A Reputation-aware Mobile Crowd Sensing Scheme for Emergency Detection

Rawan F. El Khatib[1], Nizar Zorba[1], and Hossam S. Hassanein[2]

[1]Department of Electrical Engineering, Qatar University, Qatar
[2]School of Computing, Queen's University, Canada
{rawan.elkhatib, nizarz}@qu.edu.qa, hossam@cs.queensu.ca

***Abstract*—The unforeseen proliferation of smart devices has set in motion research efforts aimed at building Smart Cities (SCs) that improve the well-being of their citizens. One of the key technologies to achieve a SC is Mobile Crowd Sensing (MCS). In MCS, data is collected from the environment surrounding the smart device owners and utilized in the provision of a wide array of SC services. A prevalent class of services which is attracting increasing attention is smart emergency services, where MCS is leveraged to facilitate the detection and mitigation operations of crises. In this paper, we study the problem of an emergency situation detection based on MCS-provided data from heterogeneous participants. Specifically, we formulate our problem based on Detection Theory and underline its computational complexity. We present a greedy algorithm that aims to balance the trade-off between the decision time and the quality of the final decision. We perform extensive simulation experiments that show how our scheme improves the correct detection rate compared to a naive reputation-unaware baseline.**

I. Introduction

With the unprecedented prevalence of sensor-enriched smart devices, *Mobile Crowd Sensing* (MCS) has emerged as a building block of the Smart City (SC) paradigm. An SC employs solutions to monitor and automate city operations, in an effort to mobilize the evolution of efficient and sustainable infrastructures. This is achieved by leveraging data collected from a combination of technologies in the orchestration of urban dynamics, with the aim to promote prosperity and enhance the quality of life of its citizens [1].

Towards this end, MCS prompts citizens to share real-time data from their surrounding environments, by utilizing the sensing and communications capabilities of their smart devices [2]. In particular, the average smart device is equipped with a wide array of sensors (e.g., the camera, microphone, etc), and it possesses powerful communication potential (e.g., 4G/5G, WiFi, etc). These capabilities secure MCS access to a rich spectrum of heterogeneous data, which is processed to infer information used in various SC services. A prevalent class of services is *smart emergency* services, which is our focus in this work.

An MCS-based Smart Emergency (MCS-SE) framework improves emergency response services by enhancing the situational awareness. The core functions of an MCS-SE framework are a) timely detection of the emergency, b) precise estimation of incurred damages, c) rapid and efficient recovery planning, and d) provision of real-time assistance to guide the affected crowds to safety. Evidently, the lack and/or tardiness of information will aggravate the crisis situation. The immediate result of this is not only misplaced response and recovery efforts, but also inevitable significant economic and human losses.

As outlined in [3], leveraging heterogeneous data improves the performance of SE systems in three ways: 1) the collection and integration of real-time data from non-conventional sources, 2) robust and efficient data delivery and analysis techniques, and 3) reliable and situation-aware decision-making. An MCS-SE system relies on the crowd to create real-time feedback loops on the emergency, which in turn are used to plan, implement, and update the appropriate response measures. It is easily seen that traditional emergency management systems, such as those based on Wireless Sensor Networks (WSNs), are usually lacking in many aspects, especially timeliness, robustness and resilience, rendering them appropriate to use in a limited scope of emergency situations.

In general, the field of SE systems is a new one, particularly MCS-based systems, where the basic idea is to exploit the availability of smart phones to achieve better management services. In this work, we focus our attention on the first core function of MCS-SE framework, i.e., *the detection of an emergency situation based on MCS-generated data*. For this function, a common metric used to benchmark the effectiveness of the detection process is the time needed by the decision maker to recognize that the data indicates an evident emergency situation, which we call the *decision time*. Intuitively, a fast decision time is pivotal to the efficacy of the SE system.

However, each data item accessible by the decision maker carries varying levels of certainty and veracity in accordance to the MCS participant who provided it. The impact of stress or disinformation, inadequate sensor-calibration, and communication-related issues are of crucial importance [3]. In worse cases, misleading data can be provided by malicious participants intentionally to hinder end-service delivery (e.g., in the case of terrorist attacks) [4]. Cursory and hasty evaluation of the data bears high risks that increase the possibility of a false alarm, or worse, the complete miss detection of an emergency situation.

Thus, the decision-making process involves a time-quality trade-off to balance the performance of the MCS-SE detection

978-1-7281-2999-0/19/$31.00 ©2019 IEEE

system to provide a prompt and reliable service. Specifically, the decision maker aims to arrive at a decision as quickly as possible such that the decision satisfies a given quality threshold. In this paper, we present this problem based on concepts drawn from Detection Theory [5], where we aim to minimize the decision time subject to a Bayesian risk criterion. We first show our problem is NP-hard and entails high computational complexity. We propose an algorithm that greedily selects participants based on their expected tardiness and uses an optimal fusion rule to make its final decision.

The remainder of the paper is organized as follows. In section II, we discuss related work. In section III, we introduce the system model followed by the proposed scheme in Section IV. Section V presents and discusses simulation results. Finally, section VI presents our conclusions.

II. Related Work

Although the advancements in the Internet of Things (IoT) technology have unfolded infinite possibilities for the realization of SC services and applications, there is still a scarcity of research exploring the field of smart emergency system.

The majority of previous research focuses on smart emergency response services aiming to navigate the crowd to safety by leveraging WSNs. In [6] the authors propose a distributed WSN-based algorithm for evacuation assistance. The goal of the proposed model is to maximize the time that a crowd member will stay ahead of the hazard as it progresses through the emergency location. Additionally, [7] develops an adaptive WSN-based guiding protocol that takes several factors into account such as distance to exits and exit capacity. The protocol guides crowd members to safety while aiming to balance the load across multiple exits. Additionally, [8] propose an integrative distributed simulation environment. The goal is to build a robust software framework to improve the real-time emergency response system's flexibility and scalability.

Other more relevant works utilize WSNs for the detection of an emergency. For example, the authors in [9] propose a new WSN-based approach for early forest fire detection based on data mining techniques. The approach partitions nodes into sets that detect fires in an energy-efficient manner. The work in [11] presents a WSN-based approach assisted by satellite monitoring and aerial patrolling for fire detection. A cluster-based network hierarchy is proposed to detect and extinguish a fire in a timely manner. As explained earlier, MCS offers a more appealing solution for its advantages over WSNs, including infrastructure-less operation, mobility, coverage, costs, connectivity, lifetime, and power-efficiency.

The work in [12] presents an efficient convolutional neural network technique for fire detection in surveillance videos. While similar machine learning techniques can be tuned for high accuracy, one major drawback is the need of huge datasets required for training and decision-making, which might be infeasible in an emergency situation. On the other hand, the work in [10] proposes a reputation-based contribution assessment scheme aiming to provide the rescue personnel with trusted data. The scheme works by dividing the area into sectors and performs inter- and intra-sector filtering rounds to evaluate the data.

A few recent works specifically consider the realization of a smart city emergency management framework. In [3] the authors present a futuristic view of an information infrastructure that leverages MCS and heterogeneous data to improve emergency services. Their proposed three-component infrastructure details the integration of large-scale MCS with heterogeneous data analytics, along with a strategic decision-making process that improves the overall efficacy of the system.

In addition, [13] presents a comprehensive discussion of state-the-art IoT-supported protocols that facilitate response services such as early warning, data analytics, knowledge aggregation, remote monitoring, and victim localization. Another work [14] proposes a novel end-to-end infrastructure for disaster detection, prediction, and response in smart cities. The proposed smart system relies on MCS for constant data collection for event detection and prediction, and the internet of everything for disaster management and response. These works are restricted to visionary discussions of the infrastructures, protocols, trends and open challenges pertaining to SE detection and response systems. Contrary, our work addresses the specific problem of an emergency detection in a heterogeneous MCS environment and provides a direct mathematical treatment of the proposed problem.

III. System model

We adopt a general MCS system model, consisting of a central server referred to as the *administrator* whose goal is to to make a decision about a certain assumption. This assumption is referred to as the *hypothesis*, which can be one of two types: the null hypothesis H_0, or the alternative hypothesis H_1. In our context, H_0 indicates that no emergency situation exists, while H_1 reflects an emergency situation. The administrator has access to a set of possible participants denoted by $\mathcal{P} : \{p_k, k = 1, 2, ..., |\mathcal{P}|\}$, each of which owns a smart device with an application that facilitates the communication with the administrator. The veracity of each participant is determined by a reputation value denoted by r_k, obtained by the participant's previous history with other MCS applications. The administrator aims to recruit a subset of $K \leq |\mathcal{P}|$ participants who travel from their current location to the area of interest to survey the existence of an emergency situation at that given area. Subsequently, each recruited participant makes a binary decision denoted by $d_k \in \{0, 1\}$, where $d_k = 0$ indicates that participant k reports the null hypothesis H_0 (no emergency situation), and $d_k = 1$ indicates that participant k communicates the alternative hypothesis H_1 (an emergency situation exists). The administrator gathers participants' decisions and combines them to arrive at a final decision D regarding the hypothesis test, where $D \in \{0, 1\}$.

Ideally, we desire to have the administrator make its final decision D in the fastest manner possible, subject to a predefined quality constraint. We interpret the quality of D as a function of the individual participants' decisions, which

TABLE I: Testing hypotheses

	Decision	
Truth	Accept H_0	Accept H_1
H_0	True negative	False positive
H_1	False negative	True positive

are based on their respective reputation levels r_k. Therefore, our problem is to select a subset of the participants $\mathcal{P}_K$ to minimize the expected decision time of the administrator $t_d(\mathcal{P}_K)$, such that the quality of D is maintained above a threshold q^*. Mathematically, this can be expressed as:

$$\begin{array}{lrcl} \min\limits_{\mathcal{P}} & t_d(\mathcal{P}_K) & & \\ \text{s.t.} & Q(D) & \geq & q^* \end{array} \tag{1}$$

where $Q(D)$ is a function that quantifies the quality of our decision.

Viewing the administrator's task as a decision problem related to a hypothesis test, we opt to borrow mathematical concepts from Detection Theory [5] to solve our optimization problem in Eq. (1). In Detection Theory, a bank of sensors observes a given phenomenon (e.g., a target) and form binary decisions that are transmitted to an administrator for fusion. In our context, these sensors correspond to our MCS participants. Usually, the objective in a Detection Theory problem is to find optimal data-dependent decision rules at the local (i.e., for every participant) or the global (i.e., for the administrator) level, such that certain performance characteristics (e.g., probability of error) are satisfied. Now, we define some probabilistic concepts that characterize the performance of the administrator as follows:

- Probability of detection P_D: The conditional likelihood of a true positive, i.e., accepting H_1 when an emergency situation exists in reality.
- Probability of miss P_M: The conditional likelihood of a false negative, i.e., accepting H_0 when an emergency situation is actually present.
- Probability of false alarm P_{FA}: The conditional likelihood of a false positive, i.e., accepting H_1 when no emergency situation exists.

Obviously, these probabilities along with the probability of a true negative $P(H_0|H_0)$ are mutually-exclusive and collectively exhaust the sample space, as illustrated in Table I. A well-known concept in Detection Theory is *Bayesian risk* β, used to gauge the incurred cost for all possible courses of action associated with these probabilities. In other words, the value of β is representative of the posterior expectation of a *loss function* associated with the all possible outcomes of the detection procedure. Let the a priori probabilities of H_0 and H_1 be $P_0 = P(H_0)$ and $P_1 = P(H_1)$, respectively. Then the Bayesian risk at the administrator is:

$$\beta = C_{00}P_0(1 - P_{FA}) + C_{11}P_1P_D + C_{10}P_0P_{FA} + C_{01}P_1P_M \tag{2}$$

where $C_{ij}, i, j \in \{0, 1\}$ is the loss associated when $D = H_i$ given that H_j is true. Note that in a general emergency situation, correctly detected positives and negatives should not incur any losses for the system administrator. Therefore, we set $C_{ii}, i \in \{0, 1\}$ to zero, and rewrite Eq. (2) as:

$$\beta = C_{10}P_0P_{FA} + C_{01}P_1P_M \tag{3}$$

In the case that $C_{10} = C_{01} = 1$, it is easily seen that Eq. (3) becomes the average probability of error made at the administrator level. In our context, C_{10} indicates the loss brought by a false alarm causing a waste of the administrator's resources (e.g., calling emergency responders where they are not needed). A high number of false alarms can lead to alarm fatigue, where one chooses to ignore an alarm given the high probability that it is false, which further worsens the time-effectiveness of the system. On the other hand, C_{01} indicates the losses resulting from a false negative, which intuitively has much more serious effects as it directly affects human lives. Here, we note that the Bayesian risk in Eq. (3) is complementary to the quality function constraining our optimization problem Eq. (1). Therefore, we can rewrite:

$$\begin{array}{lrcl} \min\limits_{\mathcal{P}} & t_d(\mathcal{P}_K) & & \\ \text{s.t.} & \beta(\mathcal{P}_K) & \leq & \beta_0 \end{array} \tag{4}$$

where β_0 is the maximum Bayesian risk allowed by the system. Note that β is dependent on the values of $C_{i,j}$ and the global probabilities P_{FA} and P_M as in Eq. (3). Clearly, these global probabilities are also strongly dependent on the subset of participants $\mathcal{P}_K$ because P_{FA} and P_M are functions of the local probabilities of false alarm and miss detection for each participant in the recruited set $\mathcal{P}_K$. In the following discussion, we aim to establish this dependence mathematically and illustrate the relationship between these local probabilities and the reputation values for each participant.

As explained earlier, participants' provided decisions have varying levels of reputations obtained from previous history (e.g., acquired from other MCS applications). In our context, we recognize the unique nature of the emergency situation where irrational behaviour is observed. This behaviour results from contagious panic and distress, causing participants to provide incorrect decisions. Nevertheless, there is a close relationship between participants' reputations and the probabilities of correct decisions. Therefore, we define the kth participant's probabilities of miss detection and false alarm as:

$$P_{M_k} = 1 - \rho_{k,m}r_k \tag{5a}$$

$$P_{FA_k} = 1 - \rho_{k,f}r_k \tag{5b}$$

where $\rho_{k,m} \in [0, 1]$ and $\rho_{k,f} \in [0, 1]$ are scaling factors defined to adjust the value of the reputation to the probabilities of miss detection and false alarm. From Eq. (5), it is straightforward that $P_{D,k} = \rho_{k,m}r_k$ which is self-explanatory. Note that $\rho_{k,m}$ and $\rho_{k,f}$ are participant-specific, and they allow the administrator to distinguish between the probabilities of a participant providing a miss detection and a false alarm decision. The final step in our mathematical treatment is to write the probabilities of miss detection and false alarm at the administrator level as functions of the local probabilities in Eq. (5). Here, we assume that participants' decisions are statistically independent. It is well-established that the optimal fusion rule for the administrator in a minimum Bayesian risk distributed detection network is actually a Likelihood Ratio Test (LRT) given by [5]:

$$L(\mathbf{d}) = \frac{P(\mathbf{d} \mid H_1)}{P(\mathbf{d} \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta = \frac{P_0 C_{10}}{P_1 C_{01}} \tag{6}$$

where $\mathbf{d} = [d_1, d_2, ..., d_K]$ is the collection of k decisions delivered to the administrator and η is called the decision threshold. Based upon Eq. (6), we can write the probabilities of false alarm and miss detection at the administrator as:

$$P_{FA} = \sum_{L(\mathbf{d}) \geq \eta} P(\mathbf{d} \mid H_0) = \sum_{\mathbf{J}} \Big| \prod_{k=1}^{K} (d_k - P_{FA_k}) \Big| \cdot U\left[\prod_{k=1}^{K} \left(\frac{P_{D_k}}{P_{FA_k}} \right)^{1-d_k} \left(\frac{1-P_{D_k}}{1-P_{FA_k}} \right)^{d_k} - \eta \right] \tag{7}$$

$$P_{M} = \sum_{L(\mathbf{d}) \geq \eta} P(\mathbf{d} \mid H_1) = \sum_{\mathbf{J}} \Big| \prod_{k=1}^{K} (d_k - P_{M_k}) \Big| \cdot U\left[\eta - \prod_{k=1}^{K} \left(\frac{P_{D_k}}{P_{FA_k}} \right)^{d_k} \left(\frac{1-P_{D_k}}{1-P_{FA_k}} \right)^{1-d_k} \right] \tag{8}$$

where $\mathbf{J}$ contains all the possible permutations of the binary variables d_k, and $U(.)$ is the unit step function. In general, the summation over $\mathbf{D}$ for k participants indicates $2^K!$ cases to be considered. Specifically, for only two participants, $2^2! = 24$ cases should be considered to evaluate P_{FA} and P_M. The implication of this is that the optimization problem in (4) can be reformulated by introducing a binary scheduling variable for each participant. By doing so, the problem becomes a non-linear binary integer program, which is known to be NP-hard [15]. Hence, in the following subsection we propose a greedy algorithm that selects participants based on their respective arrival times to the time of the emergency, and then uses an optimal fusion rule once quality-based stopping criterion is satisfied to combine their decisions to arrive at the final decision D.

IV. Proposed Solution

In the previous section, it was shown that the selection of a subset $\mathcal{P}_k$ that minimizes the decision time $t_d(\mathcal{P}_k)$ under a maximum Bayesian risk constraint is a computationally difficult task. In order to develop our greedy algorithm, let $l_k = (x_k, y_k)$ be a two-tuple denoting the current location of participant k, and let time be divided into equal-length epochs denoted by $\{e = 1, 2, ...\}$. To achieve minimal $t_d(\mathcal{P}_k)$, the administrator needs to select participants closest to the area of interest, such that the travel time is minimized. Participants' reputation levels are leveraged to a) calculate a reputation-based stopping criterion, and b) make the final decision D according to a certain fusion rule. This is achieved by carrying Algorithm 1 and 2, as follows.

Specifically, at the beginning of each epoch e, the administrator recruits the participants' subset $\mathcal{P}_e \subseteq \mathcal{P}$, where $\mathcal{P}_e$ contains the set of participants whose estimated arrival time $t_{k,e}$ falls within the time epoch e. In this manner, the administrator has access to on-site real-time information delivered by decisions from the recruited set of participants. The participants report a decision, hereinafter denoted by $d_{k,e}$ to distinguish between decisions delivered in different epochs. Here, we assume that a recruited participant continues to provide reports in each subsequent epoch until the administrator halts the sensing process. Once the decisions are collected from in $\mathcal{P}_e$. the administrator checks its stopping criterion in Algorithm 2, which will be explained shortly. If Algorithm 2 decides to continue the sensing process, the administrator recruits another subset at $e+1$ until stopped by Algorithm 2.

Algorithm 1 The participant selection algorithm

Input: $\mathcal{P}, r_k, l_k, \rho_{k,m}, \rho_{k,f} \forall k$
Output: D

```
flag ← 1
e ← 1
$\mathcal{P}_k \leftarrow \emptyset$
Get $t_k \forall k \in \mathcal{P}$
$\mathcal{P}_e \leftarrow$ all $k$ with $k \leq e$
while $flag \neq 0$ do
    $P_k \leftarrow \mathcal{P}_e$
    $\mathcal{P} \setminus \mathcal{P}_e$
    Get $d_k \forall k \in \mathcal{P}_k$
    for all $k \in \mathcal{P}_k$ do
        if $d_{k,e} - d_{k,e-1} = 1$ then
            $r_k \leftarrow max\{0, r_k - \delta_1 C_{01}\}$
            $P_{M_k} \leftarrow 1 - \rho_{k,m} r_k$
            $P_{FA_k} \leftarrow 1 - \rho_{k,f} r_k$
        end if
        if $d_{k,e} - d_{k,e-1} = -1$ then
            $r_k \leftarrow max\{0, r_k - \delta_2 C_{10}\}$
            $P_{M_k} \leftarrow 1 - \rho_{k,m} r_k$
            $P_{FA_k} \leftarrow 1 - \rho_{k,f} r_k$
        end if
    end for
    Get $A$                                  ▷ Call Algorithm 2
    if $A =$ 'stop' then
        $flag \leftarrow 0$
        Calculate $D$ according to Eq. (9)
    else
        $e \leftarrow e + 1$
        $\mathcal{P}_e \leftarrow$ all $k$ with $k \leq e$
    end if
end while
return $D$
```

Algorithm 2 The stopping criterion algorithm

```
Input: $\pi, r_k \forall k \in \mathcal{P}_k, t_k \forall k \in \mathcal{P}$
Output: $A$
$\mathcal{P}_{e+1} \leftarrow$ all $k$ with $k \leq e+1$
if $\mathcal{P}_{e+1} = \emptyset$ then
    $A \leftarrow$ stop
else
    $R \leftarrow \frac{\sum_{\forall k \in \mathcal{P}_k} r_k}{|\mathcal{P}_k|}$
    if $R \geq \frac{\pi(|\mathcal{P}_k|+1)}{|\mathcal{P}_k|}$ then
        $A \leftarrow$ stop
    else
        $A \leftarrow$ continue
    end if
end if
return $A$
```

Once the sensing process stops, the administrator combines the decisions of the participants $d_{k,e}$ delivered in the last epoch according to the LRT test in Eq. (6), which can be rewritten as [5]:

$$\sum_{k=1}^{k_e} \left[d_{k,e} \log \frac{1 - P_{M_k}}{P_{FA_k}} + (1 - d_{k,e}) \log \frac{P_{M_k}}{1 - P_{FA_k}} \right] \underset{H_0}{\overset{H_1}{\gtrless}} log(\eta) \tag{9}$$

Here, Eq. (9) resembles the optimal fusion rule that minimizes the average Bayesian risk at the administrator when making the final decision D. Obviously, D is composed based on a reputation-based weighted sum of individual participants decisions.

Note that in Algorithm 1, if an already recruited participant changes the decision from $d_k = 1$ to $d_k = 0$, then the algorithm penalizes this participant by decreasing its reputation r_k by the value $\delta_1 C_{01}$, where δ_1 is an adjusting factor to ensure that r_k is $\in [0, 1]$. On the other hand, if a participant changes the decision from $d_k = 0$ to $d_k = 1$, its reputation score is deducted by the value $\delta_2 C_{01}$, where δ_2 is also an adjusting factor to ensure that r_k is $\in [0, 1]$ (as seen in Algorithm 1: lines 10 through 21). In this manner, we decrease the weight that this participant carries in the fusion rule. These measures ensure that participants who provide fluctuating decisions are gradually eliminated in the decision making process.

At the end of each epoch e, the administrator executes Algorithm 2 to decide an action denoted by A, which indicates to the administrator whether to *continue* or *stop* the sensing process. The algorithm works as follows. At epoch e, the administrator has already recruited a set of $|\mathcal{P}_k|$ participants $\mathcal{P}_k = \bigcup_{\forall e} \mathcal{P}_e$. Let R denote the average reputation score for all recruited participants contained in $\mathcal{P}_k$. We are interested in estimating the probability that the majority of the participants in the set $\mathcal{P}_k$ will generate the correct decision. The Condorcet Jury Theorem (CJT) states that the majority of a group is better at choosing one of two alternatives than any single individual, as long as individual decisions are independent of each other [16]. Specifically, for a group of heterogeneous participants (varying r_k), 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:

$$R \geq \frac{\pi(|\mathcal{P}_k| + 1)}{|\mathcal{P}_k|} \tag{10}$$

Hence, Algorithm 2 halts the sensing process if the probability that π of the subset $\mathcal{P}_k$ will make the correct decision, and continues the sensing process otherwise. Note that a pre-check is done on the expected number of participants to arrive in $e+1$. If no participants are expected to join $\mathcal{P}_k$, the algorithm stops in order to preserve the timeliness of the decision.

V. Performance evaluation

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

A. Simulation Environment

We conduct simulation experiments to evaluate our proposed detection scheme. The scheme recruits a new set of participants in each epoch, where the maximum number of new participants is varied in $[2, 20]$. For each participant, r_k is randomly generated from a uniform distribution. We set $\rho_{k,m} = \rho_{k,f} = 1 \forall k$, and set $\delta_1 = \delta_2 = 0.001$. Let the a priori probability that the null hypothesis H_0 is true be $P_0 = 0.95$, and for the alternative hypothesis H_1 be $P_1 = 0.05$. At each run, a ground truth is generated from a Bernoulli distribution according to these a priori probabilities. Each participant generates a decision at each epoch $d_{k,e}$ from a Bernoulli distribution, where the probability of generating the ground truth is its current reputation score r_k. Moreover, let the Bayesian risk coefficients be $C_{10} = C_{01} = 1$. We let the proportion of the CJT majority π vary in $[0.5, 0.9]$.

B. Simulation Results

In order to evaluate our proposed scheme, we compare it to a widely used baseline where the decision is based on the majority in the first epoch $e = 1$. Specifically, the administrator recruits the first set of participants, and performs a simple majority test to decide D. In case of a tie, the administrator randomly chooses between H_0 and H_1. We will study two performance metrics: a) the Correct Detection Rate (CDR) defined as the ratio of correctly detected ground truths to the total number of instances, and b) the average number of epochs needed to arrive at the final decision D, to denote the delay in the system. We study the performance of our scheme under various values of the CJT majority proportion π and compare it to the baseline aforementioned.

We begin by plotting the CDR in Fig. 1 against an increasing number of the maximum new participants who join at each epoch e. The figure shows that the baseline achieves a virtually constant CDR with slight variation around 50%, and the reason is that it follows a simple majority rule regardless of

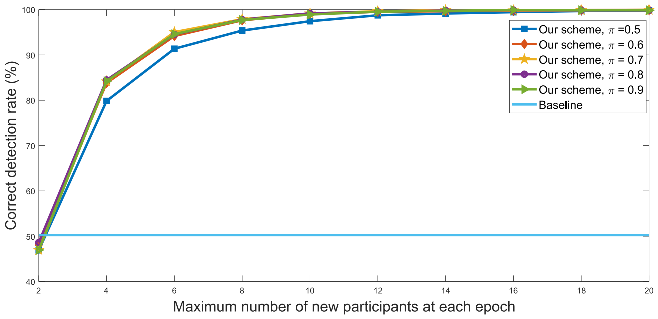

Fig. 1: Correct detection rate vs. the maximum number of new participants.

participants' reputation levels. On the contrary, our scheme begins with a CDR close to that of the baseline when the maximum number of new participants is 2, but drastically increases from the baseline's achieved CDR as the number of participants increases. Intuitively, as we set π to a larger value, more participants have a higher probability of choosing the correct decision, and thus the CDR grows more quickly to peak at around 98%. However, we notice that the CDR growth almost saturates for $\pi > 0.7$ when the number of new participants exceeds 10.

In Fig. 2, we plot the average number of epochs needed to arrive at the final decision D for a variable maximum number of new participants. Note that here we do not include the baseline because it makes its decision in the first epoch solely $e = 1$. For our scheme, it is seen that a higher CJT majority value π will require longer time to reach to the final decision D. Here, the time-quality trade-off is clear, in the sense that a higher CJT majority enforces a better quality constraint on the decision D when compared to the previous figure. Finally, as the maximum number of new participants increases, it is shown that the administrator needs a higher number of epochs to satisfy the quality criterion according to CJT, because as the number of participants increases, it is less probable that they achieve a majority proportion equal to π.

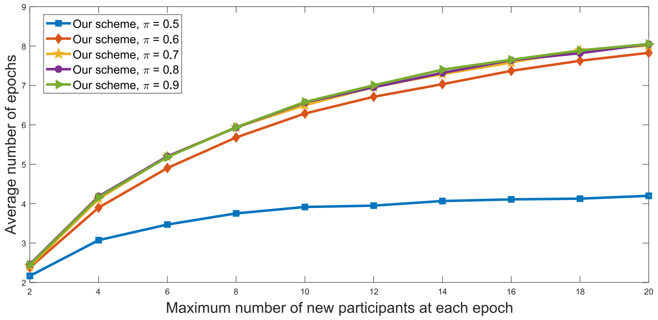

Fig. 2: Average number of epochs vs. the maximum number of new participants.

VI. Conclusions

In this paper, we explore the problem of emergency detection based on Mobile Crowd Sensing (MCS) in a reputation-aware environment. We draw on concepts from Detection Theory to formulate our optimization problem, where the objective is to minimize the time needed to detect an emergency under a predefined Bayesian risk constraint. We show that our problem is NP-hard, and propose a greedy reputation-based algorithm that reduces the tardiness of the decision-making process. Simulation results highlight the trade-off between the delay and quality, and show that our scheme improves the correct detection rate compared to the baseline technique.

Acknowledgment

This work was made possible by NPRP grant NPRP 9-185-2-096 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] A. Gharaibeh et al., "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies," in *IEEE Communications Surveys & Tutorials,* vol. 19, no. 4, pp. 2456-2501, 2017.

[2] B. Guo et al., "Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm", in *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1-31, 2015.

[3] M. Abu-Elkheir, H. S. Hassanein and S. M. A. Oteafy, "Enhancing Emergency Response Systems through Leveraging Crowdsensing and Heterogeneous data," in *Proc. of International Wireless Communications and Mobile Computing Conf. (IWCMC)*, Cyprus, Sep., 2016.

[4] R. F. ElKhatib, N. Zorba and H. S. Hassanein, "A Fair Reputation-based Incentive Mechanism for Cooperative Crowd Sensing", in *Proc. of IEEE Global Communications Conf. (GLOBECOM)*, UAE, Dec., 2018.

[5] P. K. Varshney, "Distributed Detection and Data Fusion," New York: Springer-Verlag, 1996.

[6] M. Barnes, H. Leather and D. K. Arvind, "Emergency Evacuation using Wireless Sensor Networks," in *Proc. of IEEE Conf. on Local Computer Networks (LCN)*, Ireland, Oct., 2007.

[7] C. Lin, P. Chen and W. Chen, , "An Adaptive Guiding Protocol for Crowd Evacuation Based on Wireless Sensor Networks," in *Proc. of IEEE Vehicular Technology Conf. (VTC Spring),* Germany, Jun., 2013.

[8] A. Boukerche, Ming Zhang and R. W. Pazzi, "An Adaptive Virtual Simulation and Real-time Emergency Response System," in *Proc. IEEE International Conf. on Virtual Environments, Human-Computer Interfaces and Measurements Systems*, Hong Kong, May, 2009.

[9] M. Saoudi et al., "Energy-Efficient Data Mining Techniques for Emergency Detection in Wireless Sensor Networks," in *Proc. of IEEE ICUI Conf.*, France, Jul., 2016.

[10] M.A. Alswailim, H.S. Hassanein, and M. Zulkernine, "A Participant Contribution Trust Scheme for Crisis Response Systems," in *Proc. IEEE Global Communications Conf. (GLOBECOM)*, Singapore, Dec., 2017

[11] J. Zhang et al., "Forest Fire Detection System Based on Wireless Sensor Network," in *Proc. of 4th IEEE Conf. on Industrial Electronics and Applications*, China, May, 2009.

[12] K. Muhammad et al., "Convolutional Neural Networks Based Fire Detection in Surveillance Videos," in *IEEE Access*, vol. 6, pp. 18174-18183, 2018.

[13] P. P. Ray, M. Mukherjee and L. Shu, , "Internet of Things for Disaster Management: State-of-the-art and Prospects," in *IEEE Access*, vol. 5, pp. 818–835, 2017.

[14] A. Boukerche and R. W. L. Coutinho, "Smart Disaster Detection and Response System for Smart Cities," in *Proc. of IEEE Symposium on Computers and Communications (ISCC)*, Brazil, Jun., 2018.

[15] S. Boyd and L. Vandenberghe, "Convex optimization problems", in *Convex Optimization*, 1st ed., Cambridge University Press, 2004, ch. 4.

[16] S. Kanazawa, "A Brief Note on a Further Refinement of the Condorcet Jury Theorem for Heterogeneous Groups", in *Mathematical Social Sciences*, vol. 35, pp. 69-73, 1998.