Computer Communications 159 (2020) 222–230

Contents lists available at ScienceDirect

Computer Communications

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

Rapid sensing-based emergency detection: A sequential approach ☆

Rawan F. El Khatib [a,*], Nizar Zorba [b], Hossam S. Hassanein [c]

[a] Department of Electrical and Computer Engineering, Queen's University, Canada
[b] Department of Electrical Engineering, Qatar University, Qatar
[c] School of Computing, Queen's University, Canada

ARTICLE INFO

Keywords:
Crowd sensing
Emergency detection
Sequential detection

ABSTRACT

The upsurge of smart devices has enabled the realization of safe, efficient smart cities that improve the quality of life of their citizens. A prevalent class of smart city services that are attracting increasing attention are Smart Emergency Response and Management (SERM) systems, where sensing paradigms such as crowd sensing and IoT-centric sensing are employed to facilitate the detection of, and response to a crisis situation. In this paper, we study the detection of an abnormal change in a monitored variable through crowd sensed and heterogeneous data, where the change is suggestive of an emergency situation. We formulate our problem as a sequential change-point detection problem, where the underlying distribution of the variable changes at an unknown time. We aim to detect the change-point with minimal delay, subject to a false alarm constraint. We utilize Shiryaev's test to construct two variants of the solution depending on the structure of the received data contributions and mobility of participating sensing elements. We conduct simulations experiments to show the performance of these variants in terms of the delay-false alarm trade-off in different scenarios.

1. Introduction

Today, 54% of the world's population lives in urban settings, and this number is estimated to rise to 68% by 2050, as projected by the United Nations [1]. The complications resulting from this trend are mitigated in smart cities, where state-of-the-art data collection, processing, and disseminating technologies in conjunction with networking and computing technologies, aim to enhance the well-being of citizens through an array of services [2].

Among different services provisioned in smart cities, Smart Emergency Response and Management (SERM) systems are attracting increasing attention. The services provided by SERM systems include prompt detection of irregularities associated with an imminent emergency, continuous situation monitoring and rapid recovery planning and implementation. The delivery of these services is dependent on real-time data sensed from available heterogeneous sources [3].

Crowd sensing is a key building block of the smart city, capitalizing on mobile smart devices (e.g., smartphones, tablets, wearables), static smart sensors (e.g., smart home sensors), and emerging sources such as connected vehicles. These devices offer unprecedented coverage due to the inherent mobility of their users, as well as a diverse range of sensing resources and extensive connectivity capabilities. Particularly, these smart devices are able to survey the surrounding environment using embedded sensing elements, such as GPS, gyroscopes, microphones and temperature sensors, as well as specialized sensors connected to the smart device via cables or wireless communication interfaces (e.g., air quality sensors) [4].

Additionally, crowd sensing exploits data available on Mobile Social Networks (MSNs), including posts and check-ins [5]. These cross-space crowd sensed data are further enriched with data collected from infrastructure-based sensing elements deployed on the small and large scales through IoT-centric sensing. For example, CCTV cameras, drones, weather stations, radars and road side units, in addition to dedicated sensors such as gas leak and chemical spill detection sensors [6].

As authors in [7] pointed out, harvesting this combination of crowd sensed and heterogeneous data provides an improved information infrastructure, which is essential in building situational awareness and cognisance of the disruptive event as it occurs. This crowd powered sensing paradigm facilitates the creation of real-time feedback loops on the emergency, which in turn are used to plan, implement and update the appropriate response measures.

In this work, we are concerned with the detection of a change in a monitored variable, indicating a forthcoming emergency. As an example, consider the entrance of a shopping mall where the central server, henceforth referred to as the coordinator, continuously monitors the noise levels by utilizing the microphones in crowd members' smart devices. Here, an abnormally high noise measurement may be indicative of high crowd density, which may be a sign of a large gathering that warrants attention from authorities. Another example involves

☆ A preliminary version of this work appeared in ElKhatib et al. (2019).

* Corresponding author.
E-mail addresses: rawan.elkhatib@queensu.ca (R.F. El Khatib), nizarz@qu.edu.qa (N. Zorba), hossam@cs.queensu.ca (H.S. Hassanein).

https://doi.org/10.1016/j.comcom.2020.04.060
Received 4 December 2019; Received in revised form 4 March 2020; Accepted 30 April 2020
Available online 4 May 2020

detecting a fire in an open space via a set of infrastructure-based sensors (e.g., CCTV cameras and temperature sensors).

In both examples, it is desirable that the coordinator detects the change in the monitored variable as soon as it occurs and alerts the authorities to take courses of action. In the first example, the coordinator must take into account the integrity of crowd sensed data and mitigate the effect of incorrect data contributions. In the second example, the coordinator must consider the suitability of different sensing elements to detect the change in the monitored variable.

Hence, each data contribution accessible by the coordinator carries a different level of quality, with significant implications on the outcome of the decision-making process. If the coordinator incorrectly announces that a change has happened due to cursory evaluation of the data contributions, it is said that a false alarm has occurred. The false alarms rate is a key performance metric in SERM systems, since a false alarm causes waste of resources. On the other hand, if the coordinator successfully recognizes a change in the monitored variable, then there exists a delay, which is equal to the difference between the time of the detection and the time the change happened.

In this paper, we propose an SERM framework that minimizes the delay while satisfying a false alarm constraint. Our framework has two modules, a data processing module that produces a fitness score, describing the quality of data contributions and their respective sources. In the second module, the detection module, the fitness score is used to determine the worth of each data contribution in the detection process. We implement a sequential detection technique [8], where data contributions are observed sequentially until enough have been collected to stop further data acquisition and declare a detection, subject to a false alarm threshold.

The remainder of the paper is organized as follows. In Section 2, we discuss the related work. In Section 3, we introduce the preliminaries of the SERM framework, followed by the detailed description of the data processing module and detection module in Sections 4 and 5, respectively. Section 6 introduces our simulation environment and results. Finally, Section 7 presents our conclusions.

2. Related work

Quality of Data (QoD), Quality of Information (QoI), reputation and trustworthiness quantification have been addressed in the context of crowd sensing and heterogeneous sensing architectures. The work in [9] provides a framework for defining and enforcing the QoI in crowd sensing systems underlining the implications of human participation in the sensing campaign. An overview of the need for verifying the correctness and truthfulness of crowd sensed data is demonstrated in [10] through trust and reputation management schemes. The authors illustrate the relationship among platform utility, user utility, user reputation, and data trustworthiness. In [11], the authors propose an event-trust and reputation model called QnQ, in order to distinguish among different user classes (honest, selfish, malicious). The reputation scores are based on the quality and quantity of participation for each crowd member. The model transforms the expected truthfulness into a QoI metric that aids the mitigation of selfishness and maliciousness.

Additionally, the work in [12] presents a cross-validation approach to address the QoD contributed by the crowd. Specifically, the approach introduces another layer of crowdsourced data on top of the original crowd-sensed contributed data to achieve cross-validation. The resulting validation is used to reshape the data into a higher quality representation of the reality. The work in [13] proposes a novel quality of source metric that permits anomaly detection for small-scale crowd sensing schemes. Along the same lines, [14] presents a robust metric that allows estimation of quality under the stringent conditions of small sample sizes through non-parametric bootstrap. The work in [15] provides a thematic taxonomy for trust and reputation, addressing the IoT requirements for the understanding of trust and reputation parameters, properties, entity relationships, computation schemes and attacks. In [16], the authors argue that efficient management of IoT systems in smart cities lies in both sensing systems, and in the expedited funnelling and processing of data generated over diversified sensing architectures. Crowd sensed data poses challenges related to the fidelity, trust, and accuracy of each data item, while data heterogeneity requires adaptive measures for QoD calibration.

Several works discuss the specific realization of SERM systems through combinations of heterogeneous sensing architectures, big data analytics and information exchange infrastructures and technologies. In [7] the authors present a view of an information infrastructure that leverages crowd sensed and heterogeneous data to improve emergency response services. Their proposed three-component infrastructure details the integration of large-scale crowd sensing with heterogeneous data analytics, along with a strategic decision-making process that improves the overall efficacy of the system. Similarly, [17] introduces a resilient smart city disaster management system that benefits from big data in the prevention, detection, monitoring, mitigation and recovery of disruptive events. In addition, [18] introduces a comprehensive discussion on state-of-the-art IoT-supported protocols and approaches to encounter disruptive events, including early warning, notification, data analytics, knowledge aggregation, remote monitoring, and real-time analytics.

The work presented by the authors in [19] addresses connectivity issues with a solely IoT-based SERM system, due to breakages in communication infrastructures or network congestions. The authors propose a novel end-to-end infrastructure relying on crowd sensing and the internet of everything for event detection, prediction and response. Similarly, [6] focuses on the communication infrastructure requirement to enable crowd management applications in emergency scenarios. The proposed infrastructure is composed of a power segment that provides power supplies for the core network and edge devices, a communication segment with heterogeneous communication interfaces and technologies, and a data collection and notification segment that supports collection from crowd owned and IoT-connected devices for heterogeneous data collection, analysis and visualization. More recently, the authors in [20] propose a distributed multi-tier system for adaptive emergency alerting in heterogeneous smart cities. The system is centred around a number of sensor-based event detection units to provide real-time geo-referenced information on critical events.

Several other papers discuss application-specific frameworks. The work in [21] presents a GoogleNet inspired architecture for cost-effective flame detection using CCTV surveillance videos based on convolutional neural networks. The model balances accuracy and computational complexity to reduce the rate of false warnings. Other applications include flood detection [22], toxic gas detection [23], and earthquake detection [24]. The closest work to ours is in [25], where a reputation-based contribution assessment scheme is developed to provide rescue personnel with accurate data. This is achieved by splitting the affected area into zones followed by fine-grained filtering rounds to evaluate the data.

Our work by comparison is different because it takes into account not only the quality of contributions from crowd members (i.e., their reputation values), but also the quality of infrastructure-based sensing elements (e.g., toxic gas detectors, CCTV cameras); and their suitability to survey the variable in interest. Furthermore, our work also implements a direct mechanism to detect a change in the monitored variable and determine the exact change-point at which it happened, within shortest time possible.

3. Preliminaries

We are concerned with the detection of a change in a given variable which we monitor through heterogeneous sensing elements, where the change signifies a possible emergency. We establish a mathematical framework that leverages heterogeneous variable-quality data contributions to minimize the time required to detect the change, constrained by a false alarm condition.

Specifically, data is collected via crowd sensing and IoT-centric sensing paradigms. Adopting of this diversified sensing model brings forth several challenges. In order to measure a specific variable, the coordinator must implement a data processing module that allows the SERM service provider to unify and align multimodal sensor and MSN generated data. This is achieved through feature identification and alignment mechanisms enabling seamless interoperability for robust analytics and resilient sense-making [7,16]. We assume that the coordinator implements these data fusion and integration techniques and methodologies, and restrict the scope of our mathematical discussion to the treatment of anomalies in the data contributions.

These anomalies can be a result of the impact of stress or panic, inadequate sensor-calibration, and communication-related issues. In worse cases, misleading data contributions can be intentionally provided by malicious crowd members to hinder end-service delivery [7]. In addition, the quality of each data contribution is closely related to the sensing operation mechanism, describing the sensor's suitability to directly measure or infer a change in the monitored variable.

Our framework introduces a data processing module that mitigates the effect of these anomalies through an outlier detection component and a reputation assessment component for each data contribution. The outlier detection component produces an instantaneous consistency score that reflects the degree of deviance of each crowd generated data contribution. The reputation assessment component uses the accumulative consistency scores to statistically evaluate the sensing element behaviour. Furthermore, we introduce a suitability score that describes each element's adequacy in monitoring the variable of interest through direct measurement or inference, in addition to other calibration and error margin factors. We unify these descriptors through a fitness score, as shall be explained in Section 4.

The fitness score will be used by the detection module to determine the weight of each data contribution in the decision-making process. Specifically, the coordinator monitors a variable through a set of heterogeneous sensing elements, each denoted by $s \in \{1, 2, \dots\}$. At each time slot $i \in \{1, 2, \dots\}$, element s submits data contribution $x(s, i)$, where the set of all contributions at i is denoted by the set $\mathbf{x}_i$.

There are two approaches in which the coordinator can conduct the sensing campaign. In the first approach, the coordinator aggregates the data contributions in $\mathbf{x}_i$ into one observation denoted by $X_i = A(\mathbf{x}_i)$, where $A(.)$ is an aggregation function, and perform the test procedure on this observation. Then, there exists a single sequence of observations throughout the campaign. This renders this approach appropriate in scenarios where the number of sensing elements cannot be guaranteed to stay fixed, hence the need to aggregate the multiple contributions into a single observation. The coordinator can recruit a new set of sensing elements at the beginning of each time slot, referred to as S_i, without interrupting the campaign. Additionally, this approach is also useful in scenarios where we start the campaign with a set of sensing elements whose contributions are characterized with high levels of uncertainty, mandating that the coordinator recruits other sensing elements capable of providing data contributions with higher quality.

Furthermore, this approach is suitable for scenarios where the coordinator can take advantage of sensing elements transiting the place of interest for a short period of time (e.g., portable smart devices, connected vehicles, drones, etc.). For example, crowd members walking into the main entrance of a shopping mall will usually be available there for a few seconds, allowing the coordinator to exploit their presence for a finite number of time slots. Therefore, the contributed data is from a time-varying set of sensing elements, which can be renewed at every time slot.

In the second approach, the coordinator conducts the test procedure on data contributions generated by each sensing element separately. The number of sensing elements, and the number of sequences of observations, must stay constant from the start of the campaign till its end, i.e., $S_i = S, \forall i$. Hence, this approach considers a fixed number of sensing elements committed to periodically generating data contributions until a change is declared. This is suitable in scenarios where sensing elements are situated at the place of interest for longer durations sufficient to span a large number of sensing slots. This includes fixed infrastructure-based sensing elements (e.g., CCTV cameras and road side units), as well as crowd members with limited mobility (e.g., security personnel at a mall or students in a classroom).

We observe that the fundamental difference between the two approaches is whether the source of sensory data might change at the beginning of each sensing slot, i.e., whether the same sensing element is involved in recurrent sensing. Moreover, whether the test procedure is performed in a centralized or a distributed manner. Thus, we refer to the first approach as the *Centralized Sensing* (CS) approach, and the second as the *Distributed Recurring Sensing* (DRS) approach. In the sequel, we discuss the design of the data processing module. For clarity, common notation are supplied in Table 1 at the end of the text.

4. The data processing module

The inherent openness and heterogeneity of our adopted sensing model renders the system prone to anomalous data contributions, necessitating a data processing module that alleviates the effect of these contributions on the output of the detection process. The objective of the data processing module is to determine quality level of each data contribution (and its source), prior to using them in the detection module.

Consider the case where we are interested in monitoring the structural health of a bridge. If the coordinator is alerted to a post on a MSN indicating a potential collapse in the bridge, it must verify the truthfulness of this data contribution. The coordinator confirms this by investigating the degree of strain in the bridge via in-situ strain gauges, or accelerometers that measure vibrations in its cables.

Corrupted data contributions can be a result of deliberate actions by malicious crowd members (e.g., fabricated videos of the bridge falling). In other cases, crowd members may contribute corrupted data inadvertently (e.g., placing the mobile phone inside a pocket in a noise monitoring application). For all sensing elements in general, the device's hardware plays a strong role in the quality of the data contribution. Specifically, each device performs differently due to different sensing capabilities, sampling frequency, sensor calibration and error margins.

Our data processing module must instrument the mitigation of the effect of these anomalies. In the CS approach, the coordinator calculates an instantaneous consistency score for each data contribution. In the DRS approach, the coordinator leverages the accumulative consistency scores for the elements to build a long-term view of their behaviour, since they are involved in the sensing campaign recurrently. For both schemes, we define $\Delta_{s,i}$ as an integrity score for element s at i describing the consistency of each sensing element in an instantaneous or long-term manner, depending on the approach.

Another aspect that must be taken into consideration is each sensing element's suitability in assessing the monitored variable. For example, consider the case where we would like to detect the presence of a harmful gas leak. Visual identification of the leak can be accomplished using a thermographic camera that forms a heat zone image using infrared radiation, whereas an actual detection of the gas leak can be achieved using an electrochemical gas sensor that directly measures the concentration of the leaked gas through a current resulting from an electrochemical reaction at an electrode.

We recognize that there is a difference in the operation mechanism of these two sensing elements, which amounts to whether the device infers the change in the monitored variable or directly measures it. Towards this end, we define the suitability score $\theta_s \in [0, 1]$ for each sensing element s. Here, θ_s serves to control the weight that different sensing techniques have on the detection procedure, by allocating a

high θ_s to sensing elements that directly assess the monitored variable. Note that θ_s is not indexed with i as it does not change with time.

Thus, we define the fitness score as a measure of each sensing element's capability to generate valuable data contributions for the detection process. For any sensing element s, we define the fitness $\phi_{s,i}$ as:

$$\phi_{s,i} = \beta_{s,1} * \Delta_{s,i} + \beta_{s,2} * \theta_s \tag{1}$$

where $\beta_{s,1}$ and $\beta_{s,2}$ are elements' specific weights in $[0,1]$ for fitness control such that $\beta_{s,1} + \beta_{s,2} = 1$. We assume that the coordinator can assign an appropriate suitability score for s using the device information provided once it registers in the system. In the subsequent section, we show in detail how the integrity score is calculated in the CS and DRS approaches.

4.1. Outlier detection and reputation assessment

As mentioned earlier, we aim at addressing the varying quality levels for data contributions by generating a consistency score. Accordingly, we introduce the Local Outlier Factor (LOF) algorithm [26], which is a consensus-based outlier detection method whose output is a measure of the similarity of the data contribution to other contributions in the same set. The LOF is an attractive choice because it is computationally efficient, and it does not require the knowledge of ground-truth. Alternatively, the LOF gauges the distance-based deviation of each data contributions by comparing it to its neighbours.

To clarify, let $\mathbf{x}_i$ denote an arbitrary set of data contributions received at i that we wish to evaluate for outlierness, and let s_1 and s_2 two data points (contributions) from $\mathbf{x}_i$. Additionally, let $d(s_1, s_2)$ represent the euclidean distance between these two points, and $d^k_{s_1}$ the euclidean distance between point s_1 and its kth neighbour. Then, we define $E^k_{s_1}$ as the set of all data points whose distance to s_1 is less than or equal to $d^k_{s_1}$. Based upon which, we define the k-reachability distance of s_1 as:

$$\rho^k_{s_1 \to s_2} = max\{d(s_1, s_2), d^k_{s_1}\} \tag{2}$$

Additionally, let the k-Local Reachability Density (LRD) of s_1 be the inverse of the average reachability distances in s_1's neighbourhood, found as:

$$LRD^k_{s_1} = \frac{|E^k_{s_1}|}{\sum_{\forall s_2 \in E^k_{s_1}} \rho^k_{s_1 \to s_2}} \tag{3}$$

Then, we can find the LOF of s_1 as the average of the ratio of k-local reachability densities of s_1 and its k neighbourhood. Mathematically:

$$LOF^k_{s_1} = \frac{\sum_{\forall s_2 \in E^k_{s_1}} LRD^k_{s_2}}{LRD^k_{s_1} \cdot |E^k_{s_1}|} \tag{4}$$

where $LOF^k_{s_1}$ is an outlierness measure of s_1 in $[0, \infty)$. Particularly, an LOF measure of 1 indicates an inlier that is perfectly consistent with the rest of the data contributions in $\mathbf{x}_i$. On the other hand, $LOF^k_{s_1} \gg 1$ indicates that s_1 is an outlier. To ensure reliable performance, we repeat this procedure for multiple values of the k parameter in $\mathbf{k}$ and take the maximum, as shown in Algorithm 1, line 1–line 9. Assuming that $N = |\mathbf{x}_i|$, and $M = |\mathbf{k}|$, then it is clear that the time complexity of Algorithm 1 is $\mathcal{O}(M * N)$.

In order to use the LOF score in gauging data points' consistency, we desire to convert the LOF measure into the range $[0,1]$. We achieve this via the normalization and regularization procedure presented in [27]. Specifically, this procedure normalizes the LOF value while improving the contrast between inliers and outliers. This is achieved by projecting each LOF value onto a Gaussian distribution $F_G(\hat{\mu}, \hat{\sigma}^2)$. Here, $\hat{\mu}$ and $\hat{\sigma}^2$ are the mean and variance of all the LOF scores, respectively. Through Algorithm 1, line 10–line 12, we obtain a consistency score $w_{s_1,i}$ for each data contribution in $\mathbf{x}_i$, whose value is around 0 for outliers and 1 for inliers.

Algorithm 1 The LOF algorithm

Input: $\mathbf{x}_i$, $\mathbf{k}$
Output: $w_{s,i} \forall s \in \mathbf{x}_i$

1: **for all** $s_1 \in \mathbf{x}_i$ **do**
2: **for all** $k \in \mathbf{k}$ **do**
3: **for all** $s_2 \in \mathbf{x}_i, s_2 \neq s_1$ **do**
4: $\rho^k_{s_1 \to s_2} = max\{d(s_1, s_2), d^k_{s_1}\}$
5: $LRD^k_{s_1} = \frac{|E^k_{s_1}|}{\sum_{\forall s_2 \in E^k_{s_1}} \rho^k_{s_1 \to s_2}}$
6: **end for**
7: $LOF^k_{s_1} = \frac{\sum_{\forall s_2 \in E^k_{s_1}} LRD^k_{s_2}}{LRD^k_{s_1} \cdot |E^k_{s_1}|}$
8: **end for**
9: $LOF_{s_1} = max\{LOF^k_{s_1}, \forall k \in \mathbf{k}\}$
10: $LOF_{s_1} = max\{0, LOF_{s_1} - 1\}$
11: $\hat{w}_{s_1,i} = max\{0, 0.5F_G(LOF_{s_1}) - 1\}$
12: $w_{s_1,i} = 1 - \hat{w}_{s_1,i}$
13: **end for**

As illustrated previously, in the CS approach, the coordinator expects the sensing elements to report data contributions only for a limited duration of time during the sensing campaign. Algorithm 1 provides a solid instantaneous measure of consistency which suffices to describe the quality of the contributions generated by these transitory elements. On the other hand, the DRS approach recruits sensing elements for the entirety of the sensing campaign. In such a case, we desire to extend this instantaneous score into a long term overview of the behaviour of each sensing element. This is achieved by infusing the LOF score into a reputation assessment scheme using the Dirichlet model [9].

In the Dirichlet model, the reputation of each sensing element $R_{s,i}$ is assumed to have a prior Dirichlet distribution with parameter $\beta_{s,3}$. Each time the sensing element reports a data contribution, Algorithm 1 is used to produce a consistency score for s by comparing it to all other contributions reported at the same time. Afterwards, the reputation assessment is a simple parameter update based on the most recent evidence. Specifically, the Dirichlet reputation value of s at time slot i is given as:

$$R_{s,i} = \frac{\beta_{s,3} + 2\sum_i w_{s,i}}{2(\beta_{s,3} + i)} \tag{5}$$

where $w_{s,i}$ is the consistency score for s resulting from applying Algorithm 1 at the set of data contributions received at time slot i. This procedure converts the instantaneous consistency scores into an accumulative score of the performance of s on the long run. Notably, when there is no evidence on the performance of s (i.e., $i = 0$), the value of $R_{s,i}$ reduces to 0.5, indicating a neutral view of s. As more evidence is acquired through Algorithm 1, $R_{s,i}$ will converge to its real value. For a low-quality element whose consistency scores are always 0, $R_{s,i} \to 0$, and vice versa.

Based on the above discussion, it is clear that the coordinator uses the momentary consistency score as an integrity score for elements participating in the CS campaign, i.e., $\Delta_{s,i} = w_{s,i}$. On the other hand, For the DRS campaign, we would like to take advantage of the accumulative history of the participating sensing elements, hence, defining the integrity score in the DRS campaign as $\Delta_{s,i} = R_{s,i}$.

5. The detection module

The detection module is the core of our framework, where the data contributions received from heterogeneous sensing elements are

leveraged to detect an abrupt change in the monitored variable. We begin by introducing the general detection problem and the test procedure. For clarity, we assume that we have data contributions from one sensing element, and extend the discussion of the test procedure to accommodate multiple sensing elements in the CS and DRS approaches accordingly.

5.1. The general detection procedure

Broadly speaking, detection problems involve the observation of a variable of interest in order to make a decision about it. In classical detection problems, one has access to the full batch of observations needed for the decision-making at once. On the contrary, in sequential detection we do not know beforehand the number of observations. Rather, observations are received one by one, and the coordinator must announce the detection of an event based only on past observations. Here, the decision when to stop the data acquisition process is a key part of the detection procedure.

Sequential detection is appropriate for scenarios when both the delay and the reliability of the decision are key to the performance. The Quickest Change-point Detection (QCD) problem (also known as the disorder problem), is a special case of sequential detection problems. In such a problem, the distribution of the monitored variable changes at an unknown time, and we aim to raise an alarm as soon as the change occurs, hence minimizing the delay.

Let $\boldsymbol{X}_j = \{X_i : i = 1, 2, \dots, j\}$ be a stochastic process of j real random variables observed sequentially in time slots $i = 1, 2, \dots, j$. Here, X_i resembles the value of the monitored variable obtained via sensing at time slot i. Initially, the sequence follows a distribution f_0, until a change occurs at an unknown time $\tau \in \mathbb{Z}^+$. Following the change, the random variables $X_\tau, X_{\tau+1}, \dots$ follow a different distribution, denoted by f_1. Precisely, at time slot j, the coordinator must choose between the two hypotheses:

$$\begin{aligned} H_0 :&\quad \boldsymbol{X}_j = \{X_i \sim f_0, i = 1, 2, \dots, j\} \\ H_1 :&\quad \exists \tau \in \mathbb{Z}^+, \text{s.t.:} \\ &\quad \boldsymbol{X}_j = \begin{cases} X_i \sim f_0, i = 1, \dots, \tau - 1 \\ X_i \sim f_1, i = \tau, \tau + 1, \dots, j \end{cases} \end{aligned} \tag{6}$$

where H_0 indicates no change has occurred, and H_1 indicates that a change occurred at τ. Let t_d denote the time that a change is detected. If $t_d \geq \tau$, then there exists a detection delay $\Gamma = t_d - \tau$, where Γ is a discrete random variable. We define the average detection delay as the conditional expectation of Γ, written as:

$$ADD(t_d) = \mathbb{E}\left[\Gamma \mid t_d > \tau\right] = \sum_{i=1}^{\infty} P(\tau = i)\mathbb{E}_i\left[t_d - i \mid t_d > i\right] \tag{7}$$

where $\mathbb{E}_i$ is the expectation when the change occurs at i. On the other hand, if a detection is incorrectly declared before a change to the variable actually happens, then a false alarm has occurred. In such a case, $t_d < \tau$, and the probability of a false alarm (P_{FA}) is expressed as:

$$P_{FA} = P(t_d < \tau) = \sum_{i=1}^{\infty} P(\tau = i)P_i(t_d < i) \tag{8}$$

where P_i is the probability measure when the change occurs at i. Our objective is to devise a detection policy that identifies the change as soon as it occurs, while restricting the probability of making an erroneous decision. Therefore, we present our optimization problem as:

$$\begin{aligned} \min \quad & ADD(t_d) \\ \text{s.t.} \quad & P_{FA} \leq \alpha \end{aligned} \tag{9}$$

where $0 < \alpha < 1$ is a threshold limiting P_{FA}. The above formulation is formally known as the QCD problem [8].

While no general solution has been found for the problem, there exists an explicit solution in the *Bayesian formulation*, where the change-point τ is assumed to be random with a known prior distribution. Specifically, τ is modelled as a geometric random variable with parameter $0 < \lambda < 1$. Thus, the probability that a change occurs at i is:

$$P(\tau = i) = \lambda(1 - \lambda)^{(i-1)}, i = 1, 2, \dots \tag{10}$$

Given the above, the problem is solved as follows. Let p_j denote the a posteriori probability that a change has occurred before time j, given the sequence $\boldsymbol{X}_j$. Equivalently, $p_j = P(\tau \leq j \mid \boldsymbol{X}_j)$ is recursively calculated through Bayes' rule as:

$$p_j = \frac{\left[p_{j-1} + (1 - p_{j-1})\lambda\right]L_j}{\left[p_{j-1} + (1 - p_{j-1})\lambda\right]L_j + (1 - p_{j-1})(1 - \lambda)} \tag{11}$$

where L_j is the likelihood ratio between the post-change and pre-change distributions, found as $L_j = \frac{f_1(\boldsymbol{X}_j)}{f_0(\boldsymbol{X}_j)}$. Consequently, we can solve a Lagrangian relaxation of (9) through dynamic programming to yield [8]:

$$t_s = \inf\{j \geq 1 : p_j \geq A_\alpha\} \tag{12}$$

where inf is the infimum of a set, t_s denotes the optimal stopping time at which the coordinator ends campaign, and $0 < A_\alpha < 1$ is an appropriately chosen threshold that satisfies $P_{FA}(t_s) = \alpha$. This result is known as the optimal *Shiryaev's test* for the QCD problem [8]. In general, it is not trivial to find A_α that satisfies the condition on P_{FA}. However, it has been shown in [28] that setting $A_\alpha = 1 - \alpha$ provides a guarantee that $P_{FA}(t_s \mid A_\alpha) \leq \alpha$, which satisfies the constraint in Eq. (9).

5.2. The CS approach

With regards to the shopping mall entrance example, we have established that the coordinator expects to receive data contributions at each time slot from a different set of sensing elements S_i that may not commit for the length of the campaign. Hence, we amend the set of data contributions $\mathbf{x}_i$ using the aggregation function $A(.)$, such that the output is a single data sample X_i, constituting a single sequence $\mathbf{X}_j = \{X_i : i = 1, 2, \dots, j\}$. Particularly, we employ the fitness score in Eq. (1) in a weighted average aggregation function, as follows:

$$X_i = \frac{\sum_{\mathbf{x}_i} \phi_{s,i} x(s, i)}{\phi_{avg}} \tag{13}$$

with ϕ_{avg} as the average fitness for all elements in S. Indeed, Eq. (13) enables the coordinator to cope with varying number of data contributions at each i by projecting them onto a single dimension. Secondly, the use of the fitness score alleviates the negative effect of corrupted data contributions by allocating a smaller weight through the integrity score derived from the instantaneous consistency score, and the effect of the sensing mechanism of each sensing element is attributed via the suitability score in Eq. (1).

Let us assume that the variable monitored by each sensing element follows a pre-change and post-change Gaussian distributions with $f_0 \sim \mathcal{N}(\mu_0, \sigma_0^2)$ and $f_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$, respectively. Clearly, the linear transformation performed via Eq. (13) constitutes a weighted sum of normally distributed random variables according to f_0 and f_1. Thus, the distribution of X_i before and after the change can be derived as:

$$\begin{aligned} f_0^* &\sim \mathcal{N}(\mu_0 \frac{\sum_{S_i} \phi_{s,i}}{\phi_{avg}}, \sigma_0^2 \frac{\sum_{S_i} \phi_{s,i}^2}{\phi_{avg}^2}) \\ f_1^* &\sim \mathcal{N}(\mu_1 \frac{\sum_{S_i} \phi_{s,i}}{\phi_{avg}}, \sigma_1^2 \frac{\sum_{S_i} \phi_{s,i}^2}{\phi_{avg}^2}) \end{aligned} \tag{14}$$

Note that our assumption of a Gaussian distribution for the environment carries an algebraic convenience updating f_0^* and f_1^* in (14). However, the same discussion can be extended for any distribution assumption where the weighted sum of its random variables is fully characterized. Consequently, the coordinator conducts the sensing campaign in the CS approach as follows. At each time slot, the coordinator collects as many data contributions from heterogeneous sensing elements as possible. Then, Algorithm 1 is applied on the received set

$\mathbf{x}_i$, generating an instantaneous consistency score (integrity score) for each contribution, to update the fitness value in Eq. (1). Afterwards, the aggregation function in Eq. (13) is applied to generate a single data sample, upon which the Shiryaev's test procedure in Eq. (12) is carried out, with $L_j = \frac{f_1^*(\boldsymbol{X}_j)}{f_0^*(\boldsymbol{X}_j)}$. This process is implemented recursively until the value in Eq. (11) satisfies the threshold on A_α, at which point the change is declared.

5.3. The DRS approach

In the DRS approach, the coordinator recruits a fixed number of sensing elements who are committed to the entire length of the campaign, each of which generating an independent stream of data contributions. The DRS approach performs the detection procedure in a distributed manner across a number of sequences, where the behaviour of participating elements can be characterized on the long run by accumulating their instantaneous consistency scores. Therefore, in the DRS approach, the integrity score is set to be the Dirichlet based reputation value in Eq. (5). In general, it is shown that the sequential change-point detection problem in (9) in a distributed system is computationally intractable even in its simplest form [8].

Let us assume that, in the beginning of the campaign, the coordinator recruits $|S|$ sensing elements. If an element abandons the campaign (e.g., a crowd member changing his/her location), the coordinator may recruit a replacement (e.g., another crowd member available at the sensing location) to continue the sequence generation, while taking care of appropriately updating the reputation and fitness scores. Furthermore, the coordinator may recruit more than one sensing element and combine their data contributions using the aggregate function in Eq. (13), to ensure the sensing process is not interrupted by elements leaving the campaign. For the following discussion, we assume that all elements in $|S|$ are devoted to generating their respective observation sequences until the end of the campaign (i.e., until a detection is declared).

Following with the notation in the previous section, at time slot j, sensing element s has the sequence $\mathbf{X}_j^s = \{X_i^s : i = 1, 2, \dots, j\}$ of real random variables, where each entry in the sequence corresponds to a single data contribution. For each sensing element, the optimal detection procedure in Eq. (12) is performed on its own sequence $\mathbf{X}_j^s$. Thus, our interest now shifts to construct a fusion rule for the stopping criterion which combines the local decisions from each participating sensing element. We define our fusion rule as follows:

- t_π: the coordinator ends the campaign at an individual element as soon as it achieves the threshold on P_{FA}, and declares a change is detected, provided that the average fitness score of S exceeds a certain threshold.

To benchmark the performance of the above rule, we also define the following two rules:

- t_{min}: the coordinator ends the campaign for all elements and declares that a change is detected as soon as one of the participating elements in S achieves the threshold on P_{FA} [8].
- t_{max}: the coordinator ends the campaign at an individual element as soon as it achieves the threshold on P_{FA}, and declares a change is detected once all participating sensing elements in S have achieved their respective thresholds [8].

We observe that the three fusion rules are applicable in slightly different scenarios. Specifically, t_{min} is appropriate for scenarios where a detection from a single sensing element is worthy of raising an alarm, whereas t_{max} is suitable for scenarios where unanimity of the detection must be reached. Furthermore, it is noteworthy that t_{max} is shown to be globally first order asymptotically optimal, given that an appropriate threshold on P_{FA} is chosen. On the contrary, the fusion rule t_{min} does not possess this asymptotic optimality property [8]. Inevitably, t_{max} entails longer delays than t_{min}.

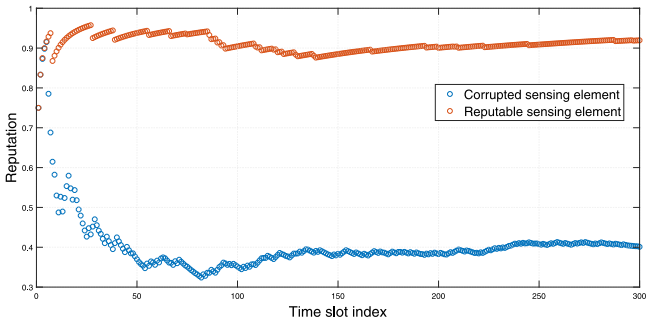


Fig. 1. Evolution of the reputation vs. time.

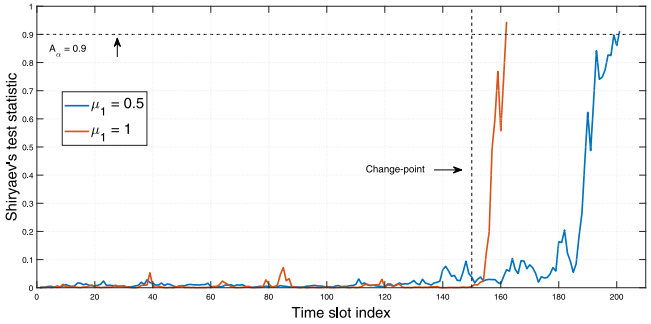


Fig. 2. Evolution of Shiryaev's statistic vs. time.

On the other hand, t_π represents a trade-off between two, by placing a threshold on the average fitness score of S. Specifically, this rule is appropriate when we desire that reputation of crowd members has converged to its true value after a number of update iterations at every i. For example, in cases where no previous history is obtained about the participating crowd members, the initial reputation value will be set to 0.5, and will be recursively updated as evidence accumulates until convergence. This implies that the average fitness score of S will also converge to reflect the true fitness of value of the set.

We determine the threshold for the average fitness using the Condorcet Jury Theorem (CJT), which states that a set of heterogeneous individuals (i.e., sensing elements) are always better at choosing one of two alternatives than a single individual (sensing element), as long as individual decisions are independent from each other [29]. Specifically, for a group of heterogeneous sensing elements with varying fitness levels, the probability that a proportion of the group, denoted by $\pi \geq 0.5$ will make the correct decision is higher than an individual decision as long as the following condition is satisfied:

$$\phi_{avg} \geq \frac{\pi(|S|+1)}{|S|} \tag{15}$$

Consequently, the coordinator conducts the sensing in the DRS approach as follows. At the start of the campaign, the coordinator recruits a set S of sensing elements. At time slot i, each element s surveys the monitored variable for a data contribution in the sequence $\mathbf{X}_j^s$. Then, Algorithm 1 is applied for the received contributions to generate evidence for element's performance, followed by a reputation and a fitness update in Eq. (5) and Eq. (1), respectively. Afterwards, the Shiryaev's test procedure is carried recursively on each individual sequence, until the fusion rule of choice is satisfied.

6. Performance evaluation

In this section, we first introduce our simulation environment and parameters, then present performance evaluation results.

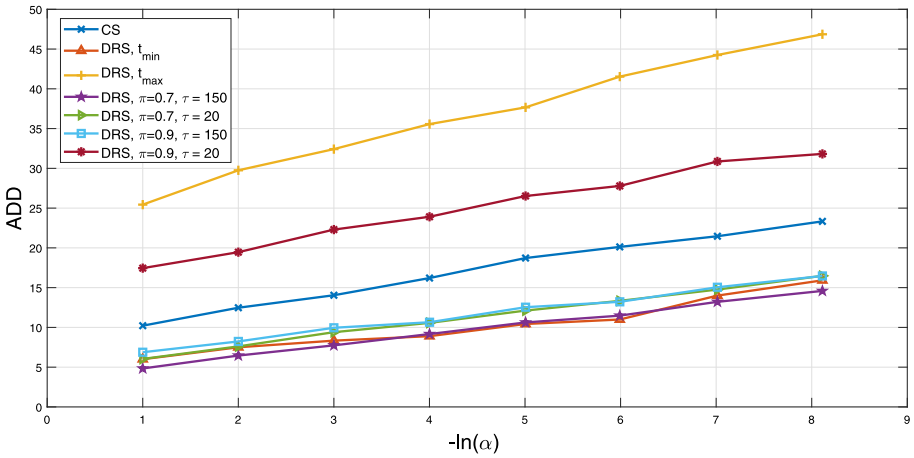


Fig. 3. Average detection delay vs. the false alarm threshold.

6.1. Simulation environment and setup

We conduct Monte Carlo simulations to evaluate the proposed framework. The CS approach collects data contributions from a set of sensing elements whose number $|S_i|$ varies in $\{6, 7, \ldots, 15\}$. These contributions are evaluated for consistency via the LOF algorithm, where $\mathbf{k} = \{2, 3\}$. In the DRS approach, we set the number of sensing elements to 10 and evaluate the Dirichlet reputation for each element with the Dirichlet distribution parameter $\beta_{s,3} = 1, \forall s$. Additionally, we generate a random number in $[0, 1]$ for the suitability θ_s. To highlight the effect of the consistency score, we set $\beta_{s,1} = 0.8$ and $\beta_{s,2} = 0.2$ for all elements. We assume the pre- and post-change distributions are Gaussian with $f_0 \sim \mathcal{N}(0, 1)$ and $f_1 \sim \mathcal{N}(1, 1)$, respectively, and set the geometric distribution parameter λ to 0.001.

6.2. Simulation results

We begin by illustrating the evolution of the Dirichlet reputation value by plotting it for a reputable and a corrupted sensing element in Fig. 1. Here, the corrupted sensing element's data contributions were corrupted by adding a normally distributed noise to the data contributions generated from the pre- and post-change distribution. As can be seen in the figure, both reputations begin with a neutral 0.5 value, and fluctuate until stabilizing after 150 time slots, reaching 0.9 and 0.4 for a reputable and a corrupted sensing element, respectively. Indeed, this convergence is reached after enough evidence is acquired from the LOF algorithm to precisely characterize the behaviour of each element. Note that the fluctuation in the early time slots directly affects the performance of our framework in cases where the change occurs before reputations converge, causing the coordinator to give an inappropriate weight to the contributions generated from corrupted sensing elements, which might impede accurate detection. Hence, the reputation value has a negative effect on the detection procedure if a change occurs early, because the reputation values are not truly indicative of the element's behaviour.

Next, to illustrate the test procedure, we plot the evolution of the Shiryaev's test statistic p_j in Fig. 2 for a sequence observed by a single sensing element. We set the change-point τ to an arbitrary value of 150, and plot the result when μ_1 is set to 0.5 and 1. We set the Shiryaev's threshold $A_\alpha = 0.9$, indicating that $P_{FA} = 0.1$. By examining the figure, we note that the statistic stays relatively low around zero until the change-point τ for both cases of μ_1. For subsequent time slots, the statistic p_j grows until it exceeds the threshold A_α at $j = 162$ for $\mu_1 = 1$ and $j = 201$ for $\mu_1 = 0.5$. Indicating that the coordinator had a decision delay of $\Gamma = 12$ and $\Gamma = 51$ time slots to detect the change, respectively. From this figure, it is obvious that the smaller the distance between f_0 and f_1, the more challenging it becomes to detect the change quickly. Moreover, choosing a higher value for A_α achieves a lower false alarm rate, but at the expense of longer delay until the Shiryaev's statistic exceeds A_α. For the following discussion, we set μ_1 to 1, and let P_{FA} vary.

In Fig. 3, we plot the ADD against α for all variants of the proposed approaches, where α varies in $[0, 0.4]$. For clarity, we plot the negative of the natural logarithm of α, as $-\ln(\alpha)$ becomes larger, the more stringent the condition on P_{FA} becomes. In order to understand the effect of the reputation convergence on the DRS CJT approach, we plot the case when the change occurs at $\tau = 150$ and $\tau = 20$ for $\pi = 0.7, 0.9$. Intuitively, setting π to a higher value entails longer delays regardless of when the change occurred, because the coordinator waits until the average fitness ϕ_{avg} exceeds the threshold set by the CJT theorem. Moreover, the coordinator benefits from a change occurring at $\tau = 150$ because the reputations are close to convergence, implying that it is easier for ϕ_{avg} to exceed the CJT threshold. In summary, the least delay is incurred by placing a low constraint on ϕ_{avg}, and is aided by reputation values that have stabilized before the change occurs.

For the CS and DRS approaches for t_{max} and t_{min}, we notice that all these approaches also follow the same behaviour, exhibiting a larger delay as the false alarm constraint becomes more stringent. In addition, we note that the DRS approach following the t_{max} fusion rule has the worst delay, representing an upper bound on the performance. This behaviour is anticipated by the t_{max} rule as it waits for all sensing elements to achieve the constraint on A_α. On the other hand, the DRS approach following the t_{min} rule and the CS approach achieve comparable performance, with the t_{min} rule attaining slightly lower delays. This can be attributed to the fact that with 10 sensing elements, it is more probable that one of these participants will detect the change faster than a single-stream data sequence observation as in the CS approach. Finally, these approaches perform comparably to those of t_π as P_{FA} changes, except for t_π for $\pi = 0.9$ and $\tau = 20$. The increase in the delay for the former case with can be attributed to the fluctuation in the reputation values and the strict constraint on ϕ_{avg} as explained earlier.

Finally, we plot the ADD against the number of participants for a constant P_{FA} in Fig. 4, with α set to 0.1. By examining the figure, it can be seen that the behaviour of all schemes and their variants aligns with that shown in Fig. 3. The DRS approach following the t_{max} fusion rule represents an upper bound on the other schemes, while showing a steadily increasing trend as the number of participants increases. Similar behaviour is shown for the DRS CJT approach for $\pi = 0.7$ and $\pi = 0.9$, when $\tau = 150$ and $\tau = 20$. For $\pi = 0.9$, the rate of increase is higher as the number of participants increases, because the condition is more stringent on the average fitness. The DRS approach following the t_{min} fusion rule shows a slight decrease with an increasing number of participants. This is intuitive, because for a larger $|S|$, there is higher

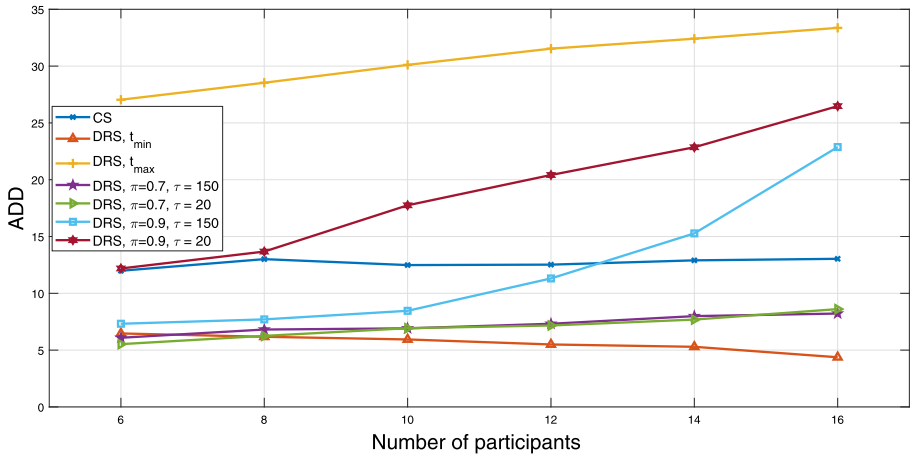


Fig. 4. Average detection delay vs. the number of participants.

Table 1
Table of common notations.

Notation	Explanation
i	Time slot index
s	Sensing element index
$x(s,i)$	Data contribution by s at i
$\mathbf{x}_i$	Set of all data contributions at i
$A(.)$	Aggregate function
S_i	Set of sensing elements at i
$\Delta_{s,i}$	Integrity score of s at i
θ_s	Suitability score of s
$\phi_{s,i}$	Fitness of s at i
$w_{s_1,i}$	Consistency score of s_1 at i
$R_{s,i}$	Reputation of s at i
$\beta_{s,1}, \beta_{s,2}, \beta_{s,3}$	Element specific parameters
τ	Change-point
f_0, μ_0, σ_0^2	Pre-change distribution, mean and variance
f_1, μ_1, σ_1^2	Post-change distribution, mean and variance
t_d	Detection time
Γ	Detection delay
ADD	Average detection delay
P_{FA}	Probability of false alarm
α	False alarm threshold
p_j	Shiryaev's statistic
L_j	Post- and pre-change likelihood ratio
$\mathbf{X}_j$	CS sequence of j contributions
$\mathbf{X}_j^s$	DRS sequence of j contributions from s
ϕ_{avg}	Average fitness
t_{min}	Minimum detection time fusion rule
t_{max}	Maximum detection time fusion rule
t_π	CJT π detection time fusion rule

probability that one participant will detect the change faster. Finally, the CS scheme shows a relatively steady performance as the number of participant varies. This can be attributed to the fact that it does not retain any information on participants' reputation values, as it assumes that a new set of participants S_i generates the data contribution at each time slot.

7. Conclusions

In this paper, we studied the detection of a change in a monitored variable via a combination of crowd sensing and IoT-centric sensing paradigm, where the change signifies a forthcoming emergency situation. Our framework presented a data processing module that enables the coordinator to cope with data contributions of varying quality levels. Specifically, we defined a fitness score for each sensing element participating in the sensing campaign, where the score reflects the element's integrity and suitability to survey the monitored variable. Our problem was formulated as a sequential change-point detection problem, where the distribution of the variable changes abruptly at an unknown time. Two variants of the problem were introduced based on the structure of the received data contributions: the Centralized Sensing (CS) and the Distributed Recurring Sensing (DRS) approaches. In both variants, we utilized Shiryaev's test to minimize the average detection delay under false alarm constraints. We conducted simulation experiments to show the performance of the CS and DRS approaches in their variants, and highlighted the scenarios in which they are applicable.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

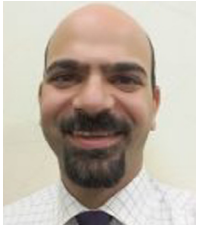
This research is supported by a grant from the Natural Sciences and Engineering Research Council of Canada (NSERC) under grant number RGPIN-2019-05667.

References

[1] Department of Economic and Social Affairs, United Nations, World urbanization prospects, available from: https://population.un.org/wup/.
[2] A. Gharaibeh, M. Salahuddin, S. Hussini, A. Khreishah, I. Khalil, M. Guizani, A. Al-Fuqaha, Smart cities: a survey on data management, security, and enabling technologies, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2456–2501, http://dx.doi.org/10.1109/COMST.2017.2736886.
[3] R.F. ElKhatib, N. Zorba, H.S. Hassanein, A Reputation-aware mobile crowd sensing scheme for emergency detection, in: Proceedings of the IEEE Symposium on Computers and Communications, ISCC, Spain, 2019, pp. 1–6, Jul.
[4] R.F. ElKhatib, N. Zorba, H.S. Hassanein, A fair reputation-based incentive mechanism for cooperative crowd sensing, in: Proceedings of the IEEE Global Communications Conference, GLOBECOM, UAE, Dec, 2018, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2018.8647555.
[5] B. Guo, Z. Wang, Z. Yu, Y. Wang, N.Y. Yen, R. Huang, X. Zhou, Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm, ACM Comput. Surv. 48 (1) (2015) 1–31, http://dx.doi.org/10.1145/2794400.
[6] A.J. Perez, S. Zeadally, A communication architecture for crowd management in emergency and disruptive scenarios, IEEE Commun. Mag. 57 (4) (2019) 54–60, http://dx.doi.org/10.1109/MCOM.2019.1800626.
[7] M. Abu-Elkheir, H.S. Hassanein, S.M. Oteafy, Enhancing emergency response systems through leveraging crowd sensing and heterogeneous data, in: Proceedings of the International Wireless Communications and Mobile Computing Conference, IWCMC, Cyprus, Sep, 2016, http://dx.doi.org/10.1109/IWCMC.2016.7577055.
[8] V.V. Veeravalli, T. Banerjee, Quickest change detection, in: Academic Press Library in Signal Processing: Array and Statistical Signal Processing, first ed., Academic Press, USA, 2014, pp. 209–252, http://dx.doi.org/10.1016/B978-0-12-411597-2.00006-0 (ch. 6).

[9] F. Restuccia, N. Ghosh, S. Bhattacharjee, S.K. Das, T. Melodia, Quality of information in mobile crowd sensing: survey and research challenges, ACM Trans. Sensor Netw. 13 (4) (2017) 1–43, http://dx.doi.org/10.1145/3139256.
[10] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, H. Song, Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd sensing, IEEE Access 5 (2017) 1382–1397, http://dx.doi.org/10.1109/ACCESS.2017.2660461.
[11] S. Bhattacharjee, N. Ghosh, V.K. Shah, S.K. Das, *QnQ*: Quality and quantity based unified approach for secure and trustworthy mobile crowdsensing, IEEE Trans. Mob. Comput. 19 (1) (2020) 200–216, http://dx.doi.org/10.1109/TMC.2018.2889458.
[12] T. Luo, J. Huang, S.S. Kanhere, J. Zhang, S.K. Das, Improving iot data quality in mobile crowd sensing: a cross validation approach, IEEE Internet Things J. 6 (3) (2019) 5651–5664, http://dx.doi.org/10.1109/JIOT.2019.2904704.
[13] S.B. Azmy, N. Zorba, H.S. Hassanein, Robust quality metric for scarce mobile crowd-sensing scenarios, in: Proceedings of the 2018 IEEE International Conference on Communications Workshops, ICC Workshops, USA, May, 2018, pp. 1–5, http://dx.doi.org/10.1109/ICCW.2018.8403744.
[14] S.B. Azmy, N. Zorba, H.S. Hassanein, Bootstrap-based quality metric for scarce sensing systems, in: Proceedings of the IEEE Global Communications Conference, GLOBECOM, UAE, Dec, 2018, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2018.8647536.
[15] A. Ahmed, S. Hamid, A. Gani, M. Khan, Trust and reputation for internet of things: fundamentals, taxonomy, and open research challenges, J. Netw. Comput. Appl. 145 (2019) http://dx.doi.org/10.1016/j.jnca.2019.102409.
[16] S.M. Oteafy, H.S. Hassanein, Big sensed data: evolution, challenges, and a progressive framework, IEEE Commun. Mag. 56 (7) (2018) 108–114, http://dx.doi.org/10.1109/MCOM.2018.1700557.
[17] C. Yang, G. Su, J. Chen, Using big data to enhance crisis response and disaster resilience for a smart city, in: Proceedings of the IEEE International Conference on Big Data Analysis, ICBDA, China, Mar, 2017, pp. 504–507, http://dx.doi.org/10.1109/ICBDA.2017.8078684.
[18] P.P. Ray, M. Mukherjee, L. Shu, Internet of things for disaster management: state-of-the-art and prospects, IEEE Access 5 (2017) 818–835, http://dx.doi.org/10.1109/ACCESS.2017.2752174.
[19] A. Boukerche, R.W.L. Coutinho, Smart disaster detection and response system for smart cities, in: Proceedings of the IEEE Symposium on Computers and Communications, ISCC, Brazil, Jun, 2018, pp. 1102–1107, http://dx.doi.org/10.1109/ISCC.2018.8538356.
[20] D.G. Costa, F. Vasques, P. Portugal, A. Aguiar, A distributed multi-tier emergency alerting system exploiting sensors-based event detection to support smart city applications, Sensors 20 (1) (2020) 1–28, http://dx.doi.org/10.3390/s20010170.
[21] K. Muhammad, J. Ahmad, I. Mehmood, S. Rho, S.W. Baik, Convolutional neural networks based fire detection in surveillance videos, IEEE Access 6 (2018) 18174–18183, http://dx.doi.org/10.1109/ACCESS.2018.2812835.
[22] S.W. Lo, J.H. Wu, F.P. Lin, C.-H. Hsu, Visual sensing for urban flood monitoring, Sensors 15 (8) (2015) 20006–20029, http://dx.doi.org/10.3390/s150820006.
[23] H. Kim, J. Shin, H. Shin, B. Song, Design and implementation of gateways and sensor nodes for monitoring gas facilities, in: Proceedings of the International Conference on Information Science and Industrial Applications, ISI, South Korea, May, 2015, pp. 3–5, http://dx.doi.org/10.1109/ISI.2015.15.
[24] O. Omosebi, S. Sotiriadis, E. Asimakopoulou, N. Bessis, M. Trovati, R. Hill, Designing a subscription service for earthquake big data analysis from multiple sources, in: Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC, Poland, 2015, pp. 601–604, http://dx.doi.org/10.1109/3PGCIC.2015.58.
[25] M.A. Alswailim, H.S. Hassanein, M. Zulkernine, A participant contribution trust scheme for crisis response systems, in: Proceedings of the IEEE Global Communications Conference, GLOBECOM, Singapore, Dec, 2017, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2017.8253927.
[26] M.M. Breunig, H.-P. Kriegel, R.T. Ng, J. Sander, LOF: identifying density-based local outliers, in: Proceedings of the ACM SIGMOD International Conference on Management of Data, USA, May, 2000, pp. 93–104, http://dx.doi.org/10.1145/335191.335388.
[27] H.-P. Kriegel, P. Kroger, E. Schubert, A. Zimek, Interpreting and unifying outlier scores, in: Proceedings of the SIAM International Conference on Data Mining, USA, Apr, 2011, pp. 1–12, http://dx.doi.org/10.1137/1.9781611972818.2.
[28] A.G. Tartakovsky, V.V. Veeravalli, Quickest change detection in distributed sensor systems, in: Proceedings of the International Conference of Information Fusion, Australia, May, 2003, pp. 756–763, http://dx.doi.org/10.1109/ICIF.2003.177315.
[29] S. Kanazawa, A brief note on a further refinement of the condorcet jury theorem for heterogeneous groups, Math. Social Sci. 35 (1) (1998) 69–73, http://dx.doi.org/10.1016/S0165-4896(97)00028-0.

Rawan F. El Khatib is a Ph.D. student at Queen's University at Kingston, Canada. She received the B.A. degree in communications engineering and the M.A. degree in wireless communications engineering from Yarmouk University, Irbid, Jordan, in 2014, and 2016, respectively. Her research interests include Multi-access edge computing services, mobile crowd sensing, and the Internet of Things.



Nizar Zorba is a Professor at the Electrical Engineering department at Qatar University, Doha, Qatar. He has authored five international patents and co-authored over 120 papers in peer-reviewed journals and international conferences. Dr. Zorba received the B.Sc. degree in electrical engineering from JUST University, Jordan, in 2002, and the Ph.D. degree in signal processing for communications from UPC Barcelona, Spain, in 2007. He is associate/guest editor for the IEEE Communications Letters, IEEE Access, IEEE Communications Magazine and IEEE Network. Currently, he is the vice-chair of the IEEE ComSoc Communication Systems Integration and Modeling Technical Committee (TC CSIM).

Hossam S. Hassanein is a leading authority in the areas of broadband, wireless and mobile networks architecture, protocols, control and performance evaluation. His record spans more than 500 publications in journals, conferences and book chapters, in addition to numerous keynotes and plenary talks in flagship venues. Dr. Hassanein has received several recognitions and best papers awards at top international conferences. He is also the founder and director of the Telecommunications Research Lab (TRL) at Queen's University School of Computing, with extensive international academic and industrial collaborations. He is a former chair of the IEEE Communication Society Technical Committee on Ad hoc and Sensor Networks (TC AHSN). Dr. Hassanein is an IEEE Communications Society Distinguished Speaker and is a fellow of the IEEE.