Computer Networks 120 (2017) 157–169

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

FIDC: A framework for improving data credibility in mobile crowdsensing

Tongqing Zhou[a,*], Zhiping Cai[a,c], Kui Wu[b], Yueyue Chen[a], Ming Xu[a]

[a] College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China
[b] Department of Computer Science, University of Victoria, Victoria, BC, Canada
[c] School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, Jiangsu 210044, China

ARTICLE INFO

Article history:
Received 9 October 2016
Revised 26 February 2017
Accepted 7 April 2017
Available online 8 April 2017

Keywords:
Mobile crowdsensing
Data credibility
Provenance information
Data clustering
Logical reasoning

ABSTRACT

Mobile crowdsensing has become a popular paradigm to collaboratively collect sensing data from pervasive mobile devices. Since the devices used for mobile crowdsensing are owned and controlled by individuals with unpredictable reliability, varied capabilities, and unknown intentions, data collected with mobile crowdsensing may be untrustworthy. In particular, a mobile crowdsensing system is subject to collusion attacks where a group of malicious participants collaboratively send fake information to mislead the system. Defending against collusion attacks requires stronger defense mechanisms not available in existing works. In this paper, we propose a new framework for improving data credibility, named FIDC, in mobile crowdsensing to alleviate the threats posed by collusion attacks. FIDC seamlessly integrates two types of correlations: the spatial correlation of sensing data and the correlation between sensing data and provenance knowledge. While both correlations have been adopted separately in previous crowdsensing systems, the exploitation of an joint effort in FIDC poses a special technical challenge to fine-tune the performance. Evaluated extensively with a public mobile crowdsensing data for temperature monitoring, FIDC outperforms existing methods with respect to false detection accuracy and overall data credibility.

1. Introduction

The past few years have witnessed the massive prevalence of human-carried smart devices. These devices are equipped or connected with a rich set of powerful embedded sensors, such as GPS, wireless interface, and air quality monitor. Such advancements lead to a new sensing paradigm, known as mobile crowdsensing (MCS) [1] or participatory sensing [2], where individuals use their own mobile devices to perform sensing tasks, and collect environmental data for specific applications running in the cloud-based platform. So far, a broad spectrum of MCS applications have been developed, including environment monitoring [3], city management [4], network measurement [5], and many more.

A major concern of MCS is on the credibility of collected sensing data [6]. MCS relies on mobile devices of individuals with unknown trustworthiness, varied capabilities, and different intentions to perform sensing tasks. In fact, it has been reported that participants may submit measurements with random values to get rewarded with minimal effort [7]. Even worse, dishonest individuals may inject deliberately fabricated data to mislead the system. As shown in Fig. 1, dishonest participants could corrupt the collected data, which results in incorrect data analysis results. If the data credibility problem remains, the MCS system would eventually become a Garbage-in-Garbage-out (GIGO) system or a system serving for illegitimate purposes. For example, in a noise monitoring application, a real estate agent may submit false noise readings with lower values regarding a specific region to promote the sale of their own properties. Overall, it is critical to ascertain data credibility in nearly all MCS applications.

While extensive research has been devoted to addressing the data credibility problem [8–10], the problem is kept largely open when the system is under collusion attacks, i.e., a group of malicious participants work together to mislead the system into making a wrong decision [11]. Specifically, for those schemes relying on the correlation characteristics of collected data to discover abnormal data [8], collusively contributed false data can be neither filtered out as outlier nor identified with majority voting. Consequently, exploiting data characteristics alone is not able to guarantee data credibility. On the other hand, building trust on the provenance (i.e., the derivation history) is suitable for the evaluation of binary observation [9,10], but not effective for decimal data, which is a more common data format under collusion attacks. For example, it is easy to find support for

* Corresponding author.
E-mail addresses: zhoutongqing@nudt.edu.cn, zhoutongqing1991@163.com (T. Zhou), zpcai@nudt.edu.cn (Z. Cai), wkui@uvic.ca (K. Wu), yueyuechen@nudt.edu.cn (Y. Chen), xuming@nudt.edu.cn (M. Xu).

http://dx.doi.org/10.1016/j.comnet.2017.04.015
1389-1286/

observation "high temperature", but difficult to find support for data "temperature = 20°C". No single solution works well under potential collusive threat, and this motivates our work.

In this work, by jointly exploiting data characteristics and provenance knowledge, we propose a novel framework to improve data credibility, named FIDC, for MCS applications. Specifically, FIDC is designed to mitigate a set of data falsification attacks which aim at compromising data aggregation process of existing systems. FIDC takes advantage of spatial correlation of sensing data and credibility metric regarding provenance[1] information. Intuitively, spatial correlation could be explored to provide discrete groups for provenance based credibility evaluation. On the other hand, provenance knowledge includes those information independent to the collected data, which makes provenance-based credibility assessment immune to collusion attacks. Hence, we could integrate spatial correlation and data-provenance correlation in a data distilling-and-filtering manner.

The major technical challenges of the integration include: (1) how to prepare proper discrete data groups by analyzing spatial correlation, and (2) how to evaluate the credibility of these groups (instead of data points) with provenance knowledge. In view of the above challenges, FIDC first introduces a clustering algorithm to exploit spatial correlation, which would formally separate data into different groups. Further, FIDC refers to provenance of two dimensions: participant provenance (reputation) and context provenance (co-located events), and leverages these information to calculate a credibility score for each group and distinguish the corrupted part. In this way, the integration is properly organized to improve the overall credibility of collected data and effectively defend against collusion attacks.

The main contributions of this paper include:

1) We propose FIDC to defend against the potential data falsification threats. In FIDC, both spatial correlation of data dimension and correlation between sensing data and provenance knowledge (w.r.t. user reputation and context) are studied to improve overall data credibility.
2) A clustering algorithm is utilized to analyze correlation characteristics of collected data; participants reputation together with context information are introduced to constitute a credibility metric to guide the false filtering process.
3) We extensively evaluate our proposed framework with synthetic traces of temperature measurements. Results show that FIDC achieves high credibility of sensing data under the collusion attacks.

2. Related work

MCS is a new sensing paradigm functionally extending the idea of traditional wireless sensor networks (WSNs). With data collection as the core mission, reliability issues of collected data in WSNs [12,13] have been well studied [14]. For example, Zhu et al. [15] propose a vote-based solution to detect injected false data packets by checking endorsements of the co-located nodes. In [16], a clustering algorithm is used to detect anomaly. While solutions in WSNs are instructive to the study of data credibility in MCS, influences of human involvement and corresponding threats (e.g., collusion attack) must be carefully considered. In addition to the studies in the context of WSNs, some recent works have focused on assuring data credibility for MCS, which can be roughly categorized into model-based schemes and false detection-based schemes, as shown in Fig. 2.

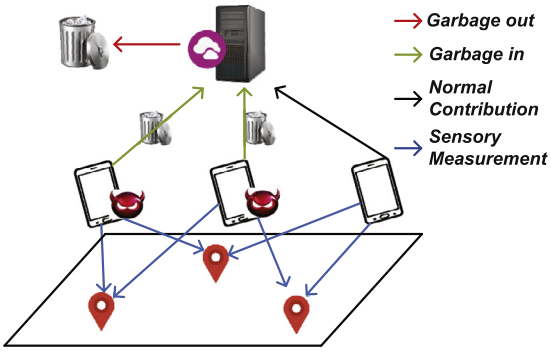


Fig. 1. An example of MCS application with dishonest participants involved in data collection. The contributions of dishonest participants are essentially garbage data. As a result, the output using the garbage data may be useless or misleading, turning the application to a Garbage-in-Garbage-out (GIGO) system.

2.1. Model-based schemes

Model-based schemes build a system to assess the credibility of collected data. Social factors are introduced to estimate data credibility in [17–19]. In these solutions, social relationship is used to describe how dependable one data source is [17], or initiate a voting on collected data among the participants by providing an interaction network [18]. In fact, having all participants in a single social group is not feasible and limits the amount of participants for an application.

In [9] and [10], provenance information is first introduced to assist the trust assessment process. Provenance is a set of user information and contextual factors that describe the origin of the collected data. Modeling and evaluating the corresponding provenance can yield an comprehensive understanding of data credibility. As one type of provenance, users' reputation information often acts as a metric of the trustworthiness of the sensing data [20,21]. To calculate participants' reputation, empirical models (e.g., Gompertz function) are adopted to estimate one's cooperative level based on their behavior in the history. In view of the context provenance, Wang et al. [10] point out that multiple events observed during a short period or at the same location share logical relations. So they propose to evaluate data credibility based on the support of co-located events. However, it is not easy to set a trust threshold to formally distinguish false and normal contribution, because contribution with more support could also be abnormal. Consequently, such solutions are not adequate for autonomous false detection.

2.2. False detection-based schemes

False detection-based solutions try to improve data credibility through identifying and discarding the false data. Techniques in this category include TPM-based schemes, location attestation-based schemes, and data analysis-based schemes.

In [22] and [23], Trusted Platform Module (TPM) is adopted to ensure that data sensed by a mobile sensor and reported to an application server are indeed captured by authentic and authorized devices within the system. In other words, sensing data that fail to pass the authenticity check are considered false. However, the embedded trust module is not readily available for most mobile devices, and malicious participants can cause distortion of the measurements by deliberately initiating sensing action.

As location being a common tag for sensor measurements, validating location can achieve a certain degree of reliability of the

[1] Provenance knowledge could be in many different forms. Its intuitive meaning refers to some extra knowledge known before hand. For instance, in an air pollution monitoring system, the provenance knowledge could be a news report of gas leak in a region.

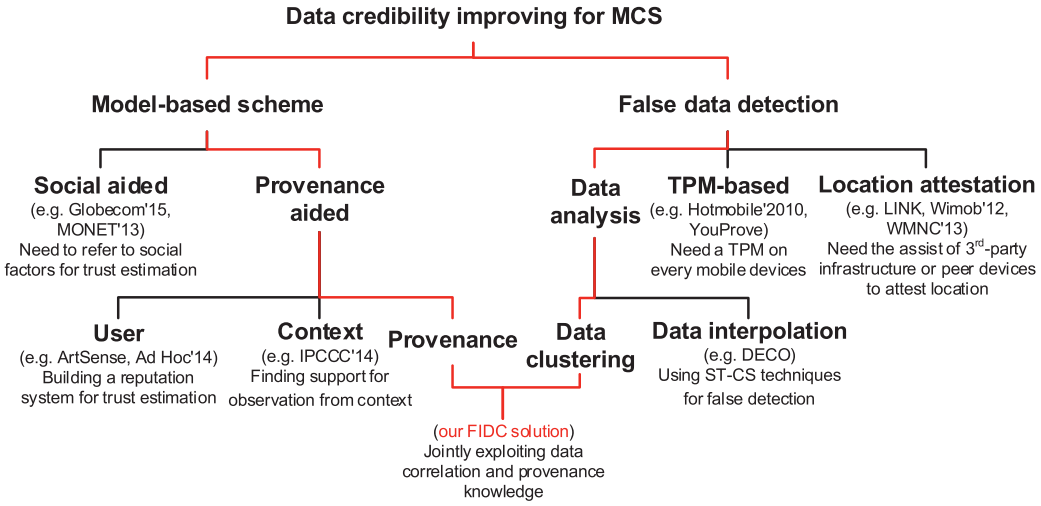


Fig. 2. Classification of MCS data credibility improving schemes.

sensing data [24]. Based on this idea, a series of approaches have been proposed, which can be classified as infrastructure-based schemes [25] and peer-assisted schemes [26]. Sastry et al. [25] propose to verify location with a challenge-response method, namely, it considers one contribution as valid only when its contributor can respond in constrained time. A peer-assisted scheme is proposed in [26] to validate user's location based on the verification from co-located users connected by bluetooth. Such solutions require either infrastructure support or neighbors' involvement, and add a high overhead on sensor devices. Moreover, those schemes implicitly ignore the case where dishonest participants submit fake data from valid locations.

In essence, false measurements could be considered as corrupted data. Hence, proper data analysis techniques should be a good choice to detect the abnormal and find the truth. Cheng et al. [8] propose a false detection and correction algorithm based on spatial-temporal compressive sensing (ST-CS). They assume that the data from low reputation participants are suspicious, and make the judgment by comparing the data with reconstruction values to tell whether they are notably different. Alternatively, Meng et al. [27] point out that correlations exist ubiquitously among entities, and correlated entities (e.g., observations in the same area or during a short period) have similar values. As such, they formalize an optimization problem to discover truth by minimizing the discrepancy between observations of entities. Expectation Maximization algorithm is used in [28] to solve a maximum likelihood estimation problem, and find observations that meet a specific probability of correctness. These techniques detect abnormal (or find truth) by exploiting the correlation among collected data. Clearly, they would lead to misleading conclusion when the false data are from a group of malicious participants.

Like [9] and [10], FIDC considers provenance information, while both user and contextual factors are utilized as the classifier of normal and false ingredient. Similar with [8] and [27], spatial correlation is exploited in FIDC, while clustering algorithm is used to analyze data characteristics. As shown in Fig. 2, FIDC is unique, since no similar method before has integrated both provenance information and spatial correlation in one solution.

3. Preliminaries

3.1. System model

We consider a typical mobile crowdsensing architecture shown in Fig. 3. It consists of a cloud-based platform and a set of participants $U = \{u_1, \ldots, u_N\}$ that perform sensing task T at location L. Typically, T is carried out in three stages: (1) task allocation to the participant crowd, (2) task execution with devices of the crowd, and (3) crowd data utilization by the application server. Over the platform, data credibility is considered an crucial part of the utilization stage, and data falsification threats are common as the crowd participants may have different purposes. A sensing task normally specifies multiple modalities of sensing data to be collected, so we consider that the collected data in MCS application are multi-dimensional numerical readings (e.g., temperature, noise level).

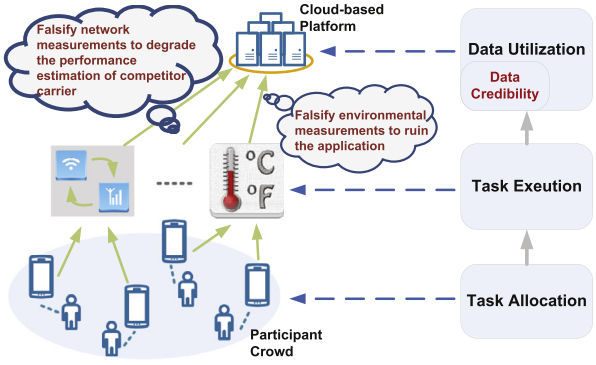


Fig. 3. Architecture of typical MCS applications. To facilitate a better understanding of data credibility issues, network measurement and temperature monitoring are depicted as two illustrative example applications with potential credibility threats.

During the execution of task T, u_i collects measurements with K different types of sensor, where each value of a measurement can be denoted by $s_i(k)$, where $i \in [1, N]$, and $k \in [1, K]$. Sensing data are submitted together with location $l_i \in L$ to the platform before time deadline. The contribution from u_i forms a tuple in key-value syntax, denoted as $d_i =< l_i, s_i >$. By the end of task execution, the cloud-based platform will obtain a data set $D = \{d_1, \ldots, d_N\}$, based on which some aggregation function f is performed to obtain conclusions.

3.2. False data in MCS

Data collected from individuals with unknown trustworthiness may be unreliable. The potentially erroneous or fabricated data would deviate the analytical result from the expected true value. Here we discuss the validity of data with respect to the validity of

Table 1
State space for the credibility of data with respect to validity of location l_i and validity of sensing measurement s_i.

$l_i \backslash s_i$	T	F
T	Normal data	Category A
F	Category B	Category C

its location and measurement component. We first explain several terms in data validity.

Definition 1. Announced location l_i of u_i is valid if it is within an acceptable distance from location l_c where u_i currently locates.

Definition 2. Sensing measurement s_i is valid if it represents the ground truth of the physical phenomenon of corresponding location l_i.

Definition 3. Data d_i is trustworthy (normal) if its location component l_i and sensing measurement component s_i are both valid.

Based on the above definitions, we can further represent the state space of credibility of data d_i with four categories as shown in Table 1, where symbol T (F) means the value in corresponding row (column) is true (false).

Note that location attestation-based schemes like [24] try to assure data credibility by detecting data with invalid location in category B and category C, ignoring possibly false data in category A. Unlike these schemes, we propose to improve overall credibility through identifying the group of data with invalid measurement. Meanwhile, we consider that the measurement data in category B are due to submission delay and thus valid data. Hence, the problem of detecting corrupted data in this paper is to identifying data in Category A and Category C.

3.3. Adversary model

We allow anyone with an appropriate device to be a participant. We consider that any participant may act maliciously and submit a false measurement. During the task, a dishonest participant is able to "fool" the sensors to create false readings (e.g., using the flame of a lighter to create the false impression of a high temperature). An adversary can also program the device to spoof the sensors' readings [29] or deliberately tamper the collected measurements. Moreover, a few adversaries may launch on-off attack, namely, they first send correct data to gain high reputation scores, then randomly send false sensing data to bypass the reputation-based detection techniques [30]. Assuming these threats and the possible false data described above, we consider two types of adversary model:

1) *Independent falsification*. Participants independently submit measurement data with random value to minimize their efforts, or tamper the measurements to mislead the system. For the latter intention, dishonest participants aim at deviating the aggregation result as much as possible.
2) *Collusive falsification*. A group of participants collude with each other to intentionally induce the final aggregation result to a wrong value by submitting false data with similar values [11]. Moreover, in order to avoid being detected by statistical analysis-based abnormal detection methods, the dishonest group is able to fabricate and submit data obeying normal distribution.

To be clear, we illustrate the adversary models regarding involved entities, their corresponding identities, and data validity in Fig. 4. The threats of both independent and collusive model arise from the data collection layer, wherein collusion among participants would result in a more significant deviation and the injected artificial data cannot be easily detected based on spatial correlation. Compared to existing works, such as Wang et al. [9] and Talasila et al. [24], we do not make any assumption or set any limitation on the number of dishonest participants in U. Under such assumption, vote-based false detection approaches are not effective any more as the amount of malicious participants may be larger than the honest group.

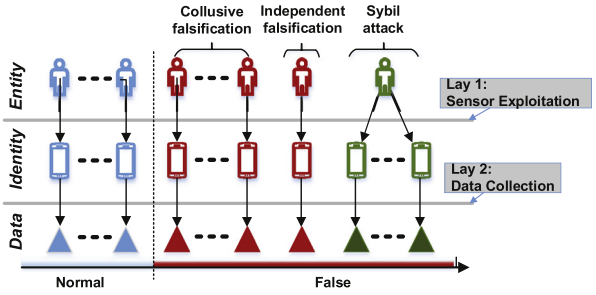


Fig. 4. A sketch of the adversary model. The model consists of three aspects, which could be divided using two layers. The sensor exploitation layer transforms physical entities into virtual sensors of MCS (i.e., identities), while the data collection layer aggregates data from the sensors. This work focuses on the assurance of data credibility, namely, the threat regarding Layer 2.

Besides, we also provide a discussion on Sybil attack, a particularly harmful attack in sensor networks [31]. As shown in Fig. 4, a Sybil attacker could generate multiple identities with only one physical device, and launch attack on data aggregation, or resource allocation. Especially, for MCS applications, these identities would: (1) constitute a malicious group to mislead the aggregation result (Layer 2), and in return, (2) earn the attacker additional reward and reputation (Layer 1). Hence, from the perspective of layer 2, Sybil attack is actually of no difference with collusive falsification, and if being successfully defended, would constitute no interference to the reward or reputation system.

3.4. Logical reasoning

Logical reasoning is the formal manipulation of the symbols representing a collection of known objects to produce representations of new ones. Logical reasoning generally involves an ontology, basic predicates, and knowledge base. Specifically, the underlying ontology can be time points, events (e.g., accident), and fluent (e.g., high temperature), while a predicate represents a property of or relation between ontology that can be true or false. Knowledge base contains general axioms describing the relations between predicates. Resolution is one of the most widely used calculi for theorem proving in logical reasoning. It proves a theorem by negating the statement to be proved and adding this negated goal to the sets of axioms that are known to be true to tell whether it leads to a contradiction.

In this work, we map and translate the sensing data collected during current MCS task into First Order Logic (FOL) predicates, and use resolution rules to tell whether the predicates are satisfiable by referring to the co-located events and basic knowledge base. We assume the basic knowledge base has been pre-established in a specific application scenario, and real-time computation only involves translating related events into predicates and add them to the reasoning knowledge base.

4. FIDC framework design

4.1. Overview

It is reasonable to assume that contribution from participant with better reputation tends to be more reliable. However, using

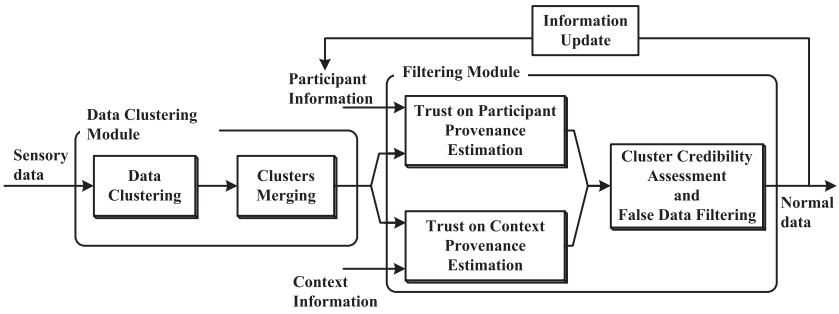


Fig. 5. Overview of FIDC.

reputation score alone as the credibility metric is not adequate, because setting a proper threshold to distinguish the corrupted crowd data is hard and inflexible. Moreover, such a strategy basically denies the possibility for participants with low reputation to submit normal data, and neglects accidentally low quality contribution from participants with high reputation. On the other hand, clustering algorithm is effective for detecting outlier of a set of data, but the choice of a proper cluster width parameter for a clustering algorithm is non-trivial. To overcome these drawbacks while retaining the advantages, FIDC proposes to utilize participant and context provenance based trust as the classifier.

As shown in Fig. 5, FIDC basically consists of two modules. The data clustering module takes the collected data as input, and formally clusters false and normal data into different groups with a clustering-and-merging method. The filtering module makes a credibility assessment for every cluster considering both participant provenance (reputation information) and context provenance (related events' support), and discards the low-rated groups to yield an improvement of overall credibility.

4.2. Data clustering

Normally, physical measurements act as signatures that characterize a place of interest, which implies that truthful measurements for the same location are correlated [32]. Meanwhile, the collected data are mainly exploited at a community scale which provides sufficient participant density. We perform data clustering as the first step towards separating false and normal data apart.

1) Initial clustering: A fixed-width[2] clustering algorithm is performed on D to group similar data instances into clusters with similar property. The first data is assigned to be the centroid of the first cluster. Then for every subsequent data d_i in D, distance between centroid of each cluster and data d_i is calculated as,

$$dis(s_i, s_c) = \sqrt{\sum_{k=1}^{K} (s_i(k) - s_c(k))^2} \tag{1}$$

where s_i is the measurements in d_i, and s_c is the values of cluster centroid. If the distance to one cluster is less than the cluster width ω, it is added to that cluster and the centroid of that cluster is adaptively adjusted to the mean of the inner data. Otherwise, a new cluster is formed with that data as the initial centroid. Here, we define ω as half of the minimum expected deviation from the true aggregation result of a potential misbehavior among the crowd data, i.e.,

$$\omega = 1/2 \cdot \min_i(|F(D(i)) - F(\tilde{D})|) = 1/2 \cdot \sigma_{dev} \tag{2}$$

where $D(i)$ represents one of the possible collected data sets containing corrupted ingredient, F denotes the aggregation function, $\tilde{D}$ denotes the set of normal data in $D(i)$, and σ_{dev} denotes the minimum expected misleading degree. The value of parameter σ_{dev} is updated adaptively depending on the application context, e.g., a dishonest participant may prefer to consider a deviation of at least $4°C$ as effective for a task that measures city temperature, while 10 dB may be a meaningful value in an application of received signal strength measuring. The clustering operation produces a set of fixed width clusters $C_{init} = \{C_1, .., C_n\}$ distributed in the feature space.

2) Merging clusters: Clusters generated in the first stage may be similar with each other as data point are added into all the clusters within certain distance. A merging stage is further introduced to combine similar clusters together. The similarity between cluster C_i and C_j can be measured by their inter-cluster distance, which is defined as the distance between their centroid s_i and s_j, namely, $dis(s_i, s_j)$. Hence, the inter-cluster distances are first calculated, and a merging operation is performed between the two clusters with the minimum distance to generate a new cluster. The new cluster combines the data points in the two neighbor clusters and is added into C_{init} to join the next round of comparison and merging. This iterative procedure continues until the inter-cluster distances of remaining clusters are all bigger than width ω.

Note that the amount of malicious participants may be larger than the honest ones, so cluster with a bigger size does not inherently indicate a higher credibility, and vote-based solutions are ineffective in this situation. In addition, we may not know the right number of clusters before hand, so we adopt a lightweight clustering-and-merging approach instead of using existing techniques like K-means.

4.3. False filtering

The clustering module provides several unlabeled clusters, new metrics are needed to classify them as normal or false. For this processing, we propose to use cluster credibility as the metric, and assess it with the aid of provenance knowledge.

4.3.1. Cluster credibility assessment

We take each generated cluster as a whole, and leverage a two dimensional provenance knowledge, denoted as $PK_i =< K_p^i, K_c^i >$, to assess each cluster's credibility. K_p^i and K_c^i represent participant provenance and context provenance. For each cluster C_i, we estimate trust based on K_p^i and K_c^i independently, and calculate its credibility assessment Cr_i as follows:

$$Cr_i = \alpha \cdot ToP_i + (1 - \alpha) \cdot ToC_i \quad i \in [1, M] \tag{3}$$

where ToP_i and ToC_i denote estimation of trust on provenance K_p^i and K_c^i, respectively. Parameter α and $1 - \alpha$ are the weights of the two trust estimations. The adjustment of the weights depends on the nature of the task. For example, in privacy preserving tasks, participant's identity is often hidden for privacy consideration. As reputation information in such situation may be unavailable,

[2] Here, the fixed-width means the width is fixed for each specific application context instead of setting a static value for all scenarios.

α is set to be 0. Similarly, for tasks with well-established user profile like social sensing, α is set to be considerably high for participant-based trust. Trust metric ToP_i and ToC_i are normalized to bring them into a notionally common scale (i.e., [0, 1]), so assessment result Cr_i is also in the range of [0, 1].

Finally, the cluster showing the highest credibility assessment score is considered to be reliable, and the data inside the cluster are regarded as normal, i.e.,

$$C^* = \arg\max_{C_i}\{Cr_i\} \tag{4}$$

Other contributions in the origin data set D are regarded as false and filtered out. Participants' reputation scores are dynamically updated with an AIMD algorithm (i.e., increase the reputation of the contributors of data in C^*, and decrease the reputation of the rest. Refer to Algorithm 1 for more details).

Algorithm 1 Participant-based Trust Estimation.

Input:
Initial reputation R_0, AIMD factors f_r^{add} and f_r^{mult}
Output:
ToP_i: trust score of the ith cluster based on cluster reputation

```
1: Set R_i ← R_0 for i = 1...N
2: // checking each measurement of each participant
3: for i = 1 → N do
4:   for j = 0 → m_i do
5:     if dist(s_i^j, s_r^j) > d_th then
6:       R_i = R_i / f_r^mult
7:     else
8:       R_i = R_i + f_r^add
9:     end if
10:  end for
11: end for
12: // checking each participant in each cluster
13: for i = 1 → M do
14:   for j = 1 → N_C^i do
15:     ToP_i = 1/N_{C_i} · Σ_j R_{u(s_j)}
16:   end for
17: end for
18: for i = 1 → M do
19:   ToP_i = (ToP_i − min(ToP_i)) / (max(ToP_i) − min(ToP_i))   //Normalization
20: end for
```

Next, we will describe the estimation of ToP_i and ToC_i for cluster C_i based on reputation information and contextual support.

4.3.2. Estimation of trust on participant provenance

Every cluster is constructed with data contributed by participants with varied capabilities and intentions. Hence, from the perspective of participant provenance, cluster's credibility can be measured by the involved contributors' reputation. We define this measurement as trust on participant provenance. Generally, the reputation of a participant, denoted as R_i, is what is generally believed about his/her behavior, and is a knowledge of the past. Trust on one cluster's data can be built on its overall reputation situation.

The proposed estimation algorithm is described in Algorithm 1, which contains a participant reputation training process (Line 3–Line 11) and a trust estimation process (Line 13–Line 17). Initially, participants' profiles may be incomplete, so we introduce an initialization phase and provide a reputation training method. During this phase, we assume that organizers of the sensing campaign would assign or deploy a reliable sensor at the spot (known as anchor node in [19]) to sense and collect the ground truth[3] s_r. By referring to this information, reputation scores of the other data contributors are assessed. Specifically, the distance between each piece of sensing data s_i and s_r is first calculated using Eq. (1). The validity of s_i is determined by comparing dist(s_i, s_r) with a predefined threshold d_{th}. Next, individual reputation scores are calculated based on the validity of contribution by AIMD (additive increase and multiplicative decrease)(Line 8 and Line 6). Traditional reputation systems are designed for commercial networks [33], while systems in existing works are based on social networks [17,18]. In such systems, entities have transaction or interaction with each other, and reputation score is calculated based on ratings from other members in the community. Typical MCS applications follow a different network architecture, namely, each participant only communicates with the centralized server, and reputation scores of them are evaluated by the server according to their performance with no peer ratings. So the reputation management strategies (e.g., sum or average the ratings) in the above works are not effective here. Here we choose to use AIMD method to distinguish the treatment of participants with different behavior, and impose costs for participants to establish and maintain good reputation.

The training phase ends up with a reputation evaluation result $REP = \{R_1, R_2, .., R_n\}$. Given the participants' reputation, the overall reputation of each cluster is calculated as the average reputation of the contributors of every piece of data in that cluster (Line 15). We then normalize these values and use them as the participant provenance-based trust estimation. The rationale is that a group with higher overall reputation tends to be more reliable.

Note that the training process is only required at the very beginning of a MCS application, and the estimated reputation information can be used as a metric in both the continued tasks and other MCS applications. User profiles from social network [17] and feedback from community [18] are feasible alternatives to obtain reputation information, while they are not in the scope of our work.

4.3.3. Estimation of trust on context provenance

Co-located events within a short period of time are likely to have logical relations with the current MCS task, so trust on one cluster can also be estimated by exploiting context specific logical support. Specifically, we propose to translate clusters into logical predicates, and leverage logical reasoning to find support and assess the context-based trust for them.

1) Projection: The clustering module provides us with M separated areas (i.e., clusters) in the K-dimension feature space. To provide predicates for reasoning, we need discrete levels, say, some points distributed in the space, so a mapping function is required to map one cluster into a single point. Generally, the centroid of a cluster can describe its property well, so we propose to use the centroid of clusters to represent them. Then the extracted M levels are defined as $Lev = \{s_c^1, \ldots, s_c^M\}$, where s_c^i denotes the centroid of cluster C_i.

2) Translation: Each quantization level is a feature vector of K-dimension, and we propose to translate them independently. Specifically, each measurement in s_c^i is first converted into fuzzy variables $M(s_c^i(k))$ with function $M(x)$. There are many works on such representation such as fuzzier in fuzzy logic. For example, the value is replaced with "WA" or "CO" (Warm or Cold) according to its scale in a temperature monitoring application. Then we introduce a FOL predicate, denoted as $H(F, T, L)$, which means Influence F holds at time interval T at location L, to describe the statements corresponding to the fuzzy variables. Finally, the

[3] Such investment is only required for the training period. We still have to find fact from the collected data during the running of MCS applications.

translation result regarding level i is defined as

$$T(i) = H(M(s_c^i(1)), T, L) \wedge \ldots \wedge H(M(s_c^i(K)), T, L) \quad (5)$$

3) Knowledge base construction: The reasoning knowledge base is constructed by incorporating related events into the basic knowledge base. Physical phenomena sensed in the same region during a time period are often related, so we define these phenomena as related events. Basically, related events can be obtained from many different sources, such as the reports of other MCS applications, the geo-tagged observations, and information collected from social networks. For example, the density of crowds in different regions of an urban area can be identified through mobility-based sensing applications [34], and can be detected from human observations from social sensing [35] as well. On the other hand, the basic knowledge base contains a set of logical formulas representing the causal relations between events and the sensed phenomena of MCS applications. The method of event collection and relation formulation are out of the scope of this paper. We assume that related events and basic knowledge base are known a priori, and denoted as E and KB_{basic}. Finally, the reasoning knowledge base can be represented as $KB = E \cup KB_{basic}$.

4) Context-based trust estimation: Given the translation results and the reasoning knowledge base, we then employ logical resolution to find evidence for each extracted level, and estimate its credibility.

The proposed algorithm is described in Algorithm 2, which

Algorithm 2 Context-based Trust Estimation.

Input:
$M(s_c^i(k))$, KB_{basic}, E, additive increase factor f_c^{add}
Output:
ToC_i: trust score of the i-th cluster based on context support

```
1:  Set ToC_i ← 0 for i = 1...M
2:  // checking each feature of each cluster
3:  for i = 1 → M do
4:    for k = 1 → K do
5:      Statement = ¬HoldsAt(M(s_c^i(k)), T, L)
6:      for ∀f ∈ KB_basic do
7:        if resolution(E, Statement, f) ⇒ NIL then
8:          ToC_i = ToC_i + f_c^add
9:        end if
10:     end for
11:   end for
12: end for
13: for i = 1 → M do
14:   ToC_i = (ToC_i − min(ToC_i)) / (max(ToC_i) − min(ToC_i))  //Normalization
15: end for
```

will be repeated sequentially for each feature dimension of the M quantization levels. First, we introduce a variable A to denotes the credibility assessment score of Lev. Then we estimate A for each level based on resolution. Specifically, for each level i, we pick out the logical predicate for its k-th measurement and negate it to obtain a statement. We then use inference rules of resolution to iteratively perform resolution on the statement, axiom set E, and every formula in KB_{basic} to show whether this leads to a contradiction (logically, an empty clause). A contradiction means that this measurement of level i is logically supported by E, in which situation we propose to additively increase A_c^i with a factor f_c^{add}. The rationale of the third iteration (Line 6) is that with more events logically supporting the current level, the current level should be more reliable, while the second iteration (Line 4) indicates that with more dimension of measurements being supportive, the current level should be more reliable. For each cluster C_i, an estimation score would be generated with this iterative reasoning procedure. Then we normalize these values to obtain the context-based trust estimation ToC_i (Line 14).

4.4. Security analysis

We prove that FIDC is able to handle the threats presented in the adversary model in Section 3.3.

Location spoofing. Some dishonest participants spoof their location (e.g., GPS spoofing) to pretend a reliable source at the interested spot of the MCS application. Unfortunately, it is unable for a participant at a wrong spot to submit data with correct value by a guess. Otherwise, it is considered to be a result of submission delay as illustrated in Table 1. Based on this fact, FIDC could mitigate such spoofing attack by checking the attached sensing data, and filtering the guessing value as a falsified one.

Independent falsification. The adversaries provide false data independently. The falsified data is different with the normal one on value, so it would be classified into different groups after the clustering operation of FIDC. The randomly generated data is lack of context support, so the corresponding group it belongs to would have a low credibility score. Finally, the independently falsified ingredient would be filtered out due to its low credibility.

Collusive falsification. Some adversaries collude to submit deliberately fabricated data, and attempt to have an advantage on amount during the voting of aggregated data. FIDC does not rely on the majority voting to decide the validity of collected data. FIDC would first separate these corrupted pieces of data and the normal ones into different clusters. Then the overall reputation and contextual support of each cluster are studied. Typically, the collusion group is characterized with relatively lower overall reputation and fewer supportive events, compared to the group formed by honest participants. Hence, the corrupted data from the collusion group would be assigned with low credibility scores, and will be discarded in the filtering phase.

Sybil attack. As aforementioned, Sybil attack on data is functionally equal to collusive falsification in MCS applications. The falsified data generated by a group of Sybil identities would be picked out in the same way as the mitigation of collusive attack. As to the threat to the reputation system, we emphasize that there are no interaction among participants in MCS, so the fake identities of a Sybil attacker cannot vote for each other to promote their reputation (like they used to do in eBay). A special case is that the attacker performs the measuring, and manipulates the identities to submit the correct data. By doing this, the attacker merely focuses on the beneficial reward, which wouldn't cause any bad effect on data quality. Some unique information (e.g., IMEI number) can be required during the registration to avoid such vulnerability [9].

On-off attack. Adversaries may behave as honest participants at first to gain high reputation scores, and then submit false data to interfere data aggregation. In this case, high reputation of individual is no longer an effective metric of data validity. In FIDC, we refer to the overall reputation of the distilled clusters for trust estimation instead of using individual reputation, so a few misleading reputation could not change the rank of the clusters' reputation and the credibility scores. An extreme situation is that adversaries collude with each other to launch on-off attack. To overcome such threat, FIDC could calibrate the weight of the provenance-based trust to rely more (or even thoroughly) on the context provenance. In fact, on-off attack compromises the individual reputation training process, while alternatively, we could refer to the social network to gain these information.

Table 2
Default parameter settings.

Parameter	Value
Additive and multiplicative factor (f_a^r, f_m^r)	(1, 1.5)
Minimum deviation expectation (σ_{dev})	4
Classifier of high and low reputation	0.3
Falsification probability (p_h, p_l)	(0.2, 0.9)
Falsification target (S_{err}^1, S_{err}^2)	(4, 8)
Deviation of the normal distribution (σ)	1
Weight on participant-based trust (α)	0.5

5. Evaluation

5.1. Setup

We test the performance of FIDC based on a typical environmental monitoring application. In such applications, portable sensors of individuals are recruited to collect environmental information and share them through mobile networks. Specifically, we utilize an open source temperature measurement traces obtained from the CRAWDAD data set [36], which contains 5030 measurement items from 289 active taxicabs collected in Rome.

We assume the raw data points in the original data set are all trusty. Hence, in order to simulate data falsification behavior of potential malicious participants, certain data items are manually modified. We set the initial reputation R_0 of each participant to 1, and assess their reputation using Algorithm 1. Then we choose to randomly falsify the measurements of a participant exhibiting a relatively high (low) reputation with probability p_h (p_l). Here, p_h is introduced to take the on-off attacks into consideration, and p_l is set to be considerably bigger than p_h as participants with lower reputation are more likely to submit false data. Meanwhile, we define that the adversaries would collusively send fabricated data, which obey a normal distribution with mean parameter μ equal to the value of misleading target S_{err} and the standard deviation parameter σ. The synthetic data set is divided into two sets according to the submission time of the contribution to conduct two experiments. We set each period to last for four hours considering both the need of certain amount of data for clustering and smoothness of data in each period.[4] As to the premise of logical reasoning, we assume the knowledge base has been pre-established for our application scenario as mentioned above.

Table 2 lists the default parameter settings. The classifier to distinguish high and low reputation is set to be 0.3, and participants with reputation higher and lower than this value would be chosen as an adversary with probability 0.9 and 0.2, respectively. Note that this classifier is only introduced to manually construct a dishonest group. According to the application context, we define the minimum possible deviation caused by data falsification to be 4°C (i.e., deviation smaller than 4°C cannot meet the misleading demand), so the cluster width is 2°C. The mean temperature measurement for the two time periods is 8.85°C and 14.05°C, respectively. In order to mislead the aggregation result, the falsification target S_{err} for time periods 1 and 2 is set to be 4°C and 8°C, respectively. The deviation parameter of the falsified distribution is 1. A same weight ($\alpha = 0.5$) is given to *ToP* and *ToC* to consider a typical situation where provenance knowledge of both participant and context dimension are known.

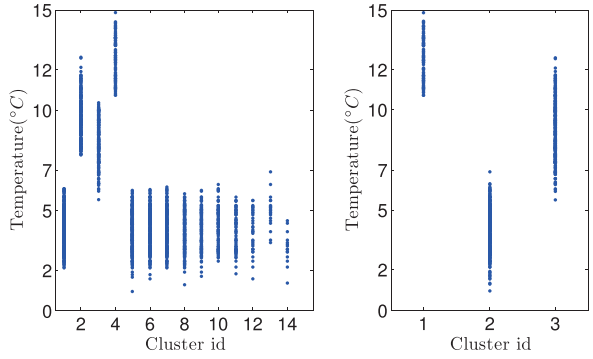
We carry out our evaluation by studying the impact of parameters on effectiveness and comparing the performance of FIDC against typical schemes, which will be introduced in Section 5.3. Specifically, two performance metrics are considered. The first one is overall accuracy, which is defined as

$$A_{overall} = \frac{(TP + TN)}{N_{data}} \tag{6}$$

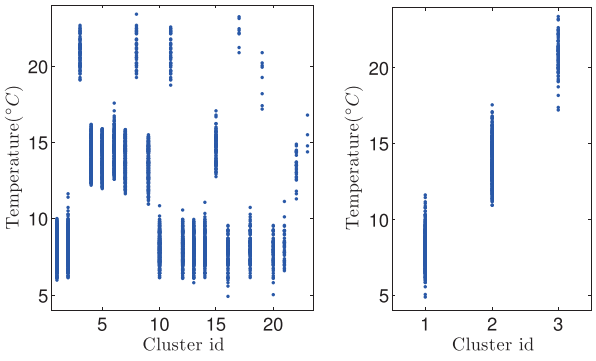
where *TP* and *TN* refers to true positive and true negative, respectively. *TP* means that a piece of sensing data is actually true and classified into C^* as trusted, while *TN* means that a false report is detected and rejected. Parameter N_{data} denotes the total number of data points in the collected data set. The second metric is overall credibility $\Re_D$, given by

$$\Re_D = 1 - \left(\frac{|F(D) - F(\tilde{D})|}{\min(F(D), F(\tilde{D}))} \right) \tag{7}$$

where $\tilde{D} = D - D_f$, and D_f is the set of false data. Compared to the cluster credibility Cr, $\Re_D$ is a posterior value calculated by comparing the ground truth and FIDC outputs. Obviously, the less false data in D, the more similar $F(D)$ and $F(\tilde{D})$ will be, and D will have a higher credibility. Without loss of generality, we adopt average function as the aggregation function F during data analysis.



(a) Clustering results for time period 1 (from 6 o'clock to 10 o'clock)



(b) Clustering results for time period 2 (from 11 o'clock to 15 o'clock)

Fig. 6. Data clustering and clusters merging results (From left to right).

5.2. Simulation results

First of all, we sequentially test the performance of the two modules in FIDC based on the default settings given above. Fig. 6 shows the clustering-and-merging results of the clustering module for the two independent time periods. For period 1, the data are first clustered into 14 groups, which are then merged by comparing their inter-cluster distance with cluster width 2, generating 3 new clusters with values distributed in the feature space. Similarly, 23 clusters are generated for the sensing data of period 2, and merged into 3 new clusters. Note that some clusters generated in the initial clustering phase are similar with each other, and hence

[4] The period length is an application specific value. Using a different period length would generate different clustering result, which can be considered as an adjustment of input, but would not impact the performance of FIDC.

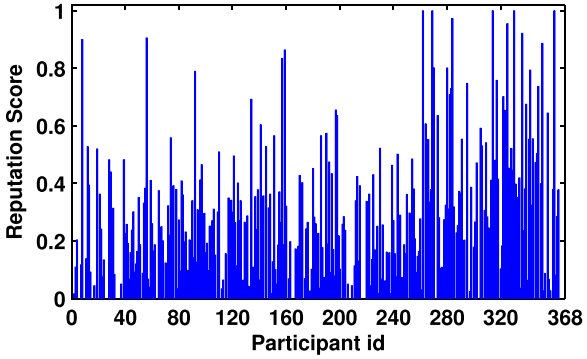


Fig. 7. Reputation of participants (participant id ranges from 4 to 368 with 289 valid ids).

Table 3
A complete knowledge base for logical reasoning.

Period	(# of events, # of logical relations)		
	Cold (<10°C)	Warm (10 ~ 20°C)	Hot (>20°C)
Morning	(8,10)	(4,10)	(1,10)
Noon	(3,10)	(9,10)	(4,10)

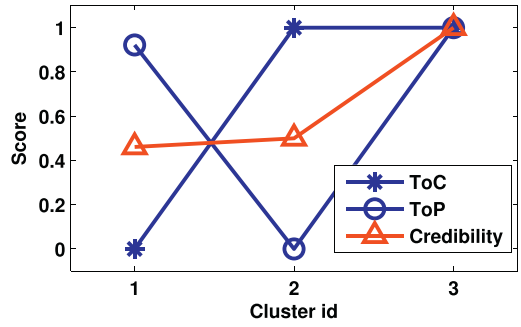
we perform clusters merging for further distillation. As expected, the clustering module roughly groups the normal ingredient (e.g., cluster 3 in period 1), collusively falsified ingredient (e.g., cluster 2 in period 1), and randomly falsified ingredient (e.g., cluster 1 in period 1) into different clusters.

To estimate the participant-based trust, individual reputation is first evaluated through training. During this phase, we compare each temperature measurement with the mean value of all measurements in the original data set[5]. Then one's reputation is decreased (increased) if the distance between the ground-truth value and his/her sensing measurement exceeds (stays below) a predefined threshold 1.5 (this parameter can be adjusted to simulate different amount of dishonest participants). Fig. 7 shows the training result of normalized participants' reputation with their initial reputation equally set to 1. Given these information, *ToP* of each cluster are estimated using Algorithm 1.

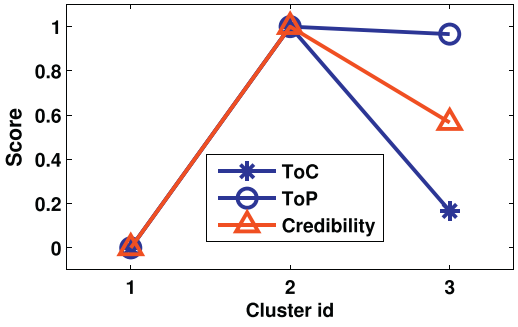
To estimate the context-based trust, centroid of these clusters are extracted to general several discrete levels, which are then mapped to different states. Here we provide 3 states (i.e., "Cold", "Warm", "Hot") for the quantization of the collected temperature measurements, and emphasize that other situations can be easily generalized. Given these application specific states, clusters of period 1 are translated into "Warm", "Cold", "Warm" and clusters of period 2 translated into "Cold", "Warm", "Hot", respectively. Further, a complete knowledge base is defined and presented in Table 3 for each period, based on which logical reasoning is performed to estimate *ToC* for each state.

Fig. 8 shows the credibility assessment results based on participant and context provenance for the two periods. As expected, clusters with more supported events have a higher *ToC* score. By jointly considering *ToP* and *ToC*, the cluster credibility of each cluster (i.e., the FIDC output) is assessed using Eq. (3) and presented with the triangle points in Fig. 8. Obviously, cluster 3 for period 1 and cluster 2 for period 2 present the highest score, so they are determined to be the normal data container. The data in the other two clusters are labeled as corrupted ingredient. Specifically, the

[5] Raw data are assumed to be reliable, and the mean value is regarded as the ground truth. Such truth is only introduced for reputation training, and the evaluation of FIDC results.



(a) Estimation result for time period 1



(b) Estimation result for time period 2

Fig. 8. Trust estimation based on participant provenance and context provenance, and cluster credibility assessment scores for the two time periods.

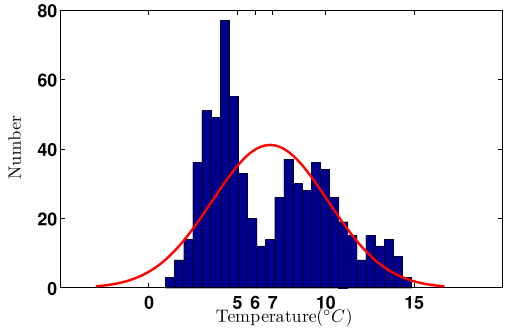
collusively groups (i.e., cluster 2 in period 1 and cluster 1 in period 2) are characterized with lower overall reputation, and the groups containing independently fabricated data (i.e., cluster 1 in period 1 and cluster 3 in period 3) are usually lack of contextual support. Hence, the corrupted part can be identified by either a low *ToP* or a low *ToC*. Here we consider a typical situation with both two provenances available, while weight α should be dynamically adjusted according to the real situation (e.g., increase the weight on *ToR* when only a few logical relations exist).

In Fig. 9, we take time period 1 as an example, and statistically compare the temperature measurement distribution of the modified data set and the output filtering results of FIDC. As shown in Fig. 9(a), the falsification ingredient deviates the mean value to around 7°C by fabricating a fake normal distribution with misleading target 4°C. On the other hand, the misleading deviation is successfully removed by FIDC as depicted in Fig. 9(b), and the statistical result are brought back to its real value around 9°C.

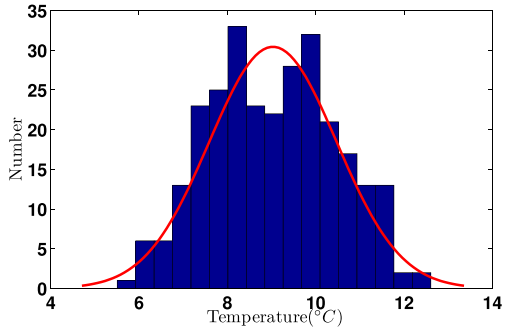
5.3. Performance analysis

5.3.1. Basic comparison

We compare the performance of FIDC against two typical schemes: reputation-based scheme (RBS) [17,18,20] and location attestation-based scheme (LAS) [24–26]. On one hand, we assume that RBS builds a reputation assessment system based on the participants' past behavior, and selects a reputation threshold r to determine the trustworthiness of the collected data (i.e., data of participants with reputation lower than r are considered as false and true otherwise). Note that we manually construct the false ingredient by setting the reputation threshold to 0.3 in Section 5.1. Thus, given all the reputation information, $r = 0.3$ facilitates the best choice for RBS. We also choose $r = 0.2$ as another comparison scheme. On the other hand, LAS acts as a baseline here, because

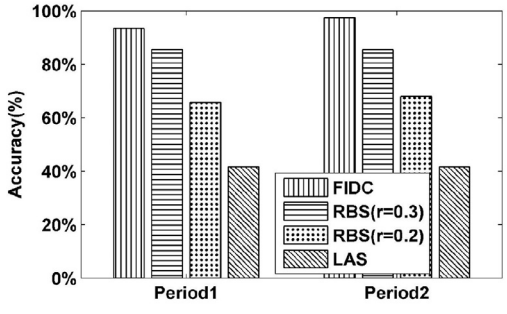


(a) Temperature distribution of the modified data set

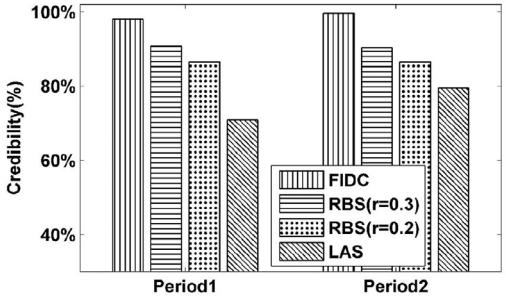


(b) Temperature distribution of the crowd contributed data after FIDC filtering

Fig. 9. Statistical analysis for data distribution before and after FIDC filtering for time period 1. The Y-axis represents the number of data points regarding different temperature readings, and the curve shows the normal fitting for the data set.



(a) Accuracy



(b) Credibility

Fig. 10. Detection accuracy and data credibility performance of FIDC, RBS, and LAS.

data used in this simulation are geographically authenticated, and are then all accepted as normal collection.

Fig. 10 shows the false data identification and credibility guarantee performance using Eq. (6) and Eq. (7). In Fig. 10(a), as FIDC exploits trust information of the provenance, it outperforms the RBS and LAS schemes, and achieves a higher detection accuracy for false data in both periods (0.93 for period 1 and 0.97 for period 2). Compared to FIDC, RBS (r=0.3) accepts more false ingredient and refuses more normal ones due to its ignorance of p_h and p_l. On the other hand, RBS (r=0.2) falsely accepts data of some dishonest participants with reputation lower than 0.3, so it has a lower accuracy than RBS ($r = 0.3$). Compared to the baseline scheme (i.e., LAS), the accuracy improvement of FIDC are 2.2 and 2.3 for each period.

Fig. 10(b) shows the credibility evaluation result based on Eq. (7). As more false data are formally identified and discarded in FIDC, FIDC achieves a higher overall data credibility than RBS and LAS. Specifically, FIDC achieves a credibility of 0.97 and 0.99 for the two periods, respectively. Compared to the baseline scheme, FIDC improve the overall credibility from 0.7 to 0.97 for period 1, and from 0.79 to 0.99 for period 2.

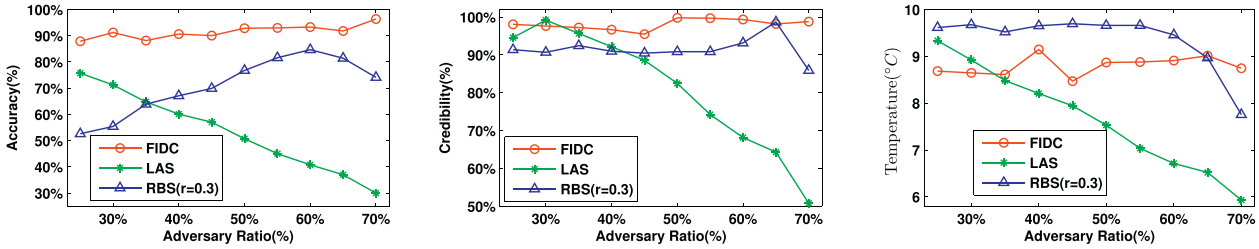
5.3.2. Impact of adversary ratio

We also compare the performance of FIDC with typical schemes under different adversary ratios. The amount of adversaries involved in an application is unknown a priori, and it directly affects the deviation level of the aggregation result. Both the adjustment on the reputation classifier and the falsification probability in Table 2 can result in a different adversary ratio. Here we choose to vary the reputation classifier (with falsification probability p_h and p_l unchanged) to construct data sets with different adversary ratio. By setting the classifier value to k, we can obtain an adversary ratio $(|D_{R<k}| \cdot p_l + (1 - |D_{R<k}|) \cdot p_h) / |D|$, where $D_{R<k}$ is the set of data whose contributors' reputation scores are lower than k. For comparison, we choose RBS with $r = 0.3$ and LAS. The evaluation results are shown in Fig. 11.

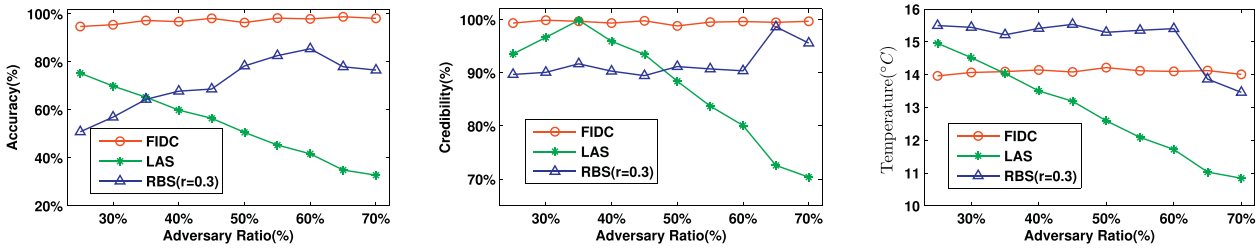
The performance on false data identification accuracy of the two periods is shown in the first column of Fig. 11. It is clear that as the ratio of adversaries increases, accuracy of FIDC keeps steady (around 90% and 95% for period 1 and 2), and outperforms RBS and LAS. Since FIDC exploits the underlying spatial correlation for data analysis, it can separate false and normal ingredient under different adversary ratios. Interestingly, the accuracy of RBS ($r = 0.3$) increases first and decreases after the adversary ratio reaches 60%. The reason is that the reputation threshold setting to form adversary ratio 60% is 0.3, exactly the same as the reputation threshold chosen by RBS ($r = 0.3$), in which case RBS could pick out all the false data (not including the probabilistic falsification). As expected, the accuracy of LAS decreases as the ratio increases, because it fails to filter out any corrupted data.

Again, for the same setting, we test the impact on overall credibility. Similarly, the curve of FIDC is steady, and keeps at a high value of about 97% for period 1 and about 99% for period 2. The performance of RBS is also steady, but it achieves relatively lower credibility than FIDC. In particular, when the adversary ratio reaches 65%, RBS ($r = 0.3$) achieves a similar credibility level as FIDC. We emphasize that this is a special case where the effect of independent falsification and collusive falsification cancel each other out. On the other hand, the curve of LAS follows the similar trend of its performance on accuracy. This is because the increase of adversary ratio would assemble a larger dishonest group, resulting in a nearly linear decrease of accuracy and credibility for the baseline scheme.

Finally, taking average function as the aggregation function of the application server, the aggregation results for each scheme in each period are shown in the third column. Obviously, FIDC provides analysis results close to the real value (i.e., 8.85°C and 14.05°C) regardless of the increase of adversary ratio. We owe this advantage to the reasonable accuracy and high data credibility of



(a) Impact analysis for time period 1



(b) Impact analysis for time period 2

Fig. 11. Impact of adversary ratio on detection accuracy, overall credibility, and aggregation result of FIDC, RBS, and LAS (From left to right).

FIDC as described above. These results demonstrate that our FIDC scheme is more effective than RBS and LAS under independent falsification and collusive falsification of a malicious group.

6. Conclusion

We presented a new clustering-based and provenance-aware framework, named FIDC, to improve data credibility for typical MCS applications. First, the data credibility issues are analyzed with a set of potential attacks. Then we propose to leverage spatial correlation characteristics of data and trust information extracted from participant and context provenance to defend against these attacks. Based on this principle, the clustering module based on clustering-and-merging approach and the filtering module based on provenance-aware credibility assessment are designed as two building blocks of FIDC. The simulation results show that FIDC improves the overall credibility, compared to existing reputation-based and false detection-based schemes.

In the future, we plan to address user privacy and data credibility issues together. We will look into the possibility of studying and introducing participants' correlation as another provenance dimension to gain trust from. In addition, we will consider other common types of data in the implementation (e.g., observations collected from social networks).

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant Nos. 61379144, 61379145, 61672195, 61402513, 61501482, and by the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant No. STPGP 494083.

References

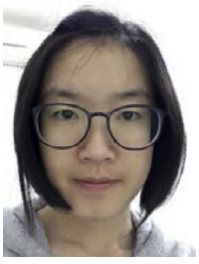
[1] R.K. Ganti, F. Ye, H. Lei, Mobile crowdsensing: current state and future challenges, IEEE Commun. Mag. 49 (11) (2011) 32–39.
[2] J.A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M.B. Srivastava, Participatory Sensing, Center for Embedded Network Sensing, 2006, pp. 117–134.
[3] 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: Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), ACM, 2010, pp. 105–116.
[4] J. Ballesteros, M. Rahman, B. Carbunar, N. Rishe, Safe cities. a participatory sensing approach, in: Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN), IEEE, 2012, pp. 626–634.
[5] P.A. Frangoudis, G.C. Polyzos, Reputation-based crowdsourced wi-fi topology discovery, Comput. Networks 79 (2015) 1–16.
[6] S. Reddy, V. Samanta, J. Burke, D. Estrin, M. Hansen, M. Srivastava, Mobisense – mobile network services for coordinated participatory sensing, in: Proceedings of International Symposium on Autonomous Decentralized Systems (ISADS), IEEE, 2009, pp. 1–6.
[7] J.S. Downs, M.B. Holbrook, S. Sheng, L.F. Cranor, Are your participants gaming the system? screening mechanical turk workers, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2010, pp. 2399–2402.
[8] L. Cheng, L. Kong, C. Luo, J. Niu, Y. Gu, W. He, S.K. Das, False data detection and correction framework for participatory sensing, in: Proceedings of IEEE/ACM International Symposium on Quality of Service (IWQoS), Portland, Oregon, USA, 2015.
[9] X. Wang, W. Cheng, P. Mohapatra, T. Abdelzaher, Artsense: anonymous reputation and trust in participatory sensing, in: Proceedings of INFOCOM, IEEE, 2013, pp. 2517–2525.
[10] X. Wang, H. Fu, C. Xu, P. Mohapatra, Provenance logic: enabling multi-event based trust in mobile sensing, in: Proceedings of IEEE International Performance Computing and Communications Conference (IPCCC), IEEE, 2014, pp. 1–8.
[11] M. Rezvani, A. Ignjatovic, E. Bertino, S. Jha, Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks, IEEE Trans Dependable Secure Comput. 12 (1) (2015) 98–110.
[12] J.-W. Ho, M. Wright, S.K. Das, Zonetrust: fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing, IEEE Trans. Dependable Secure Comput. 9 (4) (2012) 494–511.
[13] S. Ozdemir, Y. Xiao, Integrity protecting hierarchical concealed data aggregation for wireless sensor networks, Comput. Networks 55 (8) (2011) 1735–1746.
[14] Y. Zhang, N. Meratnia, P. Havinga, Outlier detection techniques for wireless sensor networks: a survey, IEEE Commun. Surv. Tutorials 12 (2) (2010) 159–170.
[15] S. Zhu, S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, in: Proceedings of IEEE Symposium on Security and Privacy, IEEE, 2004, pp. 259–271.
[16] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, Distributed anomaly detection in wireless sensor networks, in: Proceedings of the 10th IEEE Singapore International Conference on Communication Systems (ICCS), IEEE, 2006, pp. 1–5.
[17] H. Amintoosi, S.S. Kanhere, A reputation framework for social participatory sensing systems, Mobile Networks Appl. 19 (1) (2014) 88–100.
[18] B. Kantarci, P.M. Glasser, L. Foschini, Crowdsensing with social network-aided collaborative trust scores, in: Proceedings of IEEE Global Communications Conference (GLOBECOM), IEEE, 2015, pp. 1–6.
[19] M. Pouryazdan, B. Kantarci, T. Soyata, H. Song, Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing, IEEE Access 4 (2016) 529–541.
[20] K.L. Huang, S.S. Kanhere, W. Hu, On the need for a reputation system in mobile phone based sensing, Ad Hoc Netw. 12 (2014) 130–149.
[21] H. Mousa, S.B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, L. Brunie, Trust management and reputation systems in mobile participatory sensing applications: a survey, Comput. Networks 90 (2015) 49–73.

[22] P. Gilbert, L.P. Cox, J. Jung, D. Wetherall, Toward trustworthy mobile sensing, in: Proceedings of the 11th Workshop on Mobile Computing Systems & Applications, ACM, 2010, pp. 31–36.
[23] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth, L.P. Cox, Youprove: authenticity and fidelity in mobile sensing, in: Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems, ACM, 2011, pp. 176–189.
[24] M. Talasila, R. Curtmola, C. Borcea, Improving location reliability in crowd sensed data with minimal efforts, in: Prooceedings of the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), IEEE, 2013, pp. 1–8.
[25] N. Sastry, U. Shankar, D. Wagner, Secure verification of location claims, in: Proceedings of the 2nd ACM Workshop on Wireless Security, ACM, 2003, pp. 1–10.
[26] M. Talasila, R. Curtmola, C. Borcea, Link: location verification through immediate neighbors knowledge, in: Mobile and Ubiquitous Systems: Computing, Networking, and Services, Springer, 2012, pp. 210–223.
[27] C. Meng, W. Jiang, Y. Li, J. Gao, L. Su, H. Ding, Y. Cheng, Truth discovery on crowd sensing of correlated entities, in: Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, ACM, 2015, pp. 169–182.
[28] D. Wang, M.T. Amin, S. Li, T. Abdelzaher, L. Kaplan, S. Gu, C. Pan, H. Liu, C.C. Aggarwal, R. Ganti, et al., Using humans as sensors: an estimation-theoretic perspective, in: Proceedings of the 13th International Symposium on Information Processing in Sensor Networks (IPSN), IEEE Press, 2014, pp. 35–46.
[29] F. Restuccia, S.K. Das, Fides: a trust-based framework for secure user incentivization in participatory sensing, in: Proceedings of IEEE 15th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, 2014, pp. 1–10.
[30] Y. Chae, L.C. DiPippo, Y.L. Sun, Trust management for defending on-off attacks, IEEE Trans. Parallel Distrib.Syst. (TPDS) 26 (4) (2015) 1178–1191.
[31] J. Newsome, E. Shi, D. Song, A. Perrig, The sybil attack in sensor networks: analysis & defenses, in: Proceedings of the 3rd international Symposium on Information Processing in Sensor Networks, ACM, 2004, pp. 259–268.
[32] C.C. Aggarwal, T. Abdelzaher, Social sensing, in: Managing and Mining Sensor Data, Springer, 2013, pp. 237–297.
[33] A. Jøsang, Trust and reputation systems, in: Foundations of security analysis and design IV, Springer, 2007, pp. 209–245.
[34] S. Liu, Y. Liu, L. Ni, M. Li, J. Fan, Detecting crowdedness spot in city transportation, IEEE Trans. Veh. Technol. 62 (4) (2013) 1527–1539.
[35] M. Srivastava, T. Abdelzaher, B. Szymanski, Human-centric sensing, Philos. Trans. R. Soc. Lond. A 370 (1958) (2012) 176–197.
[36] A.A. Mohannad, S.H. Hossam, Z. Mohammad, CRAWDAD dataset queensu/crowd_temperature (v. 2015-11-20), 2015, (Downloaded from http://crawdad.org/queensu/crowd_temperature/20151120). 10.15783/C7CG65.

Tongqing Zhou received the bachelor's, and master's degrees in Computer Science and Technology from National University of Defense Technology (NUDT), Changsha in 2012 and 2014, respectively. He is currently working toward the PhD degree in College of Computer, NUDT. His main research interests include wireless networks, mobile sensing, and network measurement.

Zhiping Cai received the bachelor's, master's, and Ph.D degrees in Computer Science and Technology with honor from National University of Defense Technology (NUDT) in July 1996, April 2002 and December 2005, respectively. Currently he is an associate professor in Networking Engineering Department, College of Computer, NUDT at Changsha, China. His doctoral dissertation has been rewarded with the Outstanding Dissertation Award of the Chinese PLA. His current research interests include cloud computing, network security, and network virtualization. He is a member of ACM and IEEE.

Kui Wu received the B.Sc. and the M.Sc. degrees in Computer Science from Wuhan University, China in 1990 and 1993, respectively, and the Ph.D. degree in Computing Science from the University of Alberta, Canada, in 2002. He joined the Department of Computer Science at the University of Victoria, Canada in 2002 and is currently a Professor there. His research interests include mobile and wireless networks, network performance evaluation, and cloud computing.



Yueyue Chen received the bachelor's, and master's degrees in Computer Science and Technology from National University of Defense Technology (NUDT), Changsha in 2013 and 2015, respectively. She is currently working toward the PhD degree in College of Computer, NUDT. Her main research interests include mobile sensing, and task assignment.

Ming Xu has been with the Department of Network Engineering, College of Computer, National University of Defense Technology, China, where he is a professor. He is an editor of the Journal of Communications and the International Journal of Pervasive Computing, and a technical program member of several international conferences such as IEEE PerCom. His current research interests include ad-hoc networks, vehicular networks, and wireless mesh networks. He is a member of the IEEE.