of the trust scores of each pair of nodes along the route. Then, the route with the highest trust score is selected.

Each contribution is directed to a trust server. The trust server exploits the trust system previously presented in [78, 99] and discussed above to calculate trust of participants. Moreover, a suggestion component is incorporated for building the list of participants who achieve a satisfactory behavior during multiple campaigns. This system has the same pros and cons of the system presented in [78, 99] except that it enables the requester to recruit the most appropriate participants to join campaigns.

A privacy preserving reputation system for participatory sensing is presented in [82]. The authors try to compromise between both participants' anonymity and the trust of their contributions. Participants share their contributions anonymously using some changeable pseudonyms. The system relies on a trusted server referred to as (*TTP*). The server maintains a mapping list between participants' real identities and its associated pseudonyms. Then, the server assigns new reputation scores to the participants relying on Gompertz function described in Section 6.2.2. Hereafter, the server updates the corresponding reputation score and attaches it to the real identity. The server transfers the reputation score from the real identity to the next chosen pseudonym.

LotS is a privacy preserving reputation framework that is presented in [102]. In this framework, participant p_i join one of the groups created previously by a *Registration Authority* (RA). Participants can anonymously share their contributions with another entity C by signing them with the group signature. If the contribution is verified to be correct, the recipient forward it to the rest of the community. Each community member can sends a voting request to C to evaluate the received contribution. C should make sure that every entity has the ability to send no more than one voting request for the same report. Then, these votes are aggregated to calculate the reputation score of the report provider. This score is subsequently forwarded to the report provider.

SPPEAR is a privacy preserving framework that assure both privacy of participants and accountability [103]. A group manager (*GM*) announce a list of tasks. A participant selects one or more and authorize with a GM to obtain a private key and an authorization token from the GM. Participant share this token with an *Identity Provider* (*IdP*) entity which provides her with pseudonyms from a *Pseudonyms Certification Authority* (*PCA*). SPPEAR adopts a protocol for the revocation of participants who submit samples that deviate from the rest of contributions. A resolution authority (*RA*) provides the pseudonyms of those participant to PCA; PCA provides RA an authorization token including assertion that used to generate this pseudonym. RA forwards this token to the IdP who blacklists all tokens of this pseudonym and sends a confirmation to GM. A similar protocol is adopted for the revocation of participants who have a malfunctioning device and thus unintentionally provide some corrupted contribution.

Chang et al., in [59], propose a trust system for detecting Sybil attacks. Sybil nodes usually use the same radio channel for communication. Thus, this scheme detects the existence of Sybil nodes through defining the normal rates of some statistical measures of a participatory sensing network of interest (e.g. the number of participants who join the system campaigns at specific time). To determine if the node is genuine or Sybil, a regular check for these measures is performed by a *Characteristics Checking Scheme* (*CCS*). Additionally, a *Trust Credit Assessment* (*TCA*) module is adopted to collect the feedback reported about the nodes in the system. If both CCS and TCA find the measured rates outbound the normal ranges, the requester is notified that Sybil nodes exist. Otherwise, the requester is notified that the network is free of such nodes. Although this system mainly depends on the CCS, it is considered as a reputation based trust system because it aggregates the feedback of the

nodes from the requesters which is a reputation mechanism.

7.2. Collaborative Trust Systems

In collaborative trust systems, each node in the system maintains and stores trust scores in its own storage, as defined in Section 4.2.1.

The system presented in [104] enables the campaign administrator to filter out untrusted participants. First, the system exploits participants' reputation derived from both the quality of their current contribution and their old reputation scores. Feedback scores derived from the community members are aggregated. Moreover, some personal information about participant is integrated. Each one of these parameters is assigned a score. According to the scores of these parameters, a weighted sum trust score is calculated for each participant. Then, participants are ranked based on these trust scores. Finally, the most trusted participants are selected to attend the campaign. Although the authors presented an integrated system for trust assessment, they only define the system parameters that should be considered. They do not go through how these parameters should be measured.

In [79], both personal and community opinions are integrated to evaluate the trustworthiness of a specific node. First, each contribution is assigned either positive or negative feedback by the requester. This feedback is determined by calculating the numerical scores of some parameters such as the response time, time gap, familiarity, reciprocity, and the relevance parameters. Subsequently, the score of each contribution is calculated as a weighted sum of these parameters' scores. If the score of a contribution exceeds a certain threshold, the contribution is assigned a positive feedback and vice versa. In general, the responding node is assigned a positive opinion if the number of its positive contributions exceeds a specific threshold. Then, the requester queries the community opinion about the responding node. Finally, both personal and community opinions are integrated to evaluate the trust score of this node.

7.3. Hybrid Trust Systems

As previously discussed in Section 4.2.1, we refer to a trust system as a hybrid system when the application server manages both the application campaigns and participants' trust as well. These systems are constructed as either reputation or TPM based systems. Here, hybrid reputation based trust systems are presented followed by hybrid TPM based trust ones.

7.3.1. Hybrid Reputation based Trust Systems

In [95], authors propose a set of metrics that enable for evaluating participants' contributions. Participants who have some experience in the current task are selected to join the campaign. Additionally, a contribution is defined to be successful if it is captured by the appropriate sensor at the required time and location. Moreover, it should assure the timeliness, relevance, and the quality of the contribution. Finally, this system adopts Bayesian reputation function described in Section 6.2.2.

The system presented in [97] proposes a recruitment framework to define the most trusted participants for a campaign. This framework depends on the participant's reputation while the Bayesian model is used to compute this reputation score as explained in Section 6.2.2. Non-cooperative participants are defined by measuring the probability that participants are going to contribute their observations, when it is available, or not. The system seeks to measure the quality and quantity of samples that are expected from a participant.

In [80, 34], Huang et al. propose a system for evaluating trustworthiness of participants' contributions in noise monitoring participatory sensing applications. Each device is assigned a reputation score which depends on the quality of the reports submitted by this device in a specific period of time. Reports which belong to the same sensing location are grouped and directed to a watchdog module (*WDM*). WDM produces a set of ratings in the range $[0, 1]$. The rating of each contribution is used as a weighting coefficient to minimize the impact of corrupted ones. It also acts as input to a subsequent reputation module. The system incorporates some historical information about the device. Moreover, it adopts the reward/penalty mechanism. The reputation module computes a reputation score based on Gompertz function. The experimental results indicate that this system quickly adapts the reputation scores according to the changes of participants' behaviors.

Authors in [58, 35] propose a privacy preserving reputation system. In the registration phase, the server grants the participant two reputation certificates (i.e. one including participant ID while the second doesn't include this ID). The first certificate is used to construct one or more blinded ID [105] to submit one or more sensing report anonymously. The second certificate is involved into the sensing report. The system allows participants to cloak their time and location data. Then, it calculates sensitivity parameters to define contributions that are captured outside the required sensing area and time. In addition, a similarity factor is evaluated to measures the consistency of a participant's report with other reports for the same task. The server asses the trust of participant based on the reputation score contained in the certificate beside the sensitivity parameters and the similarity measure. The participant is assigned a positive feedback if the final trust score exceeds the current trust score contained in his/her reputation certificate, and vice versa.

This system maintains both the data trust and the participant's anonymity. Therefore, the participant ID and the sensing report can't be correlated. Additionally, multiple reports which sent from the same participant can't be linked to each other. Moreover, both negative and positive reputation updates are enforced. However, a large number of participants is required to preserve the participant's anonymity. Otherwise, participant's identity can be compromised.

A framework (*FIDES*) is introduced in [64] to defends against the GPS attacks. A mobile security agent (MSA) is deployed into the sensing area (e.g. a taxi driver). The application guarantees the reliability of the reports provided by the MSA due to some reward or additional credits which provided to this agent. These credits are provided by the credit-based reward mechanism in advance. The application asks both participants and MSA to share their sensed data. Participant's contribution is used to update her/his reputation score. FIDES adopts the

trust model proposed in [106] to model the uncertainty about participants reputation. In addition, this score is used to judge the contribution and to calculate the reward that should be assigned to this participant. Depending on MSA, to define the normal behavior of participant, makes this framework robust against different types of attacks such as corruption, Discrimination, reputation lag, assuming that MSA will not abuse.

In TAPAS [107], the system tries to assure both the trust of participants' contributions and their privacy preservation. The system allows multiple participants to collect their observations at each data collection point (*DC*-point) redundantly. The contribution that achieves the major consensus is verified as correct. Consequently, the large the number of the participant at the DC-point, the more the chance that the collected data are correct. The system assigns DC-points to the participants based on a privacy preserving technique [108]. Therefore, participants can't be compromised to a location based attack.

7.3.2. Hybrid TPM based Trust Systems

A trusted platform based framework for participatory sensing is introduced in [37]. An application running on a participant's phone is responsible for taking integrity measurements and passing them to TPM. Application server sends an attestation request to verify the trustworthiness of a participant's contribution. In this case, TPM signs the recorded integrity measurements and sends it to the server. The contribution is considered trustworthy if it is correctly verified with the measurements received from the TPM.

In [36], authors try to attest the integrity of sensed data through supporting each sensor with TPM referred to as *angel*. The role of the angel is to execute a code signed by a trusted third party. This code attests the integrity of sensed data through signing it. TPM is supported with a hardware cryptographic module. The private key is burned into the chip. Additionally, data are encrypted to achieve data protection. This system is resistant to both collusion and Sybil attacks. Furthermore, it ensures both content protection and access control mechanism using a broadcast encryption technique. However, uploading raw sensed data is highly expensive for mobile devices. Moreover, contributing data in their raw form acts as a deterrent to participants to contribute their personal information.

Both trust of participant's contribution and privacy preservation are considered by Gilbert et. al. in [87]. First, TPM launches a trusted software to carry out the required local processing on the raw sensed data. The data are recorded into PCR concatenated with their hash value. PCR content is updated only using the hash value of the current PCR (*extend operation*). Additionally, TPM signs its PCR in order to attest the software used for report generation. Furthermore, TPM has the ability to encrypt the data and bind them with a specific software. Consequently, only trusted software is able to access the data storage. On the application server side, the hardware used is verified using the certificate issued by a certificate authority provider. The application server compares PCR contained in the report with the expected values to assess the software validation. This system shares the same advantage and limitations of the system presented in [36] and discussed above. Additionally, a trusted software is used for local data processing.

The idea presented by Saroiu et.al. in [86] is to integrate TPM functionality with each individual sensor reading. Each sensor reading is signed by the sensor from which it was captured. In addition, a small trusted code in the cloud is used to verify the raw sensor reading and to combine these readings. Subsequently, a registration process is used by the service cloud to link between the sensors and the device in which it resides. This design assures the property of remote attestation. They have the ability to prove that the contributed data were captured by a authentic sensor within the participatory network. Neither participant's privacy nor data protection is assured by this system.

In [85], an analyzer is adopted for evaluating participants' contributions. This analyzer has the ability to measure the differences between the data that are shared by a participant and the original sensor reading. Thus, this system assures the data authenticity. However, the authors adopt a TPM emulator as a building block instead of TPM hardware.

8. Comparative Study

In this section, we use the criteria, classification, and framework introduced in Sections 4, 5, and 6 to make comparisons between the various systems that have been presented in the literature (Section 7). We used these comparisons to discuss all existing trust systems and conclude them in the field of participatory sensing.

8.1. Comparison based on Methodology and Goals

A general comparison of trust systems based on the criteria of distribution, methodology, anonymity, and goals satisfaction is presented in Table 2. These criteria hqve been described earlier in Sections 4.2, 5.2, and 6.1.

8.1.1. Analysis of TPM Trust

According to the TPM goals described in Section 5.2, Table 2 shows the guarantees that can be assures by each of TPM trust systems. Most of TPM based trust systems (such as [37, 36, 87, 85, 86]) assure the goal of integrity attestation. Additionally, they can achieve the secure boot goal (such as [87]). While other TPM based approaches are able to assure data protection and user anonymity (such as [86]).

We can deduce that TPM based trust is considered as a viable solution for trust assessment in participatory sensing applications. However, the goals achieved by these systems do not imply that they can detect the existence of corrupted contributions. TPM seeks to assure integrity regardless participant's honesty. Dishonest participants contribute false or forged contributions to disrupt the application measurements. Consequently, the need arises for trust systems which can measure the quality of the contributions and estimate the honesty of participants. Therefore, reputation based trust systems have been introduced seeking to satisfy these needs.

Furthermore, concerning TPM availability, TPM trust systems require smartphones or computing devices with special sensors that are manufactured to support trust systems through an embedded hardware chip. Thus, this property raises the prices of these smartphones that support TPM. Consequently, smartphones with embedded TPM are currently not manufactured for the mainstream market. Moreover, there is no guarantee that all smartphone users who join sensing campaigns are equipped with such devices. In addition, embedded chips consume more energy, computation, and communication capabilities, which may discourage participants to join sensing campaigns.

These limitations obstruct the widespread use of TPM based trust systems for the moment. To the best of our knowledge, TPM still a theoretical framework that was not applied to a real life participatory sensing system. However, it was successfully applied into other network domains [88].

8.1.2. Analysis of Reputation based Trust

The goals of reputation based trust system goals have been discussed in Section 6.1 (e.g. traceability, exposure, freshness, etc). Most reputation based trust systems (such as [58, 82, 103, 102, 96, 78, 34]) assure these goals as depicted in Table 2 . However, each trust system assures each one of these goals with different degrees of satisfaction. For instance, reputation trust systems have the ability to detect participants' misbehavior (i.e. exposure property). However, the speed to detect such misbehavior depends on the strength of the reputation mapping function. A reputation mapping function may incorporate some aging parameters to assign higher weight to participants' recent interactions. Furthermore, reward and penalty rules can be applied (Section 6.2.2).

Most of the current trust systems use either Bayesian or Gompertz function for reputation mapping. It was clear that the systems which exploit Gompertz mapping function have stronger capabilities than the other mapping functions exploited in participatory sensing. This is because Gompertz function has the ability to integrate both the aging parameters and the reward/penalty mechanisms, which enable the system to rapidly reflect new features of a participant's behaviors on the assigned trust score. The systems that adopt the Gompertz function include [80, 82, 96, 78]. While Bayesian model is exploited in [95, 97].

8.1.3. Privacy Preserving Reputation Systems

The goals of privacy preserving reputation system were discussed in Section 6.1. These goals include anonymous login, non-associative, and anonymous demonstration. The systems presented in [58, 82, 103, 102] have the ability to preserve participant's anonymity (Table 2). These systems satisfy the goals of privacy preserving reputation systems. The reputation systems which we have presented in [109, 110] don't hide the identity of the participants but preserve the confidentiality of their feedback. Such reputation systems are suitable for environments where participant anonymity is not possible or feedback confidentiality is the main privacy goal.

8.2. Comparison based on Architecture

As mentioned before, in Section 4.2.1, participatory sensing trust systems have three different architectures: centralized, collaborative, and hybrid. Each one has its own characteristics as discussed in Section 4. Concerning centralized trust systems [96, 78, 103, 102, 82], the existence of a central authority confirms that information collection, aggregation, and dissemination are maintained correctly. Additionally, they are resistant to some types of attacks such as Sybil and collusion attacks. Furthermore, minimal overhead is imposed on the participants' devices which usually have a computation and energy limitations. However, the central authority must be available and correct all the time. Thus, centralized trust systems are vulnerable to single point of failure problems. Moreover, the central server imposes some limitations on the system's scalability.

The limitations of centralized systems can be avoided by employing collaborative trust systems [79, 104]. Nevertheless, collaborative systems impose extra overhead on every entity in the system. Hybrid trust systems seek to find a balance between scalability and the overhead distribution among the application server and the participants [34, 35, 64].

8.3. Analysis of Attack Robustness

Participatory sensing systems are vulnerable to various attacks as described in Section 3.1. Each of the proposed trust systems shows different degrees of resistance against each of those attacks as depicted in Table 3. We will discuss the resistance of TPM trust systems to different types of attacks followed by that of reputation based trust systems.

8.3.1. Robustness of TPM Trust Systems

It is evident that most of TPM based trust systems are robust against re-entry, Sybil and on-off [36, 87, 86, 85]. TPM trust systems assure the authenticity of participants' contributions. Thus, the application server can make sure that the participant's contribution has been captured by authentic sensor. Thus, participants have to use another device to launch such attacks which inhibits attacks of these types.

TPM assures the secure boot property, which implies that the appropriate hardware configuration is used to capture the observations. It also ensure that only trusted software is used for local processing of these observations. Hence, participants have minimum control on their own observations. Consequently, they have little opportunity to coordinate their behaviors to achieve some malicious goals (i.e. collusion attack). Thus TPM are resistant under collusion attack.

Although, these systems are robust against these previous attacks, they are considered weak against corruption attacks. TPM can't detect malicious participants who deliberately initiate sensing actions to corrupt their observations, as discussed before. Additionally, the other attacks are not considered with TPM trust systems.

8.3.2. Robustness of Reputation based Trust Systems

Regarding reputation based trust systems, we can note that the trust scores usually depend on one or more of the following parameters:

Table 2: Comparison of the trust systems in terms of goal satisfaction

System	Architecture	Methodology	Anonymity	Characteristics										
				TPM			Reputation				Anonymity			
				Attestation	Data Protec.	Secure Boot	Traceability	Freshness	Separability	Exposure	Anon. login	Non-associative	MSR Unlinked	A non demon.
Dua et.al. [37]	Hybrid	TPM	N-anon	√	-	-	-	-	-	-	-	-	-	-
Dua et.al. [36]	Hybrid	TPM	N-anon	√	√	-	-	-	-	-	-	-	-	-
Gilbert et.al. [87]	Hybrid	TPM	Anon	√	√	√	-	-	-	-	-	-	-	-
Saroiu et.al. [86]	Hybrid	TPM	Anon	√	√	-	-	-	-	-	√	-	-	-
Gilbert et.al. [85]	Hybrid	TPM	N-anon	√	-	-	-	-	-	-	-	-	-	-
Reddy et.al. [95]	Hybrid	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Reddy et.al. [97]	Hybrid	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Yang et.al. [104]	Coll.	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Huang et.al. [80, 34]	Hybrid	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Jkalidindi et.al. [79]	Coll.	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Manzoor et.al. [81]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Amintoosi et.al. [96]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Amintoosi et.al. [78, 99]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Amintoosi et.al. [101]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Chang et.al. [59]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Wang et.al. [58, 35]	Hybrid	Rep	Anon	-	-	-	√	√	√	√	√	√	√	√
Huang et.al. [82]	Cen	Rep	Anon	-	-	-	√	√	√	√	√	√	-	√
Restuccia et.al. [64]	Cen	Rep	N-anon	-	-	-	√	√	-	√	-	-	-	-
Michalas et.al. [102]	Cen	Rep	Anon	-	-	-	√	√	√	√	√	√	√	√
Gisdakis et.al. [103]	Cen	Rep	Anon	-	-	-	√	√	-	√	√	√	√	-

-	Goal not satisfied	Cen	Centralized	N-anon	Non anonymous
√	Goal satisfied	Rep	Reputation	Coll	Collaborative

- The participant's old trust or reputation score.
- The quality of the current contribution.
- The end user's feedback about the contribution.
- The neighbors' rating of this participant.

Each reputation based trust system selects one or more of the previous parameters and adopts a specific reputation mapping function to calculate a trust score for every participant. Therefore, each system has a different degree of resistance against various attacks. From the discussion of the state-of-the-art of existing trust systems in participatory sensing presented in Section 7, we can deduce the following:

Corruption Attack. The system presented in [64] is considered robust against corruption attack. This systems depend on a mobile secure agent which provides the system with the most accurate information. Thus, the system can accurately define corrupted contributions.

Other trust systems depend on double checking way to define the quality of a contribution. First, outlier detection or consensus algorithms [89, 90, 91] are used to measure the deviation of the contribution from a common consensus. Second, users are supposed to assign a rate to a participant based on their satisfaction with the received contribution. Trust systems that adopt both the first and the second measures are considered robust against this attack [78, 101]. Systems that adopt only one of these measures are semi robust against this attack [103, 34, 35, 81]. However, the systems that only depend on the past interactions of the participant as a measure of trust weakly defend against this attack (such as [95, 97]), because participants may instantaneously change their behavior.

Reputation lag exploitation attack. The reputation mapping function should apply more aggressive penalties concerning badly behaved participants. This allows a trust system to have an up to date trust scores which reflect the instantaneous trustworthiness of each participant. Thus, badly behaved participants have a minimum opportunity to exploit the reputation lag for injecting corrupted or forged contributions into the system. Gompertz function apply more strong penalties compared with the other mapping functions. Thus, trust systems that depend on the Gompertz function are more rapidly adaptive for reflecting changes in the participants' behaviors.

Consequently, Gompertz based trust systems are robust against reputation lag exploitation attack (such as [80, 96, 78, 101]). Bayesian based reputation trust systems (such as [95, 97, 81, 58]) are considered semi robust against this attack. The reputation systems presented in [79, 59] are weak against the reputation lag exploitation attack, because both of them only depend on the community opinions and feedback about the participant and they have no way to penalize badly behaved participants.

On-Off attack. On-off attacker alternate between normal and abnormal behavior. Thus, the way to defend against this attack is to have a good capabilities to monitor and trace participants' behaviors. In addition, the system should involve a mechanism to evaluate the quality of the participants' contributions to be more resistant to this attack. Thus, systems which satisfy both these guarantees are robust against on-off attack. These methods include [34, 78, 101, 81, 58, 64]. However, semi robust trust systems (such as [82, 96]) only assure either the first or the second guarantee. The reputation trust systems that neglect the quality of contribution are considered weak against this at-

Table 3: Analysis of the trust systems in terms of robustness to attacks

Scheme \ Attack	Corr	Onof	Ree	Dis	Col	Syb	Lag	GPS	Unf	Bad	Ball
Dua et.al. [37]	*	-	* * *	-	* * *	* * *	-	-	-	-	-
Dua et.al. [36]	*	-	* * *	-	* * *	* * *	-	-	-	-	-
Gilbert et.al. [87]	*	-	* * *	-	* * *	* * *	-	-	-	-	-
Saroiu et.al. [86]	*	-	* * *	-	* * *	* * *	-	- -	-	-	
Gilbert et.al. [85]	*	-	* * *	-	* * *	* * *	-	- -	-	-	
Reddy et.al. [95]	*	*	-	-	-	-	**	-	-	-	-
Reddy et.al. [97]	*	*	-	-	-	-	**	-	-	-	-
Yang et.al. [104]	-	-	-	-	-	-	*	-	**	-	-
Huang et.al. [80, 34]	*	**	-	-	*	-	* * *	*	-	-	-
Jkalidindi et.al. [79]	-	-	-	-	-	-	*	-	**	-	-
Manzoor et.al. [81]	**	**	-	-	*	-	**	*	-	-	-
Amintoosi et.al. [96]	**	*	-	-	*	-	* * *	*	**	-	-
Amintoosi et.al. [78, 99]	* * *	**	-	-	*	-	* * *	*	**	-	-
Amintoosi et.al. [101]	* * *	* * *	-	-	*	-	* * *	*	**	-	-
Chang et.al. [59]	-	-	-	-	-	* * *	*	-	*	-	-
Wang et.al. [58, 35]	**	**	-	-	*	*	**	*	* * *	-	-
Huang et.al. [82]	**	**	-	-	-	*	**	-	* * *	-	-
Restuccia et.al. [64]	* * *	* * *	-	-	* * *	**	*	* * *	*	-	-
Michalas et.al. [102]	*	-	-	-	-	**	*	-	*	-	-
Gisdakis et.al. [103]	**	-	-	-	-	**	*	*	*	-	-

* Weak	** Semi Robust	* * * Robust
- Attack not addressed		

Corr	Corruption	Col	Collusion	Ree	Re-entry	Dis	Discrimination	Onof	On-off	GPS	GPS Spoofing
Lag	Reputation Lag	Unf	Unfair rating	Bad	Badmouthing	Ball	Ballot stuffing	Syb	Sybil		

tack. The systems presented in [95, 97, 59] are considered as examples of such systems.

Collusion. Collusive participants are supposed to coordinate their behaviors to achieve some malicious goals. However, trust systems adopt different algorithms that rely on consensus to measure the consistency of the participants' contributions compared with the contributions of other participants for the same task. These algorithms comprise of consensus algorithms [80], similarity measures [58], deviation from common values [81], or outlier detection algorithms [96, 78, 101]. These methods fail to properly evaluate the contributions while collusion is committed. Trust systems can provide resistance to collusion given that the number of well-behaved participants is larger than the number of collusive ones. Therefore, most trust systems are considered to defend weakly against collusion attack except [64] which is considered robust. This system compares the contributions with the one which received from a secure agent. Thus, it is resistant to collusion attack.

Sybil. Sybil attack can be launched if a participant has the ability to obtain different identification parameters. In [59], the authors address the Sybil attack. They try to analyze the system statistically in order to detect the existence of a Sybil nodes. Thus, this system is considered robust against this attack. Furthermore, the Sybil attack was mentioned by the authors in [58]. The authors suggest that the participants commit some limited resource while logging into the system. However, this solution is considered weak for such an attack. In addition, we consider trust systems which adopt some authentication mechanism as semi robust to defend against this attack [103, 102, 82], since participants still have the ability to obtain different identities unless a strong biometric authentication technique is applied. The rest of existing systems don't address this attack.

Re-entry. A re-entry attack occurs when a participant with a low reputation score leaves the system and rejoins using different identification parameters. Therefore, the attacker has the ability to avoid the consequences of his/her bad behaviors. However, this attack was not considered by any of the current reputation based trust systems in participatory sensing.

GPS spoofing attack. The system presented in [64] is considered robust against this attack. Depending on a trusted mobile secure agent enables the system to define the most accurate sensed data in the sensing area. Thus, the system can easily define dishonest participants who share inconsistent information with the sensing area. Existing trust systems that can accurately assess the quality of participant's contribution weakly defend against this type of attack [34, 78, 101, 96]. Additionally, trust systems that don't consider the quality of participant's contribution can't defend against this attack.

Unfair Rating attack. Most of the current reputation based trust systems for participatory sensing is considered weak against the unfair rating attack. Some systems allow participants to share their contributions anonymously, so that a rater has no motivation to commit unfair ratings against an anonymous participant. One of trust systems that defend against unfair ratings attack through anonymity preservation is presented in [58]. Some other systems try to overcome unfair rating attack by trying to mitigate its effect. Since the participants with high reputation scores are more likely to be honest, these systems use the reputation score of the rater as a weight for the score which he submits. These systems (e.g., [79, 78, 101]) are thus considered semi robust against the unfair rating attack. The systems (such as [59]) that adopt the rating methodology without consideration for the degree of honesty of the rater are weak against this attack.

Others. Bad mouthing, ballot stuffing, and discrimination attacks are not addressed by any of existing trust systems in participatory sensing.

8.4. Comparison of Reputation based Trust Systems

A comparison of the reputation based trust systems is shown in Table 4. This table indicates how each phase in the reputation based trust system is implemented according to the system's phases illustrated in Section 6.2 and summarized in Figure 8. We focus on the particularities which characterize the implementation of each of existing trust system individually.

9. Future Research Directions

Trust systems have been a focus of research for a number of years in various application domains. However, trust management in the context of participatory sensing systems is still an area where research is in its infancy. There are a number of open issues that need to be resolved. Firstly, the devices of participants usually have limited resource capabilities. Secondly, according to our study, many trust goals have not been satisfied yet. Thirdly, many types of attacks haven't been treated. Additionally, each of the current trust systems treats only a few of the many issues which should be considered in such environments. In this section, we highlight the unsolved research challenges of trust systems for participatory sensing.

1. *Attacks:*
   In Section 3.1, we discussed the possible attacks in participatory sensing. The resistance of existing trust systems under each one of the addressed attack is discussed in Section 8.3. From this study, we can conclude that many types of attacks haven't been addressed yet. These include discrimination, re-entry, bad mouthing, and ballot stuffing attacks. Moreover, the defense mechanisms for some other types of attacks, such as Sybil and unfair rating, are still in their infancy. We can also observe that most reputation systems are mainly concerned with detecting malicious participants who commit corruption attacks that may disrupt the application server. However, much less attention has been directed toward other types of attacks.
2. *Privacy:*
   Trust systems in participatory sensing applications seek to identify malicious participants who contribute corrupted, fabricated, or erroneous contribution. Malicious participants should be discarded during the task assignment phase and their contributions should be excluded through the campaign. These goals conflict with the objectives of preserving the privacy and anonymity of the participants. This issue was mainly considered by reputation based trust systems as presented in Section 6.1. The systems presented in [82, 35, 111, 107, 102] are concerned with this issue. However, privacy was rarely considered by TPM trust systems (Scetion 5.2) [86]. Most of privacy preserving reputation systems in participatory sensing depend on the group signature [**?**], anonymization [**?**], and blind signature [105] to preserve the identity of participant. However, there are other techniques applied on literature for privacy preservation within a reputation systems such as anonymous credential systems [**?**], Zero knowledge proof [**?**]. It is clear that the compromise between conflicting goals of both trust assessment and privacy preservation still needs a lot of work to be assured.
3. *Reputation Mapping:*
   As we described in Section 6.2.2, existing reputation based systems adopt either Gompertz function [94] or Bayesian model [93] as a reputation mapping functions. Although Gompertz function offers better capabilities for tracing participants' behaviors more than Bayesian model, both of these functions still don't assure the guarantees of a robust and reliable trust assessment system. Different mapping functions were used in literature of trust [75]. However, various other reputation mapping function can be adopted which may better fit with participatory sensing such as gamma or weibull distribution model.
4. *User and environment centricity:*
   As mentioned in [24] and explained in Section 2, participatory sensing applications may be either personal centric or environment centric. In personal centric applications, sensitive information about a participant is transferred to the application server, which may then give feedback, advice, or new sensing commands to the participant. In this case, the participant needs to ensure the trustworthiness of the application server in order to share his/her sensitive information. However, in environment centric applications, contributions are captured from the surrounding environment and forwarded to the application server. The server uses these contributions for analyzing or mapping some phenomena. In contrast, this scenario makes it important for the application server to assess the trustworthiness of the participants. Hence, a trust system should ideally manage trust for both these types of applications. To the best of our knowledge, existing trust systems focus on trust from the environment centric applications point of view. This problem has not been addressed by any of the current systems.
5. *Ensuring the trustworthiness of different parties:*
   As mentioned in [47] and discussed in Section 2, different parties need to be considered in participatory sensing applications. Each party has his own capabilities and concerns which differ according to the application. In addition, each one has the ability to tamper with the sensing campaign. Accurately assessing the trustworthiness of all stakeholders is vital for the normal functioning of participatory sensing campaigns.
6. *Measuring the quality of contributions:*
   In participatory sensing, trust systems usually adopt some consensus or outlier detection algorithms such as [90, 89]. These methods have the ability to measure the deviation of the contribution from a common consensus. However, the quality estimation is biased if the majority of participants are malicious. Therefore, measuring the quality of

Table 4: Comparison of reputation based trust systems

Scheme	Information Collection				Mapping		Dissemination		Decision		
	Source	Type	WDM	Attack	Structure	Approach	Structure	Approach	Value	Type	Reward/Penalize
Reddy et.al. [95]	M/D	+,-	N	G	Cen	Pr	-	-	Cont	B	N
Reddy et.al. [97]	D	+,-	N	G	Cen	Pr	-	-	Cont	B	N
Yang et.al. [104]	D/I/M	+,-	Y	G	-	-	-	-	Disc	B	N
Huang et.al. [80, 34]	M/D	-	Y	Corr	Cen	De	-	-	Cont	F	Y
Jkalidindi et.al. [79]	M/D/I	+,-	N	G	Cen	De	Dis	Re	Cont	B	N
Manzoor et.al. [81]	M/D	-	Y	Corr	Cen	Pr	-	-	Cont	F	N
Amintoosi et.al. [96]	M	-	N	G	Cen	De	Cen	-	Cont	B	N
Amintoosi et.al. [78, 99]	M/I	+,-	N	G	Cen	De	Cen	-	Cont	B	Y
Amintoosi et.al. [101]	M/I	+,-	N	G	Cen	De	Cen	-	Cont	B	Y
Chang et.al. [59]	M/I	+,-	N	Sybil	Cen	-	Cen	Re	Cont	B	N
Wang et.al. [58, 35]	M/D	-	Y	G	Cen	De	-	-	Disc	B	N
Huang et.al. [82]	D	+,-	Y	G	Cen	De	-	-	Cont	B	N
Restuccia et.al. [64]	M/D	-	Y	GPS	Cen	De	-	-	Disc	B	Y
Michalas et.al. [102]	I	-	N	G	Cen	-	-	-	-	B	N
Gisdakis et.al. [103]	M	-	Y	G	Cen	-	-	-	-	B	N

Y,**N**,**-**	Yes, No, Not mentioned	Dis	Distributed	**+,-**	Positive, Negative Feedback	**B**	Binary
D	Automatic Direct	**Cen**	Centralized	**Disc, Cont**	Discrete, Continuous	**F**	Fusion
I	Automatic Indirect	**De**	Deterministic	**Pr**	Probabilistic	**M**	Manual
GPS	GPS Spoofing attack	**Corr**	Corruption attack	**G**	General Misbehavior	**Re**	Reactive

the participants' contributions is one of the biggest challenges that face trust systems in participatory sensing applications.

7. *Resource overhead:*
   Applying trust systems requires loading the system entities with additional overhead. This overhead may be additional battery consumption or computational power. This overhead is often critical for the different entities in the system, especially the participants who are usually equipped with smartphones or other computational devices with limited capabilities. Most trust systems in the participatory sensing domain have not discussed this issue. Therefore, further research should be directed toward studying and reducing the resource overhead of trust systems.
8. *Scalability:*
   In participatory sensing systems, a large number of contributions is required to enable the system to carry out a stable measurement and analysis for the phenomenon under consideration. Thus, a large number of participants is usually required in sensing campaigns. Moreover, numerous message exchanges are required by each participant to accomplish a sensing campaign. Therefore, the performance of these systems may degrade due to the addition of more participants to the system. Consequently, management of trust and reputation for large scale participatory sensing systems is an issue that should be addressed by the future work.

10. Related Work

Trust management has been studied extensively in various domains of distributed computing.

In wireless sensor networks, sensor nodes may share corrupted data due to damage or malfunctioning sensor or problems in the communication between the node and the sink node. Therefore, monitoring the behavior of nodes is essential in order to detect any deviation from the normal nodes' behavior [31][32][33].

In peer to peer systems, the network is established from several distributed peers with equal privilege. Those peers should share the available resources as well as the workload. The peers are allowed to join and leave the system at any time. P2P systems don't include a central management unit that should assure the security and trust issues among the peers. Thus, P2P systems is vulnerable to malicious peer behaviors [27].

Mobile Ad-hoc Networks are structureless and dynamic networks since these networks consists of mobile nodes that have no fixed link between them. These networks have a dynamic topology and no stable structure. Users can join and leave the network within a random period of time affecting the energy, bandwidth, and memory computations of the network. Managing trust in these networks is a crucial task because many activities such as routing rely heavily on the cooperation and trustworthiness of the users [28, 29, 30].

Trust should be maintained on online applications (e.g. E-commerce) to encourage the buyers to perform transactions with the sellers. The trust score assigned to a seller enables the buyer to estimate the trustworthiness of the provided service [75].

Mobile social networks are a specific type of social network that seek to merge the merits of both social networks and opportunistic networks. Mobile social network users are able to share and access user-centric data using their mobile devices. Najaflou et al.[113] define the trust-related and other attacks faced by these systems and study the state of the art in this domain.

In this paper, we are concerned with participatory sensing. Participants, in these applications, can provide the application server with either forged or corrupted contributions which subsequently disrupt the application measurements. Subsequently, assessing the trust of participants is a a crucial task. We dis-

cussed the attacks of these systems. We then study, classify, compare, and conclude existing trust systems. We finally draw a research agenda for trust assessment in participatory sensing.

11. Conclusion

Participatory sensing systems are an emerging type of systems that seek to achieve welfare in different areas of human life. Applications of participatory sensing systems enable humans to save time (e.g., by sensing traffic), improve their health (e.g., by monitoring their health status), and live more luxury lives (e.g., by documenting their daily activities), etc. These systems exploit the mobile phones of regular citizens for capturing and sharing their sensed data. However, involving regular citizens in the sensing campaigns exposes these systems to tremendous challenges. The main challenge is the uncertainty of the participants behaviors, because different attacks can be launched from misbehaved participants. Consequently, trust systems have been proposed to detect the misbehaved participants and/or at least to mitigate the effect of their misbehavior.

In this paper, we addressed trust assurance among stakeholders in participatory sensing systems. We started by presenting a general architecture of these systems, identifying how the trust assessment process is incorporated into such participatory systems. We then deduced the threat model that describes different types of attacks and misbehavior in participatory sensing systems. In addition, we discussed these attacks and explained how they can affect these systems. The notion and characteristics of trust were discussed as a solution to defend against participants' misbehavior in different networked applications. Subsequently, we proposed a classification of the existing trust systems in participatory sensing applications. This classification has three major categories i.e. distribution, methodology and anonymity. We observed that the current trust systems can be classified mainly into TPM based and reputation based systems. We provided in depth analysis of each type of these systems. Then, we investigated the current state-of-the-art of trust management in participatory sensing systems. Furthermore, we presented a general analysis and comparisons of the existing systems, which we hope will help elucidate the current state-of-the-art of this domain for researchers as well as system designers. Finally, we identified the open challenges that need to be addressed by future work on trust systems in participatory sensing.

12. Acknowledgements

This work is supported by the regional ARC 7 2012 APDR Project.

13. References

[1] Cisco, its affiliates, Cisco visual networking index: Global mobile data traffic forecast update 2013 2018, Tech. rep.

[2] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M. B. Srivastava, Participatory sensing, in: Workshop on World-Sensor-Web (WSW 06): Mobile Device Centric Sensor Networks and Applications, 2006, pp. 117–134.

[3] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A. T. Campbell, A survey of mobile phone sensing, Communications Magazine, IEEE 48 (9) (2010) 140–150.

[4] M. Annavaram, N. Medvidovic, U. Mitra, S. Narayanan, G. Sukhatme, Z. Meng, S. Qiu, R. Kumar, G. Thatte, D. Spruijt-Metz, Multimodal sensing for pediatric obesity applications, in: Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense), 2008, pp. 21–25.

[5] T. Denning, A. H. Andrew, R. Chaudhri, C. Hartung, J. Lester, G. Borriello, G. Duncan, Balance: towards a usable pervasive wellness application with accurate activity inference, in: HotMobile, 2009.

[6] E. Kanjo, J. Bacon, D. Roberts, P. Landshoff, Mobsens: Making smart phones smarter, Pervasive Computing, IEEE 8 (4) (2009) 50–57.

[7] L. Nachman, A. Baxi, S. Bhattacharya, V. Darera, N. Kodalapura, V. Mageshkumar, S. Rath, R. Acharya, Jog falls: A pervasive healthcare platform for diabetes management, in: Pervasive Computing, Vol. 6030, 2010, pp. 94–111.

[8] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, Peir, the personal environmental impact report, as a platform for participatory sensing systems research, in: MobiSys09, Krakw, Poland, 2009.

[9] P. Mohan, V. N. Padmanabhan, R. Ramjee, Nericell: Rich monitoring of road and traffic conditions using mobile smartphones, in: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, SenSys '08, ACM, New York, NY, USA, 2008, pp. 323–336.

[10] R. K. Ganti, N. Pham, H. Ahmadi, S. Nangia, T. F. Abdelzaher, Greengps: A participatory sensing fuel-efficient maps application, in: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, MobiSys '10, ACM, New York, NY, USA, 2010, pp. 151–164.

[11] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, Q. Jacobson, Virtual trip lines for distributed privacy-preserving traffic monitoring, in: Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services, MobiSys '08, ACM, New York, NY, USA, 2008, pp. 15–28.

[12] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, J. Eriksson, Vtrack: Accurate, energy-aware road traffic delay estimation using mobile phones, in: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys '09, ACM, New York, NY, USA, 2009, pp. 85–98.

[13] N. Maisonneuve, M. Stevens, B. Ochab, Participatory noise pollution monitoring using mobile phones, Information Polity 15 (1,2) (2010) 51–71.

[14] R. K. Rana, C. T. Chou, S. S. Kanhere, N. Bulusu, W. Hu, Ear-phone: An end-to-end participatory urban noise mapping system, in: Proceeding of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN10),, Stockholm, Sweden, 2010, pp. 105–116.

[15] E. Paulos, R. Honicky, E. Goodman, Sensing atmosphere, in: SenSys 2007, Sydney, Australia., 2007.

[16] E. A. Garcia, R. F. Brena, Real time activity recognition using a cell phone's accelerometer wi-fi., in: Intelligent Environments (Workshops), Vol. 13 of Ambient Intelligence and Smart Environments, IOS Press, 2012, pp. 94–103.

[17] T. Choudhury, G. Borriello, S. Consolvo, D. Haehnel, B. Harrison, B. Hemingway, J. Hightower, P. P. Klasnja, K. Koscher, A. LaMarca, J. A. Landay, L. LeGrand, J. Lester, A. Rahimi, A. Rea, D. Wyatt, The mobile sensing platform: An embedded activity recognition system, IEEE Pervasive Computing 7 (2) (2008) 32–41.

[18] G.-S. Ahn, M. Musolesi, H. Lu, R. Olfati-Saber, A. T. Campbell, Metrotrack: Predictive tracking of mobile events using mobile phones, in: Proceedings of the 6th IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS'10, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 230–243.

[19] S. Consolvo, D. W. McDonald, T. Toscos, M. Y. Chen, J. Froehlich, B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I. Smith, J. A. Landay, Activity sensing in the wild: A field trial of ubifit garden, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '08, ACM, New York, NY, USA, 2008, pp. 1797–1806.

[20] N. Győrbíró, A. Fábián, G. Hományi, An activity recognition system for mobile phones, Mobile Networks and Applications 14 (1) (2009) 82–91.

[21] Y. F. Dong, S. Kanhere, C. T. Chou, N. Bulusu, Automatic collection

of fuel prices from a network of mobile cameras, in: Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 140–156.

[22] L. Deng, L. P. Cox, Livecompare: Grocery bargain hunting through participatory sensing, in: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, HotMobile '09, ACM, New York, NY, USA, 2009, p. 4.

[23] K. Shilton, Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection, Communications of the ACM 52 (11) (2009) 48–53.

[24] W. Khan, Y. Xiang, M. Aalsalem, Q. Arshad, Mobile phone sensing systems: A survey, Communications Surveys Tutorials, IEEE 15 (1) (2013) 402–427.

[25] A. Jøsang, Trust and reputation systems, in: FOSAD, 2007, pp. 209–245.

[26] P. Resnick, K. Kuwabara, R. Zeckhauser, E. Friedman, Reputation systems, Communications of the ACM 43 (12) (2000) 45–48.

[27] C. Selvaraj, S. Anand, A survey on security issues of reputation management systems for peer-to-peer networks, Computer Science Review 6 (4) (2012) 145–160.

[28] Y. S. Renu Dalal, Manju Khari, Survey of Trust Schemes on Ad-Hoc Network, Advances in Computer Science and Information Technology. Networks and Communications, Part 1, second international conference, ccsit 2012, bangalore, india, january 2-4, 2012. proceedings, part i Edition, Vol. 84 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Berlin Heidelberg, 2012.

[29] J.-H. Cho, A. Swami, I.-R. Chen, A survey on trust management for mobile ad hoc networks, Communications Surveys Tutorials, IEEE 13 (4) (2011) 562–583.

[30] K. Ramana, A. A. Chari, N. Kasiviswanth, A survey on trust management for mobile ad hoc networks, in: International Journal of Network Security & Its Applications;Apr2010,, Vol. 2, 2, April 2010, p. 75.

[31] O. Khalid, S. U. Khan, S. A. Madani, K. Hayat, M. I. Khan, N. Min-Allah, J. Kolodziej, L. Wang, S. Zeadally, D. Chen, Comparative study of trust and reputation systems for wireless sensor networks, Security and Communication Networks 6 (6) (2013) 669–688.

[32] H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, A. Abuhaimed, Reputation-based trust systems for wireless sensor networks: A comprehensive review, in: IFIPTM, 2013, pp. 66–82.

[33] M. C. F. Gago, F. Martinelli, S. Pearson, I. Agudo (Eds.), Trust Management VII - 7th IFIP WG 11.11 International Conference, IFIPTM 2013, Malaga, Spain, June 3-7, 2013. Proceedings, Vol. 401 of IFIP Advances in Information and Communication Technology, Springer, 2013.

[34] K. L. Huang, S. S. Kanhere, W. Hu, On the need for a reputation system in mobile phone based sensing, Ad Hoc Networks 12 (2014) 130–149.

[35] X. O. Wang, W. Cheng, P. Mohapatra, T. Abdelzaher, Enabling reputation and trust in privacy-preserving mobile sensing, IEEE Transactions on Mobile Computing 99 (PrePrints) (2014) 1.

[36] A. Dua, N. Bulusu, W.-C. Feng, W. Hu, Towards trustworthy participatory sensing, in: Proceedings of the 4th USENIX Conference on Hot Topics in Security, HotSec'09, USENIX Association, Berkeley, CA, USA, 2009, pp. 8–8.

[37] A. Dua, W. Hu, N. Bulusu, Demo abstract: A trusted platform based framework for participatory sensing, in: Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, IPSN '09, IEEE Computer Society, Washington, DC, USA, 2009, pp. 419–420.

[38] E. Kanjo, Noisespy: A real-time mobile phone platform for urban noise monitoring and mapping, Mobile Networks and Applications 15 (4) (2010) 562–574.

[39] A. Thiagarajan, J. Biagioni, T. Gerlich, J. Eriksson, Cooperative transit tracking using smart-phones, in: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, SenSys '10, ACM, New York, NY, USA, 2010, pp. 85–98.

[40] Waze application (January 2015).
URL `https://www.waze.com/`

[41] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, M. Hansen, Image browsing, processing, and clustering for participatory sensing: Lessons from a dietsense prototype, in: Proceedings of the 4th Workshop on Embedded Networked Sensors, EmNets '07, ACM, New York, NY, USA, 2007, pp. 13–17.

[42] E. P. Stuntebeck, J. S. Davis, II, G. D. Abowd, M. Blount, Healthsense: Classification of health-related sensor data through user-assisted machine learning, in: Proceedings of the 9th Workshop on Mobile Computing Systems and Applications, HotMobile '08, ACM, New York, NY, USA, 2008, pp. 1–5.

[43] J. R. Kwapisz, G. M. Weiss, S. A. Moore, Activity recognition using cell phone accelerometers, SIGKDD Explor. Newsl. 12 (2) (2011) 74–82.

[44] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, A. T. Campbell, The bikenet mobile sensing system for cyclist experience mapping, in: Proceedings of the 5th International Conference on Embedded Networked Sensor Systems, SenSys '07, ACM, New York, NY, USA, 2007, pp. 87–101.

[45] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, A. T. Campbell, Bikenet: A mobile sensing system for cyclist experience mapping, ACM Transactions on Sensor Networks (TOSN) 6 (1) (2010) 6:1–6:39.

[46] T. A. Charu C. Aggarwal, Managing and Mining Sensor Data, Social Sensing, Springer US, 2013.

[47] D. Christin, A. Reinhardt, S. S. Kanhere, M. Hollick, A survey on privacy in mobile participatory sensing applications, Journal of Systems and Software 84 (11) (2011) 1928–1946.

[48] T. Dimitrakos, R. Moona, D. Patel, D. H. McKnight (Eds.), Trust Management VI - 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012. Proceedings, Vol. 374 of IFIP Advances in Information and Communication Technology, Springer, 2012.

[49] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, Security in Wireless Sensor Networks , Handbook of Information and Communication Security, Springer Berlin Heidelberg, 2010.

[50] A. Jøsang, J. Golbeck, Challenges for robust of trust and reputation systems, in: proceeding of the 5th International Workshop on Security and Trust Management (STM 2009), 2009.

[51] K. J. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Computing Surveys (CSUR) 42 (1).

[52] L. F. Perrone, S. C. Nelson, A study of on-off attack models for wireless ad hoc networks, in: First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm 2006), Berlin, Germany, 2006.

[53] Y. Chae, L. Cingiser Dipippo, Y. L. Sun, Trust management for defending on-off attacks.

[54] H. Alzaid, E. Foo, J. G. Nieto, E. Ahmed, Mitigating on-off attacks in reputation-based secure data aggregation for wireless sensor networks, Security and Communication Networks 5 (2) (2012) 125–144.

[55] S. Abbas, M. Merabti, D. Llewellyn-Jones, Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks, in: Wireless Days (WD), 2010 IFIP, 2010, pp. 1–6.

[56] M. Feldman, C. Papadimitriou, J. Chuang, I. Stoica, Free-riding and whitewashing in peer-to-peer systems, Selected Areas in Communications, IEEE Journal on 24 (5) (2006) 1010–1019.

[57] C. Marforio, A. Francillon, S. Capkun, S. Capkun, S. Capkun, Application collusion attack on the permission-based security model and its implications for modern smartphone systems, Department of Computer Science, ETH Zurich, 2011.

[58] X. O. Wang, W. Cheng, P. Mohapatra, T. F. Abdelzaher, Artsense: Anonymous reputation and trust in participatory sensing., in: INFOCOM, IEEE, 2013, pp. 2517–2525.

[59] S.-H. Chang, Y.-S. Chen, S.-M. Cheng, Detection of sybil attacks in participatory sensing using cloud based trust management system, in: Wireless and Pervasive Computing (ISWPC), 2013 International Symposium on, 2013, pp. 1–6.

[60] W. Wei, F. Xu, C. Tan, Q. Li, Sybildefender: Defend against sybil attacks in large social networks, in: INFOCOM, 2012 Proceedings IEEE, 2012, pp. 1951–1959.

[61] A. Mohaisen, N. Hopper, Y. Kim, Keep your friends close: Incorporating trust into social network-based sybil defenses, in: INFOCOM, 2011 Proceedings IEEE, 2011, pp. 1943–1951.

[62] D. Quercia, S. Hailes, Sybil attacks against mobile users: Friends and foes to the rescue, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–5.

[63] H. Yu, M. Kaminsky, P. Gibbons, A. Flaxman, Sybilguard: Defending against sybil attacks via social networks, Networking, IEEE/ACM Transactions on 16 (3) (2008) 576–589.

[64] F. Restuccia, S. K. Das, Fides: A trust-based framework for secure user incentivization in participatory sensing, in: A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on, IEEE, 2014, pp. 1–10.

[65] W. Premchaiswadi, W. Romsaiyud, N. Premchaiswadi, Navigation without gps: Fake location for mobile phone tracking, in: ITS Telecommunications (ITST), 2011 11th International Conference on, 2011, pp. 195–200. doi:10.1109/ITST.2011.6060051.

[66] A. Jhumka, M. Bradbury, M. Leeke, Fake source-based source location privacy in wireless sensor networks, Concurrency and Computation: Practice and Experience.

[67] L. Zhang, S. Jiang, J. Zhang, W. K. Ng, Robustness of trust models and combinations for handling unfair ratings, in: Trust Management VI, Springer, 2012, pp. 36–51.

[68] Y.-F. Yang, Q.-Y. Feng, Y. L. Sun, Y.-F. Dai, Dishonest behaviors in online rating systems: cyber competition, attack models, and attack generator, Journal of Computer Science and Technology 24 (5) (2009) 855–867.

[69] A. A. Irissappane, S. Jiang, J. Zhang, Towards a comprehensive testbed to evaluate the robustness of reputation systems against unfair rating attack., in: UMAP Workshops, Vol. 12, 2012.

[70] T. Dimitrakos, R. Moona, D. Patel, D. H. McKnight, Trust Management VI: 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012, Proceedings, Springer Publishing Company, Incorporated, 2012.

[71] Z. Banković, J. C. Vallejo, D. Fraga, J. M. Moya, Detecting badmouthing attacks on reputation systems using self-organizing maps, in: Proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems, CISIS'11, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 9–16.
URL http://dl.acm.org/citation.cfm?id=2023430.2023433

[72] Y. L. Sun, Z. Han, W. Yu, K. R. Liu, Attacks on trust evaluation in distributed networks, in: Information Sciences and Systems, 2006 40th Annual Conference on, IEEE, 2006, pp. 1461–1466.

[73] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thome, M. Turuani, P. Zimmermann, Ballot stuffing in a postal voting system, in: Requirements Engineering for Electronic Voting Systems (REVOTE), 2011 International Workshop on, 2011, pp. 27–36. doi:10.1109/REVOTE.2011.6045913.

[74] O. Hasan, Privacy Preserving Reputation Systems for Decentralized Environments, Thse de doctorat en informatique, INSA de Lyon (Sep. 2010).

[75] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems 43 (2) (2007) 618–644.

[76] D. Gambetta, Can we trust trust?, Trust: Making and breaking cooperative relations (2000) 213–237.

[77] L. B. Omar Hasan, Security and Privacy Preserving in Social Networks, 2190-5428, Springer Vienna, 2013.

[78] H. Amintoosi, S. S. Kanhere, A reputation framework for social participatory sensing systems, MONET 19 (1) (2014) 88–100.

[79] R. R. Kalidindi, K. V. S. V. N. Raju, V. V. Kumari, C. S. Reddy, Trust based participant driven privacy control in participatory sensing, CoRR abs/1103.4727.

[80] K. L. Huang, S. S. Kanhere, W. Hu, Are you contributing trustworthy data?: The case for a reputation system in participatory sensing, in: Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, MSWIM '10, ACM, New York, NY, USA, 2010, pp. 14–22.

[81] A. Manzoor, M. Asplund, M. Bouroche, S. Clarke, V. Cahill, Trust evaluation for participatory sensing, in: MobiQuitous, 2012, pp. 176–187.

[82] K. L. Huang, S. S. Kanhere, W. Hu, A privacy-preserving reputation system for participatory sensing, in: Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), LCN '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 10–18.

[83] T. C. Group, Tpm main specification (29 January 2015).
URL http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[84] T. C. Group, Trusted platform module (tpm) summary (2008).
URL https://www.trustedcomputinggroup.org/news/Industry_Data/TPM_applications_paper_March_28_2008.pdf.

[85] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth, L. P. Cox, Youprove: authenticity and fidelity in mobile sensing, in: SenSys, 2011, pp. 176–189.

[86] S. Saroiu, A. Wolman, I am a sensor, and i approve this message, in: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, HotMobile '10, ACM, New York, NY, USA, 2010, pp. 37–42.

[87] P. Gilbert, L. P. Cox, J. Jung, D. Wetherall, Toward trustworthy mobile sensing, in: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, HotMobile '10, ACM, New York, NY, USA, 2010, pp. 31–36.

[88] T. C. Group, Trusted platform modules strengthen user and platform authenticity (January, 2005).
URL http://www.trustedcomputinggroup.org/files/resource_files/8D46621F-1D09-3519-ADB205692DBBE135/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf

[89] M. M. Breunig, H.-P. Kriegel, R. T. Ng, J. Sander, Lof: Identifying density-based local outliers, SIGMOD Rec. 29 (2) (2000) 93–104.

[90] S. Papadimitriou, H. Kitagawa, P. Gibbons, C. Faloutsos, Loci: fast outlier detection using the local correlation integral, in: Data Engineering, 2003. Proceedings. 19th International Conference on, 2003, pp. 315–326.

[91] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, M. Hansen, Image browsing, processing, and clustering for participatory sensing: lessons from a dietsense prototype, in: in EmNets 07: Proceedings of the 4th workshop on Embedded networked sensors, ACM Press, 2007, pp. 13–17.

[92] A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures, Vol. 4677 of Lecture Notes in Computer Science, Springer, 2007.

[93] A. Jøsang, R. Ismail, The beta reputation system, in: In Proceedings of the 15th Bled Electronic Commerce Conference, 2002.

[94] F. J. Kenney, K. S. E., Mathematics of Statistics., 3rd Edition, part 1, Princeton, NJ: Van Nostrand, 1962.

[95] S. Reddy, K. Shilton, J. Burke, D. Estrin, M. Hansen, M. Srivastava, Evaluating participation and performance in participatory sensing, in: Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense 08),, 2008.

[96] H. Amintoosi, S. S. Kanhere, A trust framework for social participatory sensing systems, in: MobiQuitous, 2012, pp. 237–249.

[97] S. Reddy, D. Estrin, M. Srivastava, Recruitment framework for participatory sensing data collections, in: Proceedings of the 8th International Conference on Pervasive Computing, Pervasive'10, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 138–155.

[98] K. Zheng, M. Li, H. Jiang, K. Zheng, M. Li, H. Jiang (Eds.), Mobile and Ubiquitous Systems: Computing, Networking, and Services - 9th International Conference, MobiQuitous 2012, Beijing, China, December 12-14, 2012. Revised Selected Papers, Vol. 120 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, 2013.

[99] H. Amintoosi, S. S. Kanhere, Providing trustworthy contributions via a reputation framework in social participatory sensing systems., CoRR abs/1311.2349.

[100] L. Page, S. Brin, R. Motwani, T. Winograd, The pagerank citation ranking: Bringing order to the web.

[101] H. Amintoosi, S. S. Kanhere, A trust-based recruitment framework for multi-hop social participatory sensing, in: Proceedings of the 2013 IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 266–273.

[102] A. Michalas, N. Komninos, The lord of the sense: A privacy preserving reputation system for participatory sensing applications, in: Computers and Communication (ISCC), 2014 IEEE Symposium on, IEEE, 2014, pp. 1–6.

[103] S. Gisdakis, T. Giannetsos, P. Papadimitratos, Sppear: security &

privacy-preserving architecture for participatory-sensing applications, in: Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks, ACM, 2014, pp. 39–50.

[104] P. R. HaoFan Yang, Jinglan Zhang, Using reputation management in participatory sensing for data classification, in: Procedia Computer Science, The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011) / The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011), Vol. 5, 2011, pp. 190–197.

[105] D. Chaum, Blind signatures for untraceable payments, in: Advances in cryptology, Springer, 1983, pp. 199–203.

[106] A. Jøsang, An algebra for assessing trust in certification chains., in: NDSS, Vol. 99, 1999, p. 6th.

[107] L. Kazemi, C. Shahabi, Tapas: Trustworthy privacy-aware participatory sensing, Knowl. Inf. Syst. 37 (1) (2013) 105–128.

[108] L. Kazemi, C. Shahabi, A privacy-aware framework for participatory sensing, ACM SIGKDD Explorations Newsletter 13 (1) (2011) 43–51.

[109] O. Hasan, L. Brunie, E. Bertino, N. Shang, A decentralized privacy preserving reputation protocol for the malicious adversarial model, Information Forensics and Security, IEEE Transactions on 8 (6) (2013) 949–962.

[110] O. Hasan, L. Brunie, E. Bertino, Preserving privacy of feedback providers in decentralized reputation systems, Computers & Security 31 (7) (2012) 816–826.

[111] D. Christin, C. Rosskopf, M. Hollick, L. Martucci, S. Kanhere, Incognisense: An anonymity-preserving reputation framework for participatory sensing applications, in: Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on, 2012, pp. 135–143.

[112] W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks, ACM Comput. Surv. 45 (4) (2013) 47:1–47:33.

[113] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang, M. S. Obaidat, Safety challenges and solutions in mobile social networks., CoRR abs/1310.5949.