<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>An efficient data evacuation strategy for sensor networks in postdisaster applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Liu, Ming; Liu, Bang; Wen, Yonggang</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Liu, M., Liu, B., &amp; Wen, Y. (2013). An efficient data evacuation strategy for sensor networks in postdisaster applications. International journal of distributed sensor networks, 2013, 718297-.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2013</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/17432">http://hdl.handle.net/10220/17432</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 2013 Ming Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.</td>
</tr>
</tbody>
</table>
Research Article

An Efficient Data Evacuation Strategy for Sensor Networks in Postdisaster Applications

Ming Liu,1 Bang Liu,1 and Yonggang Wen2

1 School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China
2 School of Computer Engineering, Nanyang Technological University, Singapore 639798

Correspondence should be addressed to Ming Liu; csmliu@uestc.edu.cn

Received 10 October 2012; Accepted 26 November 2012

Abstract

Disasters often result in a tremendous cost to our society. Previously, wireless sensor networks have been proposed to provide information for decision-making in postdisaster relief operations. The existing WSN solutions for postdisaster operations normally assume that the deployed sensor network can tolerate the damage caused by disasters and maintain its connectivity and coverage, even though a significant portion of nodes have been physically destroyed. Inspired by the “blackbox” technique, we propose that preserving “the last snapshot” of the whole network and transferring those data to a safe zone would be the most logical approach to provide necessary information for rescuing lives and controlling damages. In this paper, we introduce data evacuation (DE), an original idea that takes advantage of the survival time of the WSN, that is, the gap from the time when the disaster hits and the time when the WSN is paralyzed, to transmit critical data to sensor nodes in the safe zone. Numerical investigations reveal the effectiveness of our proposed DE algorithm.

1. Introduction

While disasters could result in a tremendous cost to our society, access to environment information in the affected area, such as, damage level and life signals, has been proven crucial for relief operations. Hundreds of disasters in various scales, including earthquakes, flooding, tornadoes, oil spilling, and mining accidents, happen around the world each year. Not only do they bring in huge economic loss by destroying assets, but also they can take lives in large quantities. According to a disaster statistic report [1], the average number of people affected by disasters is more than two hundred million per year from 1991 to 2005, and thousands of them lost their lives. When disasters hit, relief operations often focus on saving lives and reducing property damages. Given the chaos in the affected areas, effective relief operations highly depend on timely access to environment information. For example, the life vitals of survivors would be extremely helpful for rescue workers to determine where to dig a tunnel to the spot. Previously, wireless sensor networks [2–4] have been proposed to gather useful information in disasters such as earthquake, volcano eruption, and mining accidents.

However, even with sensor networks, gathering crucial information in postdisaster relief operations turns out unpredictably challenging. When a disaster strikes, the communication facilities, power units, and roads will usually be destroyed, which, along with some concomitant accidents, for example, building collapse, fires, and gas explosions, and so forth, may disrupt the normal functionalities of sensor networks. For example, sensor nodes could be damaged in the event of a fire and communication channels are thus disconnected. Previous researches [5–10] tend to overlook this possibility and thus result in relief solutions that are inherently impractical. As a result, the decision-making process could be paralyzed with incomplete information.

In this paper, inspired by the “blackbox” solution in flight industry, we propose data evacuation (DE): an original idea which utilizes the surviving time interval of sensor nodes, namely, the duration in which WSNs still function after the disaster, to transmit vital data to the sensor nodes in the safe
zone. Our idea relies on the following observation. It is quite possible that the buildings or local resources do not get damaged or destroyed at the beginning of most disasters. As a result, the deployed sensor network can keep working for a while before it becomes completely paralyzed. This grace period can be used to transit vital data gathered by the WSN.

Our proposed data evacuation works under extreme situations, thus requiring different design metrics from normal wireless sensor networks. From an engineering perspective, one would like to gather as much information as possible, preferably within short period as much as possible. The former metric corresponds to the evacuation ratio, defined as the amount of successfully rescued information in respect to the whole amount of information gathered by the network; the latter corresponds to the evacuation time, defined as the amount of time spent in rescuing all the information. However, as with any engineering design problem, these two metrics are competing with each other. Since maximizing evacuation ratio and minimizing evacuation time cannot be achieved simultaneously in any design of DE, it is our responsibility to judiciously balance a tradeoff between the two metrics in a realistic solution of DE.

In this research, we first reveal a mathematical structure of our problem, and then our main focus turns to develop and evaluate scalable distributed algorithms for our proposed DE strategy. If one would trace the path of each bit of data transits in the network, this problem can be modeled as a non-linear programming problem with multiple minimums in its support. Rather than seeking the analytical solution for such a formulation, we take a pragmatic approach to design distributed protocols to route the vital data to safe zones in an affected region. We will propose two distributed data-rescuing protocols, namely, a gradient-based (GRAD-DE) one and a gravitation-based (GRAV-DE) one. The former is related to Newton’s method [11] for non-linear programming and the latter is related to Newton’s law of physics [12]. In addition, we will evaluate their efficacy under the aforementioned design metrics with extensive simulation. Evaluation shows the significant effectiveness of DE strategies for postdisaster applications. The major contributions of this work are as follows.

(i) To the best of our knowledge, we are the first to propose the idea of data evacuation for postdisaster applications. The basic operation of DE is to send sensitive data from the whole network to the nodes in the safe zone; in that case, the relief efforts of rescue group will benefit a lot from the reproduction of “the last shot” of the monitoring region based on the saved sensitive data.

(ii) Building the mathematical structure of our problem, we propose two distributed data-rescuing algorithms. Our algorithms are mathematic avatars of Newton’s method on non-linear optimization and Newton’s law of physics.

(iii) Extensive simulation has been conducted to verify the efficacy of GRAD-DE and GRAV-DE and illustrate the fundamental tradeoff between the two design metrics: evacuation time and evacuation ratio.

The remainder of this paper is organized as follows. Section 2 discusses the related work. Section 3 gives the definitions and assumptions about disaster scenario and network model. Section 4 presents the detailed design of GRAD-DE and GRAV-DE, followed by their evaluations in Section 5. Section 6 concludes the paper.

2. Related Work

One of the critical tasks for postdisaster relief is to collect urgent information quickly and safely to rescue lives and control damages. There have been a lot of research works on data collection with wireless sensor networks. However, research on vital data collection in disaster circumstances has been rare.

Some previous research employ wireless sensor network to gather useful data in a hostile environment like earthquake or volcano [2–5]. Suzuki et al. present a high-density earthquake monitoring system in [2]. The raw data about earthquake is gathered by a sink node and can be used for further analysis after earthquake. But the collected data is just about earthquake rather than survivors. To estimate the individual damage in personal area, a WSN system is proposed in [3] to provide useful information to predict the individual damage, which is not accurate to serve for rescuing. In [5], Cayirci and Coplu presents a wireless sensor network (i.e., SENDROM), in which nodes are randomly deployed before disaster occurs, for disaster relief operations management. In postdisaster relief, rescue teams use mobile central nodes to gather information such as survivor’s location by querying the sensor nodes.

To collect data more efficiently, some works have studied hybrid networks for data collection in disaster situations [6–8]. These systems employ cellular systems (or wires systems) and sensor networks in parallel to achieve a superior performance, such as, high speed, high capacity, and wide area coverage. A hybrid network model in [9] collects damage assessment information from a large number of nodes, and its connectivity is maintained by an alternative route in the event of disasters. Fujiwara et al. employ a hybrid of sensor and cellular networks in [10]. They present a data collection system to detect damage in a disaster and to transmit the data to an emergency operation center. It applies the network scheme to a versatile data collection system using sensor networks for damage assessment and for victim detection beneath the rubble of collapsed buildings. However, in the hybrid network, the cellular network could be paralyzed by disasters quickly or congested by the sudden high load even if it survives so that the data collection system breaks down.

Among these works, they did not consider the possibility that some base stations of cellular networks or the sensor nodes might be collapsed or unreachable during or after disasters. In [13], authors presented a data collection framework which employs Ad hoc Relay Stations (ARSs). It can convey data from the collapsed area by sending them to the nearest ARSs. However, it is built on cellular networks, which would be destroyed immediately during disasters. Li and Liu present SASA [14], a Structure-Aware Self-Adaptive
wireless sensor network, for underground monitoring in coal mines. By regulating the mesh sensor network deployment and formulating a collaborative mechanism based on the regular beacon strategy, SASA is able to rapidly detect structural variations caused by underground collapses. The collapse holes can be located and outlined and the data can be transferred outside of the collapsed region. However, the stationary mesh network could be ruined and become unreliable when a collapse occurs.

To the best of our knowledge, this paper is the first one that considers a wireless sensor network under stress and evacuates the critical data to the safe zone for postdisaster relief operations.

3. System Models and Problem Description

3.1. Network Model. In this paper, we assume that $N$ sensor nodes are randomly uniformly deployed in an $M \times M$ square area $A$, and the communication radius of sensor node is $r$. The network can be modeled as an undirected graph $G = (V, L)$, where $V$ is the set of sensor nodes in the network, $|V|$ is the number of sensor nodes, and $L$ is the set of links between sensor nodes in the network. For any two nodes $v_i$ and $v_j$, if $\text{dist}(v_i, v_j) < r$, $v_i$ and $v_j$ are neighbors and there is a link $l(v_i, v_j)$ between them. For any node $v_i$, its neighbor node set is $\text{neighbor}(v_i)$.

In the event of a disaster, the capability of sensor nodes is assumed to be as follows.

(i) It can sense some meaningful event around. For example, sensor node can sense human vital signs through sound, infrared rays, temperature, image, and vibration sensors.

(ii) Sensor node can sense and measure the surrounding physical intensity (like the intensity of earthquake shock, temperature and smoke density in the fire, gas density before gas explosion, etc.) variation caused by a disaster.

(iii) Sensor node can rank itself as safe, critical, or dangerous, according to a predefined algorithm using the physical intensity variation it senses as inputs.

We do not assume the existence of a sink node that gathers all the data and routes to the relief center. When a serious disaster occurs, original communication infrastructure may be destroyed; even if some of them survive, they usually cannot provide effective service for disaster relief applications. In our approach, data evacuation is accomplished by collaborative efforts of every sensor node in the network to route the critical information to a few safe zones in the affected region.

3.2. Disaster Model. In this subsection, summarizing a set of common characteristics in most disasters, we construct a simplified disaster model, as follows.

Definition 1 (devastating event). We use a Quaternion ($C_i$, $I_i$, $T_i$, and $A_i$) to represent a devastating event $E_i$, where $C_i$ is the centre point of the zone where the devastating event occurs, given by the coordinate $(x_i, y_i)$; $I_i$ is the intensity of the devastating event; $T_i$ is the attenuation coefficient of disaster propagation; $A_i$ is the region that the devastating event affects.

Definition 2 (disaster). Disaster is a set of devastating events and could be denoted by $D = \{E_i \mid 0 \leq i \leq d - 1, d \in N\}$.

Let us look at an example. When a coal-mine accident (disaster) occurs, it probably consists of several gas explosions and water leak accidents, each of which corresponds to a devastating event. Each devastating event could be described by four elements: the position of event occurrence, the intensity of this event, the attenuation coefficient of this event, and the region affected by this event. The intensity $I_i$ is the highest in the centre point of a devastating event and weakens as it gets further away from the center point. Usually $T_i$ reflects the change of $I_i$ in the region where disaster affects. There is no common attenuation coefficient for disasters. For simplicity, we assume a linear attenuation coefficient denoted as $T_i$. Under the impact of $T_i$, a devastating event can be depicted as a subarea of which the intensity is linearly descending from a centre point. As an example, Figure 1 illustrates a typical intensity distribution of a disaster with four devastating events, and the intensity is collected with four devastating events, and the intensity is collected by sensors in the affected region. The centers of the four devastating events are $(15, 25), (25, 40), (55, 85),$ and $(85, 60)$. It can be seen that the intensity function has multiple sets of minimum points in its support (i.e., the affected region).

In this paper, according to the data that the sensor nodes collect, we define an algorithm to classify the state of the sensor node into three categories: safe, critical, and dangerous. Let $\text{intens}(v_i)$ be the intensity that the node $v_i$ senses; $I_s$, $I_d$ ($I_s < I_d$) are two thresholds which are predefined according to the disaster scene. Then, we have

$$\text{rank}(v_i) = \begin{cases} \text{safe,} & \text{intens}(v_i) < I_s, \\ \text{critical,} & I_s \leq \text{intens}(v_i) < I_d, \\ \text{dangerous,} & I_D \leq \text{intens}(v_i). \end{cases}$$

Let $V_S$, $V_C$, and $V_D$ represent the set of safe nodes, critical nodes, and dangerous nodes, respectively.

When a disaster occurs in a certain place, the disaster usually only affects a limited area near the center, and similar disaster damage often shares the same zone. According to
this, the three sets $V_S$, $V_C$, and $V_D$ will have their own zones geographically, and since, after a disaster happens, there exists a short period of time when the sensor nodes collect the intensity data and rank themselves, the disaster area will be divided into several zones, which could be safe, or critical, or dangerous.

**Definition 3 (zone).** The sensor nodes in a zone has the same rank level, and they are connected. Consider the zone to be a connected subgraph $G_i = (V_i, L_i)$, where $V_i \subseteq V$, $L_i \subseteq L$, $0 \leq i \leq g - 1$, $g$ is a positive integer and it represents the total number of zones in the whole area. For arbitrary two zones $G_i, G_j$, there are $V_i \cap V_j = \emptyset$, $L_i \cap L_j = \emptyset$, $1 \leq i < N$, $1 \leq j \leq N$, and $\bigcup_{i=0}^{g-1} V_i = V$. According to the rank level of each zone, we call it safe zone, or critical zone, or dangerous zone.

Figure 2 gives a vertical view for the disaster shown in Figure 1. Without the loss of generality, we adopt a normalized threshold of 0.5 for nonsafe zone in this paper and the threshold can be any value that manifests the physical meaning of a specific disaster (e.g., the Richter magnitude in earthquakes). In Figure 2, most area is covered by dangerous zone and critical zone (intens($v_i$) $\geq$ 0.5, for all $v_i \in V_C \cup V_D$), due to the devastating event’s influence, and only a small area is covered by safe zone (intens($v_i$) $< 0.5$, for all $v_i \in V_S$).

Sensor nodes in different ranks have varying surviving time, resulting in different roles in our data evacuation strategy. Sensor nodes in the dangerous zone have the shortest life time, only several seconds or dozens of seconds. Sensor nodes in the critical zone live longer, usually minutes or hours, because of less damage the devastating event causes in this zone, but the continuous damage will make the sensor nodes in critical zone ultimately destroyed. Sensor nodes in safe zone can live much longer, usually hours or days or longer, because of the long distance from the dangerous zone and the least damage the devastating event causes, so the sensor nodes in this zone are suitable to store valuable data for assisting personnel rescue and disaster analysis.

In our scheme, if one follows a piece of information, it normally traverses from dangerous zones, with possible route via critical zones, to two alternative destinations. It either arrives at some safe zone, or is trapped in dangerous/critical zones (lost in the end). For the former case, we adopt a definition for the path through which the information traverses, as follows.

**Definition 4 (effective evacuation path).** If a path $P = v_0v_1 \cdots v_{n-1}v_n$, $1 \leq i \leq n, v_0 \in V_C \cup V_D$, and $v_i \in V_S$ and such link $(v_j, v_{j+1})$, $0 \leq j \leq i-1$, $v_j \in V_S \cup V_C$, and $v_{j+1} \in V_D$ do not exist in path $P$, then $P$ is the effective evacuation path.

3.3. Problem Formulation and Its Mathematical Structure.

The end goal of our proposed data-rescuing strategy is to route the critical data sensed in the dangerous zone and critical zone to the safe zone for disaster relief and disaster analysis. The process of data evacuation can be expressed like this: for every sensitive data in any sensor node $v_i, v \in V_C \cup V_D$, data evacuation is to find an effective path and transmit the data to the safe zone. Any solution in this domain should have at least two desirable features. First, it should route as much information as possible. Second, data evacuation should be fast; otherwise the sensor nodes in the dangerous zone and critical zone could lose their data, or the sensor nodes in the effective evacuation path could be inactive.

As a manifest of the aforementioned features, we will focus on the following two performance metrics: (a) evacuation time: the time to complete the data evacuation process and (b) evacuation ratio: the percentage of whole sensitive data preserved in safe zone after finishing the data evacuation process. Data evacuation should be quick; otherwise the sensor nodes in the dangerous zone and critical zone could be damaged. As a result, some effective evacuation paths could fail to send the sensitive data to the safe zone.

The data evacuation protocols need to guarantee that the amount of preserved sensitive data can provide enough useful information for postdisaster applications.

This formulation renders itself an elegant mathematical polymorphism. For each piece of information, it should strive to follow a path to any safe zone as fast as possible. If one considers the disaster intensity map as a two-dimensional function and any safe zone as a set of points with a minimum value, the data evacuation problem is equivalent to a non-linear programming problem with multiple (usually unknown) minimums in its support. This structural polymorphism with non-linear optimization will inspire the development of two efficient data-rescuing algorithms, both of which will be elaborated in the next section and are distributed in nature.

4. Data Evacuation Protocols

In this section, we present two alternatives DE protocols, each of which is a greedy algorithm seeking to optimize one design metric. The first protocol routes the critical information through effective evacuation paths following the highest gradient in the disaster intensity map, and thus denoted as GRAD-DE. The second protocol routes the critical information by effective evacuation paths leading to the closest safe zone with the largest storage capacity. Intuitively,
the information is attracted by the gravitation (proximity and capacity) of the safe zone, and thus the protocol is denoted as GRAV-DE. The GRAD-DE protocol performs better in minimizing the evacuation time, while the GRAV-DE protocol excels in maximizing the evacuation ratio.

4.1. GRAD-DE Protocol

4.1.1. Detailed Design of GRAD-DE Protocol. The GRAD-DE protocol stems from the Newton's method (gradient based) for non-linear programming problems. One of the potential issues with Newton's method is that it could converge to local minimums. In our protocol, we allow a few steps to route the information to nodes with higher intensity, so that the critical message will not be trapped. Here is how the protocol works.

First, each sensor node obtains the intensity and the rank level of all its neighbors through a round of hello-message exchange. In the event of any disaster, a sensor node first senses the intensity of devastating event and determines its rank level based on the predefined $I_e$ and $I_d$. After that, it will broadcast a hello message, including its sensed intensity and self-determined rank level, to all neighbors.

Second, as water always flows downwards, in the GRAD-DE protocol, each sensor node forwards the sensitive data sensed locally or received from other nodes to its neighbor with the minimum sensed intensity. Obviously, in most cases, it is reasonable to send the sensitive data to the node with lower sensed intensity because it is the most logic step toward the safe zone (also suggested by the Newton's method). In order to avoid collision and reduce the communication cost, we adopt a single-copy forwarding strategy in the design.

This simple gradient-based forwarding strategy, however, could result in data trapped in stressed zones. For example, if a disaster consists of several devastating events, the sensed intensity ($>I_e$) of nodes in a certain region could be lower than the sensed intensity of any other nodes that surround this region. In this situation, the sensitive data of surrounding nodes may be forwarded to the "Highland Basin" as shown in Figure 3, and all sensitive data in this region will be trapped.

In order to avoid this problem (equivalently, the local minimums in non-linear programming problems), the GRAD-DE algorithm consists of three correction steps as follows.

Step 1. Upon receiving all the hello messages from its neighbors, each node marks itself if its intensity is lower than that of any other neighbor and broadcasts a warning message to prevent all its neighbors from sending sensitive data to it.

Step 2. When a node receives a warning message, if its all neighbors with smaller intensity have send warning messages to it, it will mark itself and broadcast a warning message to inform that it cannot play a relay role in an effective path. Otherwise, it just drops the received warning message.

Step 3. When a node has sensitive data to forward, it will check whether it has been marked. (a) If yes, it will send the sensitive data to the unmarked neighboring node with the lowest intensity. If it cannot find any unmarked neighboring node, it will send the sensitive data to the neighboring node with the highest intensity, with the hope that the data will escape from the trapped region from the trapped region as soon as possible. (b) If not, it means that this node is not located in a "Highland Basin" region, so the sensitive data can be sent to the unmarked neighboring node with the lowest intensity.

4.1.2. Pros and Cons of GRAD-DE Algorithm. In this subsection, we will discuss the advantages and disadvantages of the GRAD-DE protocol, respectively.

On one hand, the GRAD-DE protocol comes with a few desirable characteristics. First, the control-message overhead for the GRAD-DE protocol is limited and upper bounded by two times of the total number of sensor nodes. In most cases, each node broadcasts a one-hop hello message to all its neighbors. Only when a "Highland Basin" problem appears will the nodes in this region broadcast an extra one-hop warning message to prevent sensitive data being transmitted to this region. As a result, even in the worst case, the number of control messages sent by one node is 2. Second, the GRAD-DE protocol does not rely on detailed information of the network topology. Specifically, each node simply sends sensitive data to its neighbor with the minimum intensity. As a result, the evacuation time will not be too long since we do not incur additional delay in topology discovery. Third, the GRAD-DE protocol is a scalable and distributed algorithm for data rescuing under stress, with some resemblance to the famous Newton’s method in non-linear programming domain.

On the other hand, the GRAD-DE protocol has several drawbacks. For example, any effective evacuation path is predetermined by the intensity distribution in the affected region. If a relay node is damaged by devastating events, sensitive data transmission cannot be adapted to a new path. Although such an issue can be avoided by periodically sending hello messages, the control-message overhead would increase. Collision is another issue, which is caused by no topology control for the GRAD-DE protocol and cannot be solved thoroughly by relying on the IEEE 802.15.4 MAC protocol. Adjusting the time interval for data sending could...
be a way to avoid collisions; however, such a strategy would pay the penalty of prolonging evacuation time. Buffer overflow is also a problem for the GRAD-DE protocol. As shown in Figure 4 where $G_1^1$, $G_2^2$, and $G_3^3$ are three safe zones, the number of member nodes of these three safe zones are 2, 11, and 3, respectively. Unfortunately, the GRAD-DE protocol does not provide any information about safe zones, such as the number of safe zones and the storage capacity of safe zones. As a result of the blind data forwarding, Figure 4 illustrates that too many nodes blindly send their sensitive data to $G_1^1$ and $G_1^2$, although the storage capacity of these two zones is limited.

4.2. GRAV-DE Protocol

4.2.1. General Principle. The GRAV-DE protocol is proposed to avoid the buffer overflow problem in the GRAD-DE protocol, which happens because each sensor node blindly forwards its data to a random safe zone. Indeed, we believe that the protocol would better off if the data is forwarded to the closest safe zone with the maximum storage capacity. Such a principle is similar to Newton's theory of gravitation.

Intuitively, the movement of every single sensitive message to a certain safe zone can be regarded as it is attracted by the safe zone and moves to this zone along the direction of gravitational force between them if this gravitational force is bigger than that of any other force caused by different safe zones. As a result of this parallelism, one can see a natural mapping between concepts in data evacuation and those in physics, as summarized in Table 1, where $D_{ij}^j$ denotes the $j$th sensitive message of node $v_i$, and $\text{space}(G_j^j)$ denotes the storage size of certain safe zone $G_j^j$.

<table>
<thead>
<tr>
<th>Concepts in physics</th>
<th>Concepts in data evacuation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object 1</td>
<td>Single sensitive message of $v_i(D_{ij}^j)$</td>
<td>Single sensitive message can be seen as an object with unit mass</td>
</tr>
<tr>
<td>Object 2</td>
<td>Space of certain safe zone ($\text{space}(G_j^j)$)</td>
<td>The mass of $G_j^j$ is the storage size (messages) of this safe zone</td>
</tr>
<tr>
<td>$</td>
<td>D</td>
<td>$</td>
</tr>
</tbody>
</table>

For this object, the GRAV-DE protocol follows a three-step procedure.

(1) **Safe zone organization**: in our design, each connected component or isolated node with maximum sensed intensity $I_s < I_s$ can be seen as a safe zone.

(2) **Safe-zone/evacuation-path broadcast**: after safe zones have been identified, they will advertise their existence by broadcasting announcement messages to all nodes in critical or dangerous zones.

(3) **Evacuation path decision**: nodes under stressed zones can determine the effective evacuation path for data evacuation, similar to the Newton's law of gravitation.

In next three subsections, we investigate the detailed implementation for the three steps in our proposed GRAV-DE protocol.

4.2.2. Safe Zone Organization. In this phase, the major task is to identify all connected components with the maximum sensed intensity $I_s < I_s$. Each component will be organized as a cluster with one head, and the head node has the knowledge of the storage size of its cluster. This problem exhibits a strong resemblance to the gossip problem in [15].

Leveraging the rich set of results from the gossip protocols, we propose the following distributed algorithm for safe zone organization. At the initiation phase, each node $v_i$ with $\text{intens}(v_i) < I_s$ sets its ID $i$ as its component ID and broadcasts it to its all neighbors. Upon receiving other component IDs broadcasted by its neighbors, it will set its component ID to the minimum of its ID and all of its neighbors. Finally, the component ID of every node in the same connected subgraph will converge to a fixed ID. Algorithm 1 illustrates the safe zone organizing algorithm. The convergence and the correctness of this algorithm is omitted in this paper due to space limitation.

4.2.3. Safe-Zone/Evacuation-Path Broadcast. The next logical step is for each sensor node to obtain an evacuation path to all valid safe zones. Intuitively, this problem is equivalent to finding the set of the shortest paths from each sensor node in stressed zones to the list of safe zones. A rich set of research existed for this problem [16–18], among which the famous Dijkstra’s algorithm [19] inspires us the following distributed implementation for the evacuation-path broadcast protocol.

The protocol works as follows. After the safe-zone organizing phase is completed, the head node will broadcast an announcement message, including its unique component ID, its storage size, and hops with initial value 0, to all nodes in critical or dangerous zones. When a node receives an announcement message, it will check whether it receives
a message from the same safe zone. If yes, it will compare the value of hops in this new message with that of former messages and record the announcement message with lower value and the forwarding neighbor; otherwise, it will record the message and the forwarding neighbor. After this step, it will rebroadcast its own record of safe zones. At last, every node in danger area will have the knowledge of evacuation paths to all safe zones.

4.2.4. Evacuation Path Decision. This step addresses how each node should choose its evacuation path to one of the safe zones, by adopting a similar criterion as in the Newton’s theory of gravitation. When a node $v_i$ with $\text{intens}(v_i) > I_s$ receives announcement messages from all safe zones (for all $G_j$, $1 \leq j \leq m$), the gravitational force between one sensitive message $D_j^i$ and $G_j^i$ can be calculated using the following equation:

$$ F(D_j^i, G_j^i) = \frac{G \cdot \text{space}(G_j^i)}{(\text{dist}(v_i, G_j^i))^2}, \quad (2) $$

where $G$ is a constant called the universal gravitation constant; $\text{space}(G_j^i)$ denotes the storage size of $G_j^i$, and $\text{dist}(v_i, G_j^i)$ denotes the hops from $v_i$ to the corresponding border node of $G_j^i$. It then chooses the safe zone with maximum gravitational force as the destination for sensitive data evacuation of $v_i$. Note that there are other possible decision criteria, as long as it generates an index increasing with higher storage capacity and decreasing with longer distance. In our research, we focus on one representative criterion, derived from Newton’s law of physics, but it is not necessarily optimal.

Notice that the location of head could affect the performance of the GRAD-DE protocol significantly. For example, as illustrated in Figure 5, the sensitive data of node $A$ can choose an evacuation path from path 1 or path 2 to evacuate its sensitive data to a safe zone. If the head node is the destination of an effective evacuation path, the distances of $A$ to $G_1^i$ and $G_2^i$ are 4 and 2 hops, respectively, and our criterion indicates that the sensitive data of $A$ will be transmitted to $G_2^i$ although the mass of $G_1^i$ is 2.5 times the mass of $G_2^i$. A corrective measure we can apply is for the border nodes in a safe zone to reincarnate itself as the head one of its associated

**Algorithm 1**: Safe zone organizing algorithm.

```
(1) if (\text{intens}(v_i) < I_s) then
(2) component_id = i and broadcasts $M_i^j$ message
(3) while ($v_i$ receives $M_j^j$ from its neighbors) do
(4) if (component_id > j) then
(5) component_id = j and broadcasts $M_j^j$ message
(6) else drop $M_j^j$ message
(7) endwhile
(8) if ($i \neq \text{component_id}$) then
(9) send a join_msg to node with id = component_id
(10) else receive join_msg from all members
```

![Figure 5: The impact of the location of head.](image-url)
and put a devastating event in every small rectangle. The location of each devastating event is randomly chosen in the corresponding small rectangle. For simplicity, we presume that the intensity of the centre place of any devastating event is a real number between [0.8, 1]. For any point \( P(x, y) \) in network, the intensity of \( P \) caused can be calculated according to

\[
\text{intens}(P) = \begin{cases} 
1 - \frac{k \text{dist}}{M} & \text{dist} < M, \\
0 & \text{dist} \geq M,
\end{cases}
\]

where \( \text{dist} \) denotes the Euclidean distance between \( P \) and \( D \); \( M \) is the longer side of the small rectangles.

5.2. Impact of the Number of Sensitive Messages. We first look at the performance of our proposed algorithms, with a rising number of sensitive data messages ranging from 1 to 10, for two network topologies (100 nodes, \( 100 \times 100 \) m\(^2\) and 600 nodes, \( 300 \times 300 \) m\(^2\)). As a benchmark, we have also included a simple flooding protocol in our simulation.

Simulation results are summarized in Figure 6, which verifies our intuitions. First, we notice that the GRAV-DE protocol reaches a higher evacuation ratio, which outperforms both the GRAD-DE protocol and the flooding protocol. Specifically, the evacuation ratio for the GRAV-DE protocol is stabilized over 0.8, even in the worst case, as the number of message varies from 1 to 10. The reason
why the evacuation ratio of the GRAD-DE protocol is low is because too many messages could be forwarded to safe zones with smaller storage space. Second, the flooding algorithm has a higher evacuation ratio than the GRAD-DE protocol when the number of messages needed to be evacuated is very small. However, the evacuation ratio of the flooding approach drastically decreases and is lower than that of the GRAD-DE protocol as the number of messages increases. This observation can be traced back to two effects of the flooding algorithm. First, the chance of wireless collision is higher when flooding a lot of messages into the network; second, the storage space in safe zones will be occupied by replicated message soon. Third, as expected, the GRAV-DE protocol has a higher evacuation time than other two protocols, because it has to pay some time penalty in the two phases of safe-zone organization and evacuation-path broadcast.

5.3. Impact of the Number of Devastating Events. For simulating the different destruction degrees of disaster, we set a different number of devastating events on the network. Specifically, we randomly pick out \( n \) from \( 2 \times 3 \) small rectangles and set a devastating event into each of the \( n \) small rectangle(s), where \( 1 \leq n \leq 6 \).

From Figure 7, we see that both the GRAV-DE protocol and the GRAD-DE protocol obtain high evacuation ratio when the number of devastating events is small. As the number of devastating events increases, the evacuation ratio for the GRAD-DE protocol decreases faster than that of the GRAV-DE protocol. As a result, we argue that the GRAV-DE
5.4. Impact of Communication Radius. The network connectivity is related to the communication radius of sensor nodes. In this subsection, we characterize the performance of the GRAV-DE algorithm and the GRAD-DE algorithm under different communication radius.

As shown in Figure 8, our proposed algorithms experience different performance trends as the communication radius increases. For the GRAD-DE algorithm the evacuation ratio increase monotonically as network connectivity improves. For the GRAV-DE algorithm the evacuation ratio first increases and then decreases as the communication radius increases. The main reason is that the rising communication radius increases the chance of wireless collision at the phase of organizing safe zones, which in turn results in a partial loss of the information of safe zones. From Figure 8, the evacuation time of both of the two proposed schemes descends slightly with the larger communication radius, since the average hop number from the node under stress to safe zones decreases.

5.5. Impact of Nodes’ Survival Time. The performance of our proposed algorithm highly depends on the survival time of sensor nodes. In different types of disasters, nodes have different survival time in dangerous and critical zones. To evaluate the impact of nodes’ survival time on the data evacuation performance, we vary the lifetime of nodes in

![Figure 8: Impact of communication radius on evacuation ratio and evacuation time with different network sizes: (a) average evacuation ratio (100 × 100), (b) average evacuation time (100 × 100), (c) average evacuation ratio (300 × 300), and (d) average evacuation time (300 × 300).](image)
dangerous and critical zones from 10 s to 40 s. The results are shown in Figure 9.

When the nodes’ survival time in dangerous and critical zones is too short, a large number of data messages cannot be evacuated to safe zones timely, so that both the GRAV-DE protocol and the GRAD-DE protocol have very low evacuation ratios. With the rising survival time, the data evacuation performance of both of the two schemes clearly improves. Because the evacuation time of the GRAD-DE protocol is much shorter than that of the GRAV-DE protocol, the evacuation ratio of the GRAD-DE protocol does not go up any more after the node’s survival time reaches 25 s, whereas the evacuation ratio of the GRAV-DE protocol increases till the node’s survival time rises to 40 s. As far as the evacuation time is concerned, the longer survival time of nodes in dangerous and critical zones means the larger number of data messages needed to be evacuated. Therefore, the evacuation time of both of the two schemes gently goes up as the nodes’ survival time increases.

5.6. Blancing Raito-Time Tradeoff. As verified in Sections 5.2–5.5, the tradeoff between the evacuation ratio and the evacuation time can be balanced by judicially applying either the GRAD-DE algorithm or the GRAV-DE algorithm. The GRAD-DE algorithm outperforms the GRAV-DE algorithm in minimizing the evacuation time, while the GRAV-DE algorithm dwarfs the GRAD-DE algorithm in maximizing the evacuation ratio.
6. Conclusion

In this paper, motivated by the serious damages incurred by a few recent disasters around the globe, we have investigated on how to apply wireless sensor networks for postdisaster relief operations in a more realistic situation, where the sensor nodes could be paralyzed by the devastating events. Rather than relying on the sensor network for information gathering for a long time, we believe that a more relevant strategy would be to exploit the survival time of sensor nodes for transmitting critical information, for example, a snapshot of the affected region before the network is destroyed (similar to what blackbox preserves in flight accident), to safe zones in affected regions.

In this context, we formulate the data-evacuation problem with two competing design metrics: the evacuation ratio and the evacuation time. The former captures the amount of information rescued and the latter captures the time incurred in data rescue. Mathematically, this problem is similar to a non-linear programming problem with multiple minimums in its support. This structural parallelism inspired two alternative data-rescuing algorithms, both of which manifest some kind of principle derived by Newton. The GRAD-DE algorithm, named after its gradient-based approach, provides a superior time performance, but suffers from a throughput perspective, while the GRAV-DE algorithm, named after its resemblance to the law of gravitation, exhibits a higher throughput, but only takes much longer to rescue critical data. Our numerical study verifies the tradeoff between these two metrics. It is the field engineers’ responsibility to judicially apply either algorithm in a realistic situation to rescue lives and/or control damages.

For future research, a direct extension of this work would be to compare different criteria to decide which evacuation paths to take. Another possible topic would be to make it possible to multiply evacuation paths for each sensor node and evaluate the associated tradeoff between the evacuation time and the evacuation ratio.

Acknowledgments

This work is supported by National Science Foundation under Grant numbers 61170256, 61103226, 60903158, 61173172, 61003229, and 61103227 and the Fundamental Research Funds for the Central Universities under Grant number ZYGX2010J074.

References
