A Wireless Sensor, AdHoc and Delay Tolerant Network System for Disaster Response

H. Chenji, A. Hassanzadeh, M. Won, Y. Li†, W. Zhang, X. Yang, R. Stoleru, G. Zhou†
Department of Computer Science and Engineering, Texas A&M University
†Department of Computer Science, College of William and Mary

Abstract

This paper presents AnonymousNet (AnonNet), a system for emergency response in large scale disaster areas, e.g., earthquake and tsunami in Japan (2011) and earthquake in Haiti (2010). Despite the attention the "emergency response" application area has received, we still lack data at the high spatial and temporal resolution needed to save lives, and to support disaster recovery efforts. Disaster victims are rescued after days, if not weeks; victims' physiological information is not delivered reliably on time; good coordination among responders is lacking, or it is based on archaic methods (pencil, paper, paint on walls); the delay in receiving vast amounts of information is bounded by the time used to physically transport tapes or hard drives; and no sensing/communication system built and deployed lasts more than a few days. AnonNet, designed in collaboration with US&R responders, is a first step to address these challenges. It is designed to aid in identifying victims under collapsed buildings, deliver victims' physiological information on time, deliver high volumes of field data at high throughput and in an energy efficient manner, and integrates new social networking paradigms. AnonNet is a large academic effort, proposing open systems, instead of proprietary solutions. AnonNet and its subsystems are evaluated in real deployments and simulations.

1 Introduction

Disasters, natural or man made, are unexpected events that cause significant distress and havoc on a global scale. The best that can be done in the face of such uncontrollable acts of nature is speedy and effective recovery. Recent disasters in Japan and Haiti [1, 2] have shown the effect that they can have on people, property, and the economy. Repercussions include, but are not limited to shortage of electric power, food, potable water, protection from the elements of nuclear and/or chemical hazards. In such situations, disaster response becomes increasingly difficult and constrained.

Several countries have set up governmental agencies to deal with such disasters, such as the Urban Search & Rescue (US&R), an agency part of FEMA [3] in US. Several Task Forces comprising of trained personnel and specialized equipment have been deployed by FEMA in the event of such disasters. From our collaborations with US&R responders, we are keenly aware of the 66 tons of equipment emergency responders maintain in their cache. While this equipment has been tried and tested in the field, there are numerous examples in which new technologies like deeply embedded sensors, adhoc and delay tolerant networking, energy efficient communication, high capacity storage devices and social networking can make a significant impact. Some of these technologies have not been considered robust enough unless deployed by a military/government contractor until recently, when the US Army announced that it plans to adopt commercially available hardware (e.g., iPhones) for combat [4].

Preliminary goals (requirements) for AnonNet, obtained in consultation with US&R responders are to enable the discovery of victims under the rubble of collapsed buildings in a timely manner (unlike several days in Japan), to deliver physiological data from victims to specialized personnel in an energy efficient manner and ontime (unlike in Haiti), to enable responders with access to services in the cloud, over a delay tolerant network, to deliver large amounts of data from field, to the Command & Control Center (C2), in an energy efficient manner so that AnonNet can operate entirely off batteries for 10-14 days. AnonNet's sensing is focused on collapsed buildings and emergency responders. AnonNet's networking is focused on energy efficient and reliable delivery of large amounts of data over a multitude of networking technologies, including victims' physiological data.

We propose AnonNet, a second generation wireless sensor, adhoc and delay tolerant network system for disaster response. Thousands of sensor networks, equipped with vibration and acoustic sensors, are deployed over all collapsed buildings, continuously monitoring them for potential survivors under the rubble. Buildings surveyed by US&R responders are digitally tagged, allowing for fast, reliable and inexpensive high resolution data collection and situational awareness. Teams of responders are equipped with mobile computing devices, warning the team members when they dangerously separate from their team, and providing the team members access to services in the cloud. Data and generated events in the field are relayed over an open standard delay tolerant network to the Command and Control (C2). Strategically placed data waypoints allow for high throughput, energy efficient delivery of massive amounts of data. The entire AnonNet runs on batteries, as US&R emergency responders learned is necessary, during Hurricane Katrina. More precisely, the contributions of our paper are as follows:

- To the best of our knowledge, we present the first design and implementation of a complex system (i.e., sensing, networking, data management) for emergency response that addresses US&R responder requirements and is evaluated in a realistic environment.
- Development of sensing modality that allows continu-

ous monitoring of a large number of collapsed buildings for survivors, in stark contrast with today's state of art, requiring responders to be physically present in the field, and requiring no noisy activity, interfering with their acoustic monitoring.

- Development of networking analysis for energy efficient delivery of physiological data, with soft real-time guarantees, over heterogeneous wireless networks.
- High throughput data dissemination and energy efficient management of data, communicated over heterogeneous networks involving delay tolerant, WiFi, mesh, 802.15.4 technologies.

2 Motivating Scenario and State of Art

Our motivating scenario is a large scale disaster (e.g., entire cities/regions are affected) and not a local, block-wide emergency in a city or a town. Unfortunately, recent history gives a few motivating examples, e.g., the earthquake and tsunami in Japan [1], and the earthquake in Haiti [2]. In these incidents, the communication infrastructure is disrupted (i.e., cellular networks are completely or partially damaged, satellite networks are overloaded) for weeks if not months, there are serious shortages of power (i.e., local power utilities - nuclear reactor, are damaged), surveying the disaster area for survivors under the rubble takes from days to weeks (with some inspiring examples of survivors emerging after tens of days), large areas are set up for triage of victims, the C2 is flooded with sensing and multimedia data from the field. This febrile, fast pace environment lasts from one to several weeks, until the infrastructure is being repaired.

2.1 State of Art

A mandated and standardized equipment list for FEMA US&R teams is available online [5]. Each task force maintains its own cache, containing over 16,000 items. The technical equipment details Project 25 (P25) [6] compatible 2 way portable wireless radios. A 120V AC powered base station is also mentioned, along with battery powered repeaters. Such radio systems have a large radio range capable of covering large areas and are securely encrypted. However, only voice and data channels are available on such systems at very low data rates of 9.6kbps [7]. Since the P25 systems defines a physical as well as a MAC layer, it is difficult to integrate protocols meant for low power wireless like 802.15.4 (henceforth referred to as 15.4). Although reliable real time long range secure communication systems like Project 25 exist, they have several caveats like cost, difficult integration with other systems, high power requirements, physical bulk.

Seismic sensing has been used alongside WSNs to predict volcano activity [8], perform intrusion detection based on footstep detection [9, 10] and heritage building monitoring [11]. In [12], seismic data is analyzed both in the time and frequency domain. A method to differentiate walking footsteps from running is also presented, based on the Fourier Transform technique. Techniques involving the sampling and processing of seismic data are the focus of research in home intrusion detection systems and military area monitoring.

The Wireless Internet Information System for Medical Response in Disasters (WIISARD) [13, 14] is a 802.11 based wireless mesh network (WMN) tailored to provide effective medical response in the event of a disaster. Mobile clients like PDAs and laptops roam around the geographical area while being connected to the Internet via multiple backhaul connections [15]. Digital tags on patients [16] are read by medical personnel using PDAs. Changes to such digital records are tracked and can be easily rolled back in case of conflict due to multiple simultaneous editing. It is to be noted that network connectivity is assumed to be persistent and highly available.

Body sensor networks (BSN) are used for timely, reliable reporting of physiological and behavioral information of victims in a disaster. Throughput and time delay performance assurance is needed over heterogeneous sensing and communication hardware and software platforms. In [17], the authors propose or extend specific MAC protocols and radio platforms for providing statistical throughput and/or time delay performance assurance. [18] presents adaptive and radio-agnostic QoS solutions for BSN but do not consider joint throughput and time delay performance assurance. [19] guarantees different throughputs but only a single time delay bound for different BSN data streams. This solution is also based on a costly individual polling scheme, with 50+% overhead, rather than a more effective group polling scheme [18] [20]. Although [20] provides both throughput and time delay performance assurance, it neglects the analysis of energy consumption in a two hop setup where sensor data is aggregated over 15.4 by a battery powered device like a cellphone and is delivered to the cloud over 802.11. We propose a model of two-hop data transmission and analyze energy consumption minimization opportunities, by reducing the packet size.

We draw upon a large body of research experiences in the field of delay tolerant networking (DTN). [21] advocates the use of DTN to provide situational awareness in a disaster. The proposed system provides elementary social networking by helping victims disseminate information while not overwhelming the system. Dieselnet and the DOME testbed [22] provide rich information about implementing routing protocols, providing services and a public DTN testbed using WiFi devices mounted on buses covering a large area. In [23], data is collected from sensors deployed in a wildlife tracking environment leveraging the frequent movement of zoologists and scientists in the area.

Project RESCUE [24] provides an overview of a WMN for effective emergency response. [25, 26] argues for a WMN to be used in disaster response. It cites several shortcomings in several real use cases which provide a baseline comparison to such systems. In [27], a hybrid WMN makes use of wireless WANs as a backhaul link to access traditional networks. Several portable networked devices make use of routers affixed to lamp posts in order to achieve network connectivity. The SAFIRE project [28] deals with situational awareness for firefighters. Among the many problems dealt with are reliable data dissemination over adhoc networks. Responders use a WiFi enabled tablet which uses a central push-pull method of data movement. The intended purpose is for use in a local emergency, and not a region wide dis-

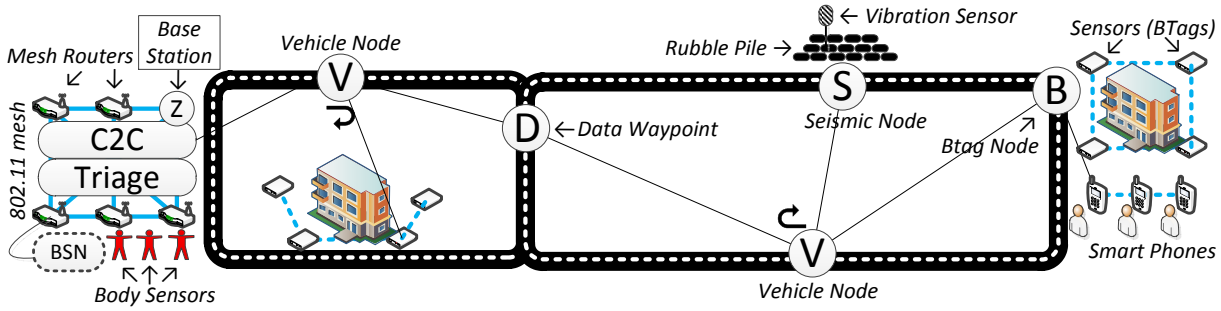


Figure 1. AnonNet architecture

aster. [29] has commercial offerings which accomplish network centric warfare. Based on the limited details available, the system offers robust middleware based on 802.11 and/or WiMax based networking. To the best of our knowledge, these systems assume an AC powered connected network and do not offer integration of low power smart devices.

The problem of intelligent placement of relays to improve the performance of mobile DTNs have been studied [30, 31, 32, 33]. [30] presents a scheme to deploy relays, called throwboxes, in mobile DTNs to maximize data rate between mobile nodes. [32] studies the hardware architecture for such relay nodes in an attempt to increase the lifetime. In [33], analysis on the performance of different relay strategies is presented. [31] later considers other types of infrastructures such as mesh networks and provide cost-performance trade-offs. In this paper, we deal with a slightly different problem where instead of maximizing the data rate between mobile nodes, we focus on optimizing the throughput of data delivered to the C2. This objective is based on an observation that no matter how high a data rate a mobile node has, limited vehicle movement bounds the possible throughput, and hence, the amount of unique data passed to a vehicle has to be maximized.

Sink election is an important primitive in AnonNet. Most of the early research in this area propose single sink solutions for wireless sensor networks. Such solutions assume that sink is always fixed and concentrate on delay and energy consumption [34]. However, for our large scale application domain, this imposes drastic data latency and power consumption requirements. On the other hand, the position of sinks must be changed depending on the traffic pattern. In [35], sink repositioning is proposed to maximize the network life time. Other recent research like [36], finds optimal positions for the sinks in large scale sensor networks.

3 AnonNet Architecture

The AnonNet architecture is shown in Figure 1. Broadly, there are four classes of devices:

Monitoring/Sensing These are typically comprised of low power sensors, or sensors provided by third parties. The data sensed may be either time critical or informational. Being heavily duty cycled, they are designed to last for several weeks with a single charge. 802.11 support is rarely found on these devices, with 15.4 or no networking being more common.

End User Interactive Devices Smartphones and popular network centric consumer electronics like tablet PCs which have networking capabilities. These provide a rich interface to the data collected in the field, while also providing some functionality themselves. Not as resource constrained as the sensors to warrant 15.4, most devices have 802.11 capability and are designed to last a few days on a single charge.

Network Backbone Non-interactive devices which provide basic networking functionality and are deployed in the field. An example is a common 802.11 router found in most homes today. They can be assumed to have expansion ports to provide additional functionality like persistent storage or cellular connectivity. They consume a little more power and need to be powered by batteries, but are still portable. These can either be static or deployed inside a vehicle. In AnonNet, these devices are the only ones implementing delay tolerant capabilities and act as a middleman between sensed data and C2.

Fixed Mesh Technically a subset of the network backbone, the fixed mesh comprises a C2 as well as the surrounding geographical area to a small extent. This region typically has a medical triage area as well as internet connectivity through terrestrial networks. Electric power usually comes from diesel generators and can be used to power routers and servers.

Table 1. AnonNet Components

Component	Software Class	Hardware Class
BTag	Sensor w/ UDP	Monitoring
Seismic Sensor	Sensor w/ UDP	Sensing
Body Sensor	Sensor w/ TinyOS AM	Sensing
Smartphone	Smartphone	End User Device
Vehicle Node	DTN Router, w/ 15.4	Network Backbone
Data Waypoint	DTN Router, w/o 15.4	Network Backbone
Seismic Node	DTN Router, w/ 15.4	Network Backbone
BTag Node	DTN Router, w/ 15.4	Network Backbone
Mesh Router	Mesh Router	Fixed Mesh
Base Station	DTN/Mesh Router, w/o 15.4	Network Backbone, Fixed Mesh
Extenders	Mesh Router w/ IBSS	Network Backbone

An explicit list of AnonNet components is shown in Table 1. BTag, which stands for BuildingTag is a 15.4 based monitoring device which is intended to be attached to buildings externally. A BTag can have a dedicated BTag Node which aggregates multiple buildings, or it can do the aggre-

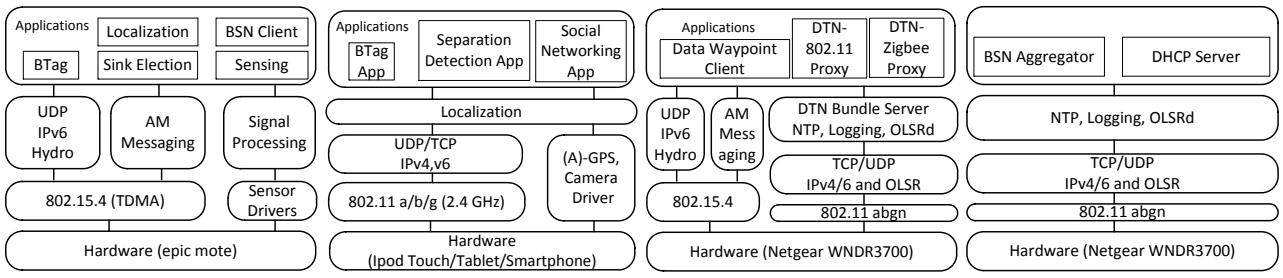


Figure 2. AnonNet software architecture of (a) sensors; (b) mobile computing devices; (c) DTN router; (d) mesh router.

gation itself. In the latter case, they upload their data to Vehicle Nodes in their vicinity. Smartphones can be used to get and set BTags via any router with a 15.4 interface. Seismic Sensors are an example of a third party IP-incapable device. IP capable motes query the seismic sensor and transmit the data to a nearby Seismic Node. Body Sensors are 15.4 devices which sense physiological data and send it to a 802.11 capable aggregator, which is typically a smartphone.

Vehicle Nodes, BTag Nodes, Seismic Nodes and Data Waypoints are battery powered DTN capable routers. Only the Data Waypoint does not have a 15.4 interface since it instead has a large persistent data store. Upon receiving data from sensors, these routers convey the data in a DTN capable format to the Base Station. The Base Station is a special router that has both DTN as well as mesh capabilities. All data in the field is aggregated at the Base Station.

An Extender is a special kind of router that is cheaper, energy efficient due to duty cycling, has fewer capabilities (802.11bg only as opposed to 802.11abgn "bang" routers) including limited storage and computation). They are meant purely for extending the service range of DTN routers in the field. A typical use case would be that of a team of S&R personnel wishing to deploy a BSN in a location that is not within range of the nearest DTN router. In such cases, these simple Extenders can act as a proxy between the BSN and the DTN router using 802.11 networking.

3.1 Software Architecture

Devices in AnonNet fall into four broad device categories of sensors, smartphones, DTN routers and mesh routers as shown in Figure 2.

3.1.1 Sensing & Applications

Applications are deployed on end user devices as apps (various apps in Figure 2(b)) and on the sensors in AnonNet (sensing, sink election in Figure 2(a)). All the applications can either use their own data format or use a public schema as the network is payload agnostic. In case they need to use DTN capabilities, they have to use a DTN proxy within range. A reverse proxy (which is also a DTN app) at the destination converts the DTN format to an application native format. In this way, third party applications can be easily integrated since (reverse) proxy servers can be configured with a predetermined port number assigned in the system to a particular application.

In case the third party application does not support IP or networking, there are several choices: it can proxy the data via a mote running IP using on board interfaces like a serial port, or it can connect directly to the router itself via USB or any available interface.

3.1.2 Networking & Data Management

The network architecture spans multiple protocols at all layers of the network stack. The dominant stack used is 802.11abgn in IBSS mode below IP/UDP (Figures 2(c) 2(d), and 2(b)). Since sensors use 802.15.4, an edge router or a gateway is needed before the data can reach traditional networks. This conversion happens in the Network Backbone hardware class of devices where 802.15.4 capable routers (Figure 2(c)) act as a proxy between sensors and 802.11 devices. Smartphones which are 802.11 capable can communicate with each other in IBSS mode and also with 802.15.4 devices via proxies. 15.4 devices need not have an IP based stack, but a compatible interface needs to be available on the corresponding router.

DTN is implemented as an overlay network in the application layer solely on DTN routers (Bundle server in Figure 2(c)). Each DTN compliant device has a local server to whom DTN "apps" (Data Waypoint client in Figure 2(c)) can attach via a local API. In AnonNet, these apps can act as proxies and present a DTN interface to smartphones ("DTN IP Proxy" in Figure 2(c)) and 802.15.4 devices ("DTN 802.15.4 Proxy" in Figure 2(c)). When such devices request data to be sent over DTN, the proxy enqueues the data in the local server queue. When a suitable neighbor is found in the future, either directly or via delay tolerant routing, the data is sent.

The fixed mesh operates as a regular WMN. The routers forming this network are not DTN capable (except the Base Station). Services provided by these devices include DHCP ("DHCP Server" in Figure 2(d)) and BSN aggregator capabilities which aggregates data from BSN clients on motes.

4 AnonNet Sensing and Apps Design

4.1 Building Sensing Networks

The FEMA US&R equipment cache list [5] mentions Delsar Life Detection sensors. These sensors are used by responders to probe a rubble pile for victims and/or signs of life. A steel spike is driven into rubble or a magnetic box attaches the sensor to metallic rubble. Responders can then monitor the pile for human voices or vibrations caused by victims knocking on surrounding objects. Based on the strength of these vibrations, the responder can know how deep or shallow the victim is within the pile. Upon taking

multiple measurements at different places, the victim can be localized and rescue operations can commence. These Life Detectors have been incorporated into AnonNet. Since they do not have any native networking capabilities, EPIC motes are used to provide an interface. The onboard ADC samples the seismic sensor, which is then processed to yield useful data.

A victim trapped under a rubble pile may attempt to knock or pound on walls or use small objects like stones to do the same. These events need to be detected effectively. However, there are sources of noise in a disaster area which are also picked up by the seismic sensor. Common sources of noise include footsteps and vibration caused by moving vehicles. To garner knowledge of these different types of data and their intrinsic properties, we gathered a few samples using these motes outdoors. The steel spike of the sensor was driven into a small wedge in a pavement outside our building on campus. Three sources of data were profiled: a stone drop from a height, footsteps of pedestrians and a knock made by a hammer on a pavement. After sampling the vibration caused by these events using the mote, fixed-point in-place 1024-bin FFT was performed. This knowledge of the spectrum is essential for classifying these events as shown below. The eventual goal of using classification is to separate useful data like a knock made by a victim from a source of noise like footsteps caused by movement in the area with high accuracy.

Both the raw signal and the FFT data for one sample of each type of event is shown in Figure 3. A stone when dropped from a height tends to bounce and create vibrations once more - this is why we see multiple activity in Figure 3(a)(top). It is important to note that amplitude alone cannot be used to classify a signal; the same stone dropped from a different height on the same point causes a signal with different (which is not shown here for compactness). Two features which best represent the data numerically were chosen: (i) average value of the frequencies weighted by their respective amplitudes and (ii) the mean amplitude of the frequencies. In Figure 3(d) we can see how these simple features cause the data to fall into different clusters.

We then design a simple feature based KNN (k-nearest neighbor) classifier to differentiate between the types of data. This choice is motivated by the fact that classification has to be done on a Seismic Node which is a battery powered router and hence resource constrained. Suppose that we have g different types of data $G_1 \ldots G_g$. For each group, we have n samples which makes for a total of gn samples $s_1 \ldots s_{gn}$. Let each sample be a vector consisting of (for simplicity), two features $[f_1, f_2]$. The KNN classifier first needs to be trained using these samples. Training consists of storing each sample and its corresponding group in memory. Now, given a new sample $S = [F_1 F_2]$ that needs to be classified, Algorithm 1 explains the working of a Euclidean distance based, k nearest neighbor classifier which calculates the group G that S belongs to.

4.1.1 *Building Tags*

Building Tags are low power devices which manage metadata related to a building from a search and rescue viewpoint. Data includes but are not limited to the last date/time it

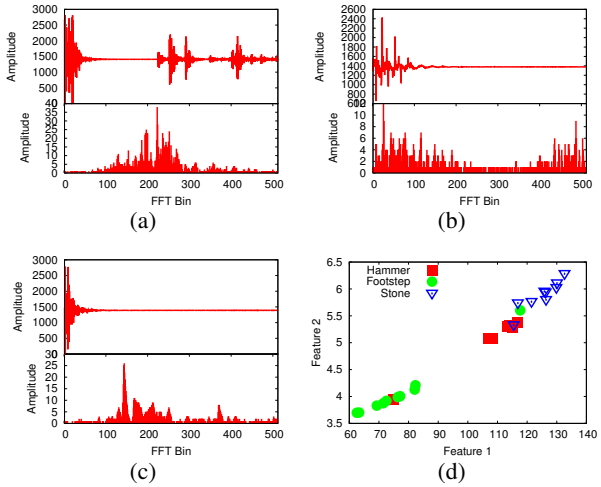


Figure 3. Spectrum and signal of (a) stone drop (b) footstep (c) hammer strike. (d) shows the classifier results based on 2 features

Algorithm 1 k-NN Classifier

1: **for** each $s_i \in s_1 \ldots s_{gn}$ **do**
2: Compute $d_i \leftarrow \sqrt{(F_1 - s_i^{f_1})^2 + (F_2 - s_i^{f_2})^2}$
3: **end for**
4: $r_1 \ldots r_k \leftarrow$ The k smallest d_i
5: *groups* $\leftarrow$ Union of groups that each of $r_1 \ldots r_k$ belong to
6: $G \leftarrow$ most common group in *groups*

was searched for survivors, any possible hazards inside and the number of survivors present. This data is most likely to remain constant and not change very often. For the purposes of saving energy and choosing an aggregator who is most likely to encounter a vehicle node, these tags perform sink election. Such aggregation by a sink ensures that nodes which may not have a LoS to a nearby road can still communicate its data to the base station efficiently. These tags are first programmed by search and rescue personnel once the search is complete, by using the "BTag App" (Figure 2(b)).

4.2 US&R Team Separation Detection App

US&R operations in an unexplored large area with low visibility and potential hazards (e.g., collapsed tunnel, chemicals) is dangerous. Members of a S&R team need to ensure that they are within a safe range from the team leader. To meet this need, we develop an iOS application that enables each team member to monitor the connectivity to a team leader in real time using an iPod Touch, which then warns a team member of impending physical separation from the team leader, using audio-visual means. The design of the algorithm and the app saves energy by exchanging messages only with its immediate neighbors instead of multi-hop communications, eliminating the need for the implementation of routing protocols.

This app is inspired by the distributed cut detection algorithms [37] which enables each node to autonomously determine the connectivity to a specially designated node called the "source node", say v_1, in the network. In these algo-

rithms, each node v_i maintains a positive scalar $s(v_i)$ called the "state". This value is updated at a regular interval by averaging the scalars $s(v_j)$ of immediate neighbors $v_j \in N_i$, where N_i is the set of immediate neighbors of node v_i. Formally, the state in the next iteration of the algorithm is computed as the following: $s(v_i) = \sum_{v_j \in N_i} \frac{s(v_j)}{|N_i|+1}$. In particular, the source node "injects" a positive constant s' at each iteration of the algorithm. Specifically, the next state of the source node is computed as the following: $s(v_1) = \sum_{v_j \in N_1} \frac{s(v_j)+s'}{|N_1|+1}$. Consequently, if a node is connected to the source node, its state converges to some positive value. On the other hand, if a node is disconnected from the source node, its state rapidly converges to 0, signaling a cut. The nodes that are still connected to the source node detect a cut by observing a sudden change in the converged value.

In our app, a team leader becomes the source node by selecting the appropriate option using the touchscreen based interface (screenshot not shown for brevity). This app is not limited to the separation detection among the team members: a compatible IBSS capable device attached to expensive hardware also runs the cut detection algorithm, allowing team members to make sure that hardware is not lost. Simultaneous monitoring of multiple source nodes is supported. Unlike existing solutions that focus only on the "binary problem" (i.e., is there a cut or not?), each member can keep track of connectivity to multiple team leaders. This feature is useful when a team needs to be separated into sub-teams, and team members need to know the connectivity to each subteam leader. We implement this by maintaining an array of states, each representing the connectivity to corresponding leader. Each state of the array is updated by using the same state update rule at a regular interval. The set of states are then encoded in a single packet and broadcast to immediate neighbors. In essence, the support for multiple source nodes is based on overlaying multiple executions of cut detection process for each source node while not increasing the communication overhead.

5 AnonNet Networking Design

A 802.11 wireless network is the fundamental networking primitive in AnonNet and is present both in the fixed mesh component as well as the field routers. The WNDR3700 routers used have two wireless interfaces which provide 802.11an on the 5GHz band as well as 802.11abgn on the 2.4GHz band. Since most COTS WiFi compliant devices support only the 2.4GHz band, we decided to use the 5GHz interface exclusively for implementing a mesh backbone between routers and providing related services. This interface always operates in 802.11 IBSS mode to facilitate easy neighbor discovery. In the fixed mesh component, the 2.4GHz interface broadcasts a WPA encrypted network in infrastructure mode, whereas an IBSS mode network is broadcast in the field. This is because the iPods are placed in IBSS mode since they need to communicate with each other with or without a router nearby, and there is no facility to make them act as a station in infrastructure mode.

Services which are provided on the 5GHz interface are primarily those which are not needed by end user devices, like the DTN service (neighbor discovery and the actual transfer of bundles) and routing. DHCP is provided on 2.4GHz interface. All routers have statically assigned IPs - router n has an IP of 192.168.50.n for its 5GHz interface and 192.168.n.1 for the 2.4GHz interface. Each router can handle 255 end user devices - they are assigned IPs in the 192.168.n.0/24 range.

Energy Efficiency through duty cycling In our power-constrained application domain, we consider energy efficiency as an important issue. A common method is duty-cycling, which saves more power while keeping network availability and performance at an acceptable level. However, duty cycling COTS wireless routers is unsupported and highly hardware and driver dependent. Consequently, we propose to use a simple application layer duty-cycling scheme as a first approximation. Based on our experience with Linksys WRT54GL wireless routers running OpenWRT, turning the radio on and off using the *iwconfig* tool reduces the current drawn by 70mA, while not allowing the established IP layer connections to time out. We use this scheme to save power on Extenders (Table 1) which are essentially WRT54GL routers.

5.1 Routing

Mesh Routing OLSR (RFC 3626) provides mesh routing services in AnonNet. It is implemented on all routers - both in the fixed mesh component as well as the network backbone component. Using the HNA feature, the local subnet of 192.168.n.0/24 is advertised, thus allowing every device in the network to talk to all other devices. To illustrate this, a few hypothetical routes on router #10 are provided below. The link quality algorithm was "etx_ff", which is an ETX ($= \frac{1}{LQ*NLQ}$) based algorithm that includes a hysteresis mechanism to guard against fluctuations in link quality metrics LQ (Link Quality) and NLQ (Neighbor Link Quality). Hysteresis was disabled since the contact times of 2 DTN nodes in the field is quite less and can cause problems. The HELLO/TC/MID/HNA intervals were set to 5s,5s,18s,18s respectively.

192.168.50.4	192.168.50.10	$wlan1(5GHz)$
192.168.4.0/24	192.168.50.4	$wlan1(5GHz)$
192.168.10.0/24	192.168.10.1	$wlan0(2.4GHz)$

Note that an end user device connected to this router with IP 192.168.10.24 can talk to its counterpart 192.168.4.25 at router #4 via 192.168.10.1 $\rightarrow$ 192.168.50.10 $\rightarrow$ 192.168.50.4 $\rightarrow$ 192.168.4.1.

DTN Routing There are several routing protocols specifically designed for delay tolerant networks. Node encounters can be categorized into scheduled and opportunistic encounters. Since scheduled encounters are not very common in AnonNet, we choose to model DTN routing based on opportunistic encounters. Epidemic routing is a simple scheme where a copy of each pending bundle is transferred to every new node encountered. Prophet routing aims to select only those nodes which have a high probability of encountering the destination. These protocols are implemented within the DTN server itself as a module in user space. Simulations

were conducted in order to determine the most suitable routing protocol (Sec. 7).

End User Devices COTS smartphones in general do not allow applications (developed using the offered SDK) to insert routes into the kernel for security reasons. Because of this limitation, the smartphones used in AnonNet were restricted to one hop communication. Data was sent over multicast when a suitable router was within range. The IP proxy present on the router then encapsulated the data in a bundle and transmitted it via DTN to the base station.

Motes For UDP/IP based sensor devices, the stable version of the Blip stack based on TinyOS was used. The default routing protocol available, Hydro, was used for multihop communication.

5.2 Delay Tolerant Networks

A comprehensive description of motivating factors for a new delay tolerant architecture can be found in [38] and RFC 4838 [39]. Interoperability between devices with heterogeneous capabilities and functionality is important. Specialized low power devices should be able to seamlessly integrate with other classes of devices, different network stacks notwithstanding. Since there may exist different types of data with different priorities and useful lifetimes, programmatic support for prioritizing data and specifying lifetimes is essential. Nodes may have a combination of many characteristics like low energy resources and limited storage capacity. In the event that such nodes find that their resource requirements hamper functionality, the node needs to be able to delegate the responsibility of ensuring data flow to another suitable node in the network.

With the above motivation, the Bundle protocol is presented in [40]. The primary data unit is called a "bundle". Application layer implementation ensures network abstraction. The actual implementation of a DTN gateway will need to have support for "convergence layers" which are essentially interfaces to one or more network interfaces present. The custody transfer feature ensures that node can delegate responsibility to another node. Acknowledgements can be requested either on a per-hop or on an end-to-end basis.

Each DTN node is identified by a special scheme-specific URI like $dtn://dn.zigbeegateway1$. Applications which connect via the API need to provide an ID like $mote1$. Thus, any traffic intended for this application will need the destination field to be set to $dtn://dn.zigbeegateway1/mote1$. Traffic intended for all applications at a node can use the URI $dtn://dn.zigbeegateway1/*$, for example.

5.2.1 Bundle protocol

The proposed Bundle protocol [40] can be seen as a protocol which implements features outlined above. The primary data unit (PDU) of this protocol is called a bundle. Different headers and flags are defined by the RFC which enable features like custody transfer and forwarding. A "Bundle Protocol Agent (BPA)" provides bundle services via a service interface/API. "Application Agents (AA)" connect to a BPA in order to utilize bundle services. Note that the method of access is not specified - this is how protocol stack transparency is effected.

Custody Transfer This is of importance in mobile adhoc networks. If ACKing of successful bundle delivery is requested, a lot of network overhead is generated as the sending node moves further away from the destination or is disconnected. For this purpose, highly mobile nodes can transfer custody of bundles (originated or relayed) to certain special nodes with large storage capacity (data waypoints in AnonNet). These nodes then take responsibility for delivering a bundle to its destination.

5.3 Body Sensor Networks

Power efficient sensors placed on victims' bodies in a medical triage area provide a reliable, low cost victim status monitoring solution in the event of a large disaster. In a BSN, multiple simple sensors like body temperature sensors, blood pressure sensors, and EKG sensors are attached to a victim's body. The readings are transmitted to an aggregator (a cell phone in our case) that can be put in a victim's pocket. The aggregator consolidates and delivers this data using 802.11 facilities in the Fixed Mesh to the intended destination which can be a medical cloud service. The victim's status can be monitored by a doctor in real-time through the cloud, and treatment or surgery can be performed by a robot. In this section, we investigate energy minimization in such scenarios while at the same time providing the required throughput and latency performance assurance.

Definitions and Models Consider a two-hop packet transmission communication system based on the bulk preferred TDMA in the first hop and CSMA in the second. Consider N simple sensors and a more powerful aggregator in the first hop, while the second consists of the aggregator and an Access Point (AP) belonging to the Fixed Mesh. Concretely, the aggregator delivers data from the sensors to the AP while contending with $M-1$ potential contenders over CSMA. Both sensors and aggregator are battery powered and energy constrained. We first develop analytical models for the energy consumption when communicating over two hops, and finally minimize the overall energy consumption. The notations we use are in Table 2.

Energy Analysis in the First Hop In the first hop, N sensors with their priorities try to transmit data to the aggregator using TDMA. The priority is used to schedule the access of each sensor to the aggregator. For a standard packet transmission from a sensor to an aggregator, the aggregator first polls the sensor who then attempts to transmit. Since the transmission/reception of a polling message consumes much less energy than transmission/reception of data, we neglect polling energy consumption. Assume that all sensors generate data at an effective rate of b bps, and send it using equal sized packets composed of header and data, of sizes of S_{h1} and S_{d1}, respectively. Further, due to wireless phenomenon, the probability of a successful transmission from all sensors to the aggregator is p_1.

The total energy consumed by N sensors, generating data at b bps for transmitting packets, under consideration of retransmissions over the time period t is formulated as $E_{11} = \rho_{st} t_1 (Nbt)/(S_{d1} p_1)$, where ρ_{st} denotes the transmission power consumed by one sensor, $t_1 = (S_{h1} + S_{d1})/\theta_1$ specifies the average time period for a transmission attempt, N indicates the number of sensors and $1/p_1$ is the ex-

Table 2. Notations

N	Number of sensors in the first hop
M	Number of contenders in the second hop
t	Time period for test in the model
t_1	Average time period for a transmission attempt in the first hop
t_{2t}	Average time period for a successful transmission without backoff in the second hop
t_{2i}	Average idle time period of one packet transmission in the second hop
p_1	Possibility of a successful transmission from a sensor
p_2	Possibility of a successful transmission from an aggregator
b	Data generation rate of a sensor
S_{h1}	Bit size of a packet header in the first hop
S_{d1}	Bit size of effective data of a packet in the first hop
S_{h2}	Bit size of a packet header in the second hop
S_{d2}	Bit size of effective data of a packet in the second hop
ρ_{st}	Transmission power consumed by a sensor
ρ_{at}	Transmission power consumed by an aggregator
ρ_{ar}	Receiving power consumed by an aggregator
ρ_{ai}	Idle power consumed by an aggregator
CW	Size of the backoff window
R	Maximum number of backoff retries
θ_1	Throughput capacity of the first hop
θ_2	Throughput capacity of the second hop
D	the whole delay of packets transmission from sensors to AP

pected number of retransmissions needed for a successful delivery. The energy consumed by the aggregator for receiving all packets from N sensors with consideration of retransmissions over a time length of t is formulated as $E_{12} = \rho_{ar} t_1 (Nbt)/(S_{d1} p_1)$, where ρ_{ar} indicates power consumed by the aggregator that receives packets. Therefore, the average power consumed under possible retransmissions in the first hop is expressed as $E_1 = E_{11} + E_{12} = (\rho_{st} + \rho_{ar}) t_1 Nbt/(S_{d1} p_1)$.

Energy Analysis in the Second Hop In the second hop, one aggregator with other $M-1$ potential contenders attempts to transmit packets to the AP using CSMA. All contenders deliver the same size packets, each of which is also composed of header and data, with bit sizes of S_{h2} and S_{d2}, respectively. The packet transmission bandwidth provided by the aggregator is Nb bps, which means the aggregator delivers packets with the same transmission rate to that of all sensors. Using CSMA, the aggregator having a packet to transmit senses the medium. If the channel is idle, it transmits the packet immediately, else it randomly selects a time from [0, CW] as a backoff time counter before transmitting, where CW denotes the backoff window size, composed of time slots with each $t_{sl} = 20\mu s$. The backoff time counter is decremented as long as the channel is sensed idle, is stopped when a transmission is detected on the channel, and reactivated when the channel is sensed idle again. It sends packets with a probability of p_2 when the backoff time reaches 0 if the channel is clear, otherwise it backsoff again. If we assume that all collisions are eliminated, the average backoff time of each packet can be approximated by $CWt_{sl}/2 \cdot min\{(M-1)/2, R\}$ (i.e., idle time), where R is the maximum number of backoff retries.

We calculate the energy consumption of the aggregator for successfully transmitting the whole effective data Nbt from N sensors under consideration of retransmissions in the second hop over the same time period t is described as $E_{2t} = \rho_{at} t_{2t} (Nbt)/(S_{d2} p_2)$, where ρ_{at} indicates the transmission energy consumption by the aggregator, $t_{2t} = (S_{h2} + S_{d2})/\theta_2$ specifies the average time period for a successful transmission without backoff in the second hop and $1/p_2$ denotes the expected number of retransmissions needed for a successful delivery.

The energy consumed by the aggregator during the idle period is formulated as $E_{2i} = \rho_{ai} t_{2i} (Nbt)/(S_{d2} p_2)$, where ρ_{ai} shows the energy consumption when the aggregator is idle due to carrier sensing and $t_{2i} = CW \cdot t_{sl}/2 \cdot min\{(M-1)/2, R\}$ specifies the average backoff time period of one packet transmission. Therefore, the average power consumed by one aggregator with states of transmission and idling in the second hop is expressed as $E_2 = E_{2t} + E_{2i} = (\rho_{at} t_{2t} + \rho_{ai} t_{2i})(Nbt)/(S_{d2} p_2)$.

Energy Consumption Minimization As assumed in the previous sections, we address the problem of how to choose the size of S_{d1} and S_{d2} over a time period of t, so that the total energy consumption of N sensors and one aggregator in the model can be minimized in this paper. Therefore, the minimization problem of energy consumption can be formulated as:

$$\text{minimize} \quad E_1 + E_2 \tag{1}$$

$$\text{subject to:} \quad Nb(S_{d1} + S_{h1})/(S_{d1} p_1) \le \theta_1 \tag{2}$$

$$Nb(S_{d2} + S_{h2})/(S_{d2} p_2) \le \theta_2 \tag{3}$$

$$S_{d1}/b + t_1/p_1 + (t_{2t} + t_{2i})/p_2 + \\ + S_{d1}/(Nb)(S_{d2}/S_{d1} - 1) \le D \tag{4}$$

where θ_1 and θ_2 denote the throughput capacities of the first and second hops in Equations 2 and 3, respectively, D specifies the whole delay requirement of packet transmission from sensors to AP in Equation 4. Equation 4 is the packet transmission delay constraint, which consists of the time period needed for packet generation by a sensor in the first hop, delivery in two hops and the left packets generation which construct a new packet with the delivered packet in the second hop. It is significant to note that only S_{d1} and S_{d2} are variables and others are constants, which can be obtained during implementation.

6 AnonNet Data Management Design

Vehicles are the main data carrier in AnonNet. They gather data from various data sources such as sensors and deliver it to the C2. Some vehicles like ambulances go to the C2 more frequently, while there may be some vehicles that do not visit C2 for hours. Time is a critical factor in disaster response. Thus, US&R operations happen simultaneously all round the disaster area, as long as the access to the area is cleared. These operations typically last for days; such patterns indicate that we may be able to take advantage of the traces of vehicles from a previous day in order to improve the data reception rate at C2.

Using the scenario above, our problem is described as the following. Given a large amount of data generated from var-

ious data sources, how can we achieve maximum throughput from the field to the C2? Consider two techniques: first, a sink for each sub sensor network (e.g., the network of building tags) responsible for handing over the data to the vehicles passing by must be elected such that the data can be delivered to C2 as quickly as possible (e.g., a sink might prefer to deliver data to the vehicle that more frequently visits the C2). Second, a fixed number of nodes called "data waypoints" are optimally placed in the disaster area to bridge the data transmission between the vehicles that have different frequencies of visiting the C2. Vehicles which visit the data sources more frequently drop off data at these waypoins, which then act as a data source to vehicles that visit the C2 more often. Note that these nodes are not storage databases, but merely a waypoint for data which is on its way to the C2.

Assuming that we have the GPS traces of vehicles from previous day and locations of deployed sensors and routers, selecting a sink for each sub sensor network and placing data waypoints can be together formulated as centralized optimization problem. When a vehicle (broadcasting beacons) comes within communication range of a sink node, data segment d_i is received until the vehicle is out of the communication range. A set $D = \{d_1, d_2, ..., d_n\}$ represents all the data received during the operation. For each data segment, $t_f(d_i)$ is the contact time with the vehicle, $t_c(d_i)$ is the flush time (i.e., the time when the data is flushed at C2). $s(d_i)$ is the size of data segment d_i, and the throughput of d_i is defined as $r(d_i) = s(d_i)/(t_f(d_i) - t_c(d_i))$. Assume that we have n sensors in the field, denoted by a set $V = \{v_1, ..., v_n\}$. Each node v_i has residual energy $b(v_i)$ and the total number of received beacons $c(v_i)$. The set V consists of k sub-sensor networks S_i as $V = S_1 \cup ... \cup S_k$. Each sub-sensor network S_i has a sink s_i. We denote the set of sinks as a set $S = \{s_1, ..., s_n\}$. Also, a set $P = \{p_1, ..., p_n\}$ represents the data waypoints. Now we are ready to define the Data Placement Problem (*DPP*) as follows:

$$\text{maximize} \quad \alpha \cdot \sum_{d_i \in D} r(d_i) + \beta \cdot \sum_{s_i \in S} sc(v_i) \tag{5}$$

$$\text{subject to:} \quad |P| \leq M \tag{6}$$

$$\forall i, S_i \neq \emptyset \tag{7}$$

$$\forall i, \exists s_i \in S_i \text{ and } |S| = k \tag{8}$$

where $sc(v_i)$, the eligibility score of node i to be selected as sink, is based on sink's residual energy and the number of received beacons from vehicles. The parameters α and β are used to determine the priority between the throughput and the score of a sink. The first constraint (6) means that the number of data waypoints are limited by M. The second constraint (7) shows that sub sensor network is not empty, and the last constraint (8) means that only a single sink is elected from each sub sensor network. The above problem is NP-Hard by reduction to the facility location problem, but the proof is omitted due to space constraints.

We separate the throughput maximization ($\Sigma_{d_i \in D} r(d_i)$) and resource maximization ($\Sigma_{s_i \in S} sc(v_i)$) problems into two optimization problems and provide sub-optimal solutions for them in the following sections. We call the former problem as Waypoint Placement Problem and the latter one as Sink Selection Problem.

Algorithm 2 Waypoint Placer

```
while k > 0 do
    for each l_i ∈ L do
        Place a storage unit at l_i (Previously selected storage units are in positions).
        Simulate the operation (using GPS traces, or mobility model).
        Compute K_i ← Σ_{d_i ∈ D} r(d_i).
    end for
    Find the largest K_j.
    L ← L \ {l_j}.
    k ← k − 1.
end while
```

Algorithm 3 Sink Election

```
Broadcast (HELLO)
create (CanTbl_{i,h})
if f_i > f_j for all j ≠ i then
    Snk_i = 1
    Broadcast (IAMSINK)
    while Snk_i = 1 do
        Collect-Pass (DATA)
    end while
    Broadcast (RE-ELECTION)
else
    set-sink()
end if
```

6.1 Waypoint Placement Algorithm

Our problem is to maximize the aggregate throughput (i.e., $\sum_{d_i \in D} r(d_i)$) by placing k temporary data holders called the *storage units*, denoted by a set $L = \{l_1, l_2, \cdots, l_n\}$ in the target region. We use a greedy algorithm to find the locations to place k storage units. The algorithm is shown in Algorithm 2. The algorithm proceeds by greedily selecting one storage unit. Once a storage unit is selected, the next storage units are selected based on an assumption that the previously selected storage units are already in position.

6.2 Sink Election Algorithm

Given a set of n deployed sensor nodes in the disaster area which attached to the buildings denoted by $V = \{v_i : i = 1 \ldots n\}$, $b(v_i)$ is the residual battery charge of node i, and $c(v_i)$ is the number of beacons received from vehicles in the last τ time units. We normalize these two parameters by dividing them to maximum battery charge and maximum number of beacons node can receive in τ; that depends on number of vehicles and their beaconing rate. Now, Let $sc : V \longrightarrow [0,1]$ be a scoring function that assigns the eligibility score to any node i based on $c(v_i)$ and $b(v_i)$ as two independent events; $sc(v_i) = c(v_i) \times b(v_i)$. The sink selection problem can be formulated as the maximization of $\Sigma sc(v_i)$ for a set of selected sinks, each of which are at most h hops from any node. This problem is reducible to the k-hop dominating set problem and is thus NP-Hard, but the proof is once again omitted for reasons of space.

This problem can be solved in a centralized way, where a powerful central processing node collects all information about the nodes and finds the optimal solution. However, because of resource constraints and lack of any base station, we propose a distributed solution for it where nodes elect sink nodes to cover all h hops nodes around.

We propose a distributed algorithm which is run by each sensor node, given a h which is determined pre-deployment. Sensor nodes periodically broadcast HELLO messages including their node ID, list of one hop neighbors, and their score as sc_i. After receiving HELLO messages, every node creates a table, $CanTbl_{i,h}$, of all the nodes within h hops. As shown in Algorithm 3, each node checks whether it has a higher score than all its h hop neighbors. If it does, the node broadcasts an IAMSINK message. According to the

assumption for maximum hop count, any sensor node will receive at least one IAMSINK message from h-hop neighbors. Sink nodes periodically update their score and compare it with others to see whether they are still a suitable node for being a sink or not. In case a sink finds itself an unsuitable candidate, it broadcasts a RE-ELECTION message to all the nodes and goes to non-sink mode.

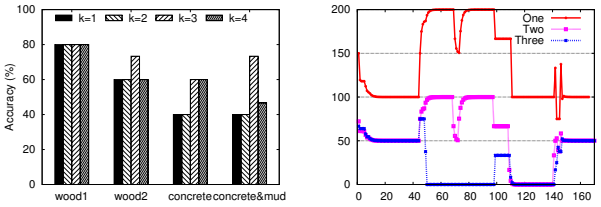
7 System Implementation and Evaluation

Hardware The hardware used in AnonNet includes the Netgear WNDR3700v1 router, EPIC motes, iPod Touchs and the Linksys WRT54GL which acts as an Extender. The WNDR3700 at an average cost of 100USD is in our opinion the best suited router, mainly because of the dual band 802.11 radios (2.4 and 5 Ghz), the support available for an open operating system (OpenWRT), a USB peripheral port and the comparatively luxurious 8MB of ROM and 64MB of RAM. The USB port can be used to provide exciting functionality like a new physical layer such as 802.15.4, enhanced storage like a USB flash drive or all of them (using a self powered USB hub). A cellphone can also be "tethered" to the router providing it with cellular network access. For implementing DTN functionality, we used the IBR-DTN implementation which is readily available as a package for OpenWRT. The software ecosystem offered by OpenWRT allowed us to completely customize the router according to our needs, with a variety of available and possible functionality. Using the widely used iOS SDK, the iPod Touch was customized. However, we were limited to the application layer since the SDK does not allow non-trivial modifications to the operating system for security reasons. The fact that 802.11 IBSS mode was readily supported out of the box made us choose iOS over Android.

Evaluation AnonNet is a complex wireless, sensor and adhoc network system. In this section we present the performance evaluation of the individual components of the system, as well as the entire system. AnonNet was evaluated over a period of 5 days in DisasterNewYork. (Figure 4(a)). DisasterNewYork is a comprehensive 52-acre training facility for emergency responders with extremely realistic wrecks. These include a passenger train wreck, several rubble piles of wood and concrete, a collapsed parking lot with automobiles, a collapsed strip mall and a damaged movie theater. The entire setup ensures a very realistic life sized replica of a modern disaster.

Simulation Evaluation of such a diverse system consisting of mobile nodes by varying scenarios and parameters with several runs per parameter is extremely labor/cost intensive and consumes precious man-hours. Therefore, we decided to conduct certain experiments using simulation that is as close to a real scenario as possible. We used the Opportunistic Network Environment simulator (TheONE) as it meets our needs for a mobility and networking simulator. Using a digital GIS map of DisasterNewYork and a GIS editing program, routes for the vehicles along with the locations of other components were designed and used in the simulator. All of the simulations described below use the same mobility traces, thus ensuring consistency.

Simulation Setup The entire setup in simulation consists



(a) (b)

Figure 5. (a) KNN classifier accuracy as a function of k. (b) Graph of state versus time for a team of three responders.

of 26 nodes - 15 data sources, two routes with 5 vehicles on each route and a C2 node. The default number of data waypoints is two, the vehicles move at a speed uniformly chose between $\mathcal{U}(5, 10)$km/h by default. The transmission range is 13m, in order to allow for a multi hop network. Each data source sends a packet of size $\mathcal{U}(2, 4)$KB every $\mathcal{U}(200, 300)$ seconds to the C2 and each of the data waypoints if applicable. The total simulation time for each scenario is 10h unless specified otherwise.

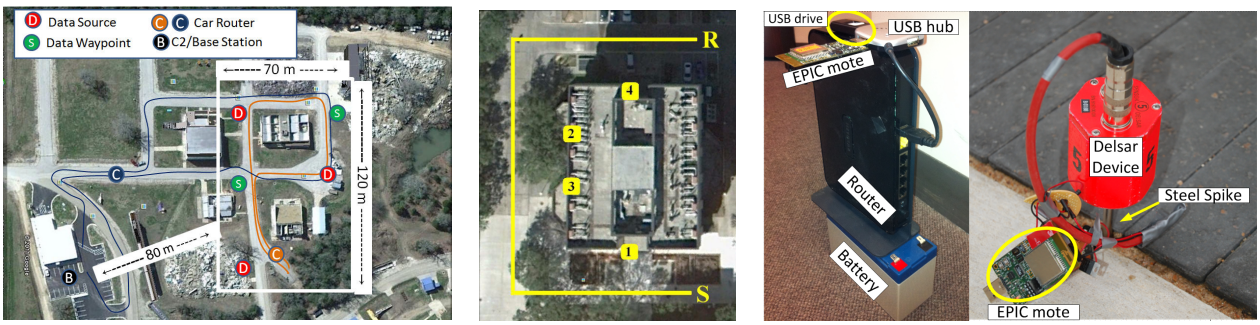
7.1 Building Sensing Networks

We evaluated our building sensing network in DisasterNewYork on three different rubble piles: one consisting of wooden rubble, one of concrete, and another with a combination of concrete and mud. In the latter one, the soft mud dampens the vibrations caused inside the pile and hence makes detection with a seismic sensor difficult. Using a spike-based seismic sensor, samples for different types of events were gathered at each of these piles: a stone drop, a footstep and a hammer strike. Half of the samples were used to train the KNN classifier, and the other half to evaluate performance.

All samples were taken at slightly different strike intensities and distances from the sensor. In our opinion, this method of sampling homogenizes the samples and does not tune the classifier to one particular distance or intensity. Results are shown in Figure 5(a). "wood1" represents samples taken at the wooden pile with the default sensitivity threshold of 25 and "wood2", at a threshold of 50. A higher threshold implies lower sensitivity. This higher threshold was not possible on the two other piles since the sensor could not register soft knocks and events. We conclude that a k of 3 provides for optimal performance from the KNN classifier with an average detection of accuracy of 73.33%. It is to be noted that this accuracy is independent of type of rubble pile, strike intensity of the event and the distance from the seismic sensor.

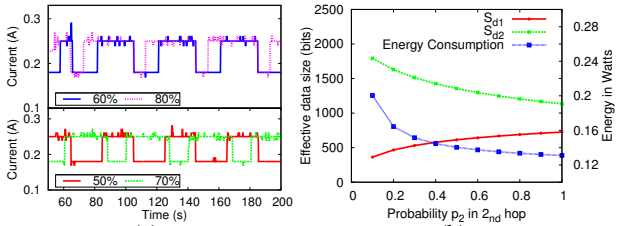
7.2 Separation Detection

The effect of separation upon the state of a team member is shown in Figure 5(b). An experiment was conducted inside an urban building where iPod touches running the separation detection app were given to each member. "One" is the team leader and hence injects a constant state into the network. Initially, all the team members were present in a single room until time 30. Then, One and Two separated from Three by going into another room. As a result, the state of Three drops to zero since it is no longer connected to One, and the states of Two as well as One increase and converge



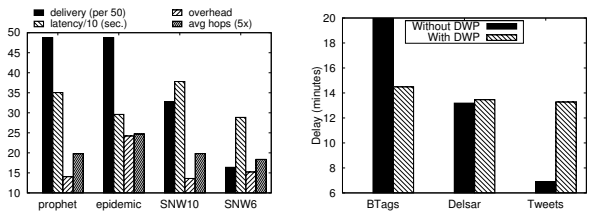
(a) (b) (c)

Figure 4. (a) Deployment Area. (b) Sink Election Real Test Area; (c) (Left) The WNDR3700 router with EPIC mote, USB hub, 8GB USB flash drive attached, and mounted on a 9Ah battery. (Right) A Delsar life detector with steel spike driven into the ground, and interfaced with an EPIC mote.



(a) (b)

Figure 6. (a) Routers exhibiting duty cycling at ratios of 50-80% uptime in a 40s period and (b) relationship between packets sizes in two hops and minimum energy consumption per second with increasing p_2



(a) (b)

Figure 7. (a) Evaluation of latency, delivery rate, overhead and average hop count for four different DTN routing protocols in simulation. (b) Evaluation of latency in AnonNet DTN using two data waypoints (DWP).

(time $40-60$). Then, One and Two move around in the large room with lot of metallic wall sized objects, causing disconnection. This disconnection is temporary and does not signal a separation. Later, Two returns to the same room as Three at time 95. As a result, the state of Three increases for time $100-110$ due to the residual state brought by Two, but both of them quickly decrease to zero at 110 since they are no longer connected to One. Finally, One reunites with Two and Three at 140 causing all of their states to converge once again to their initial values.

7.3 AnonNet Networking

Router Duty Cycling Fig. 6(a) shows the current drawn by Linksys Extenders undergoing duty cycling at various ratios with a 40s period. The base draw without any radio is 180mA, which increases to 250mA when the radio is active. With a portable 9Ah SLA battery, the avg. current drawn given a duty cycle of $0 < d < 1$ is $(180 + 70d)mA$. Given a base lifetime of 36h, a simple 70% duty cycle increases the lifetime by 3.3 hrs. Efficient duty cycling while providing acceptable performance, and extending it to multi-radio routers like the WNDR3700 are the subject of ongoing research.

DTN/Simulation The performance of several DTN routing protocols was evaluated in simulation with the simulation setup described above so as to choose the best protocol for the DisasterNewYork deployment. Epidemic routing aims to deliver messages by delivering to any neighbor that it encounters. As seen in Figure 7(a), it has one of the highest delivery rates and the lowest latency. A caveat is the overhead which is the number of extra messages created while routing per delivered packet, and the average hop count. In PRoPHET routing, each node maintains the probability of each of its neighbors being able to deliver a packet to a given destination. This information is exchanged at every encounter. While boasting a high delivery rate compared to a low overhead, the average latency is 50 seconds higher than epidemic routing. SNW refers to the Spray and Wait protocol which aims to bound the number of copies of a packet in the network by a given parameter. For 2 values of 10 and 6, the SNW protocol has a very low overhead and hop count, but has a low delivery rate and high latency. Given these performance metrics, we chose to use the epidemic protocol for its high delivery rate and low latency.

DTN/Implementation In order to evaluate networking, an experiment involving mobility and delay tolerant networking was conducted at DisasterNewYork. A router acted as the C2 and the endpoint for all data. Three data sources consisting of BTag data, tweets sent by first responders, and spectrum data from Delsar nodes were installed - along with two routers acting as data waypoints. Two vehicles carried one router each for a total of 8 DTN capable routers, as shown in Figure 4(a). The effective 802.11 radio range was about 5m. since the routers were kept on the floor of the vehicle's cabin. Both the vehicles moved on their predefined routes at irregular, unspecified times with near-constant but different speeds, limiting contact times to about one second.

None of the vehicles stopped or slowed down near any node. We chose this particular mobility model in order to evaluate based on harsh realities and not idealized, predetermined movement patterns like in simulations. To record the performance gain due to intelligent data waypoint placement, three bundles containing identical data was being generated every 30 seconds on each of data source nodes - one for the C2, one for each of the two data waypoints. Our results are presented in Figure 7(b).

For each stream of data, the end-to-end delay for each packet is computed and averaged. On a whole, the presence of data waypoints decreased the latency because picking up data from a fixed DWP is deterministic, while obtaining the same identical data from another mobile vehicle node is highly opportunistic. DWPs also ensure that some data which would have otherwise never made it to the C2 is now delivered because it is first handed over to a DWP which then acts as a data source for other vehicles. For BTags which were generated at the node in the bottom left, the presence of data waypoints decreases the delay. This can be seen since both DWPs are on the routes of both vehicles. The Delsar source is similar - since it is situated on a corner, contact times are also slightly higher. For tweets generated at the data source in the bottom, the number of packets received directly was extremely low because the only route is through non-storage routers. Because of this, the few packets that were received had a low delay. In conclusion, the presence of data waypoints improves packet delay on average, in the sense that it helps deliver packets which otherwise would never have reached the C2. A lot of other factors like the temporal nature of wireless links also play a significant role in these results.

Body Sensor Networks The optimal packet sizes to ensure minimum energy consumption in a two hop TDMA/CSMA network was investigated using MATLAB. The modeling parameters used [41, 18] were: $N = 3, \rho_{at} = 1.65W, M = 5, \rho_{ar} = 1.4W, t = 1s, \rho_{ai} = 1.15W, p_1 = 80\%, CW = 32, p_2 = 10\% \sim 100\%, R = 5, b = 5kbps, \theta_1 = 250kbps, S_{h1} = 88bits, \theta_2 = 54Mbps, S_{h2} = 240bits, D = 177ms, \rho_{st} = 35mW$. It is worth to note that D can meet the requirement of a mouth-to-ear delay [42]. Based on p_2 = 80%, we obtain $E = 0.1335W$, $S_{d1} = 690$ $bits$ and $S_{d2} = 1205$ $bits$. Fig. 6(b) shows the effect p_2 has on E. We conclude that with increasing successful transmission probability p_2, the energy consumption gradually decreases, and S_{d1} increases while S_{d2} reduces. Actual implementation and evaluation of these packet sizes and energy consumption in the sensing networks of AnonNet is ongoing.

7.4 Data Management

Data Waypoints/Implementation We use the experiment described above to look at how throughput is affected with the placement of data waypoints. To calculate the delay for a packet, we do not consider the end to end delay but the delay from a data waypoint to the C2 instead. This is because DWPs act as custodians of data - as an aggregator of data sources and thus data sources themselves. Results for the throughput and latency are presented in Figure 8.

We can see that using DWPs is once again beneficial in improving the throughput as well as the latency. The "Without DWP" component is the same as in Figure 7(b). The throughput performance is analogous to the delay. BTag packets are 79B each, Delsar packets are 1000B and tweets are 140B long. Needless to say, the Delsar data stream provides superior throughput because of the large data size of each packet. Since very few tweets make it directly to the base station, the low amount of packets received as compared via data waypoints introduces some abnormalities causing the direct throughput to be higher. In conclusion, data waypoints greatly improve the overall throughput. The very low throughput rates seen here as compared to those in traditional networks is due largely to irregular vehicle movements resulting in delays of 10s of minutes.

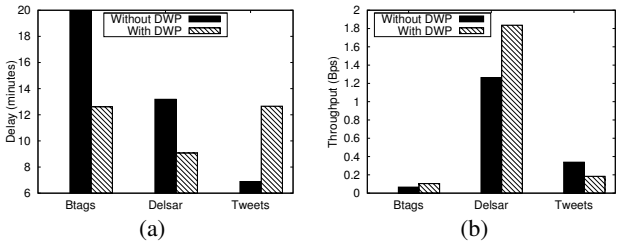


Figure 8. Data waypoint (DWP) performance in terms of (a) latency and (b) throughput, based on three data sources

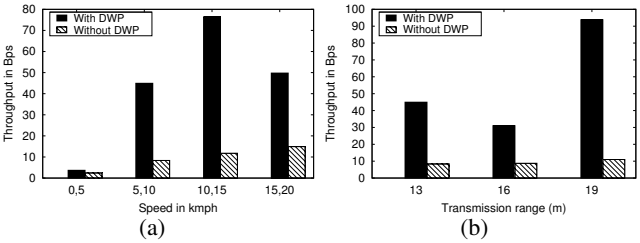


Figure 9. Dependence of aggregate throughput on (a) vehicle speed and (b) node radio transmission range, for two data waypoints

Data Waypoints/Simulation The effect of vehicle speed and node radio transmission range on the system's aggregate throughput was examined in simulation, since varying these parameters over a wide range in reality is labor intensive. Results are shown in Figure 9 for a system with two data waypoints as located in the map above, and with the parameters described above. We can see that DWPs provide superior throughput in all cases. At a speed of $\mathcal{U}$(10, 15)km/h, the throughput is the greatest. This is a speed attainable by most vehicles and a safe speed for a disaster stricken area. The radio range of a vehicle node does affect the throughput, but not as much. The throughput obtained by using data waypoints is much higher than without them, as seen in Fig. 9(b). Above 20m., some of the data sources were within range of the routers, causing an artificial increase in throughput. We find that a value of 13m. provides the best throughput.

Sink Election/Implementation A set of four building tag nodes was deployed around a building on campus as shown in Figure 4(b). A vehicle carried a "beacon node" which broadcast every second, back and forth from location S to R with a travel time of 61 seconds. We recorded the bea-

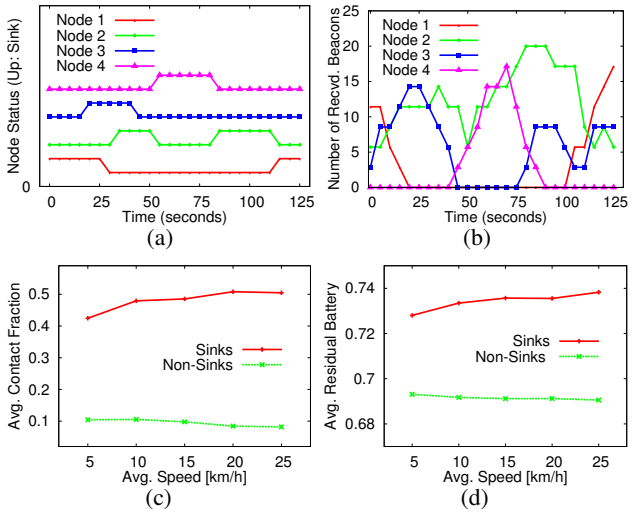


Figure 10. Sink election evaluation based on real implementation and simulation

con receiving rate of each node and its *elected*. The beacon receiving rate was considered as number of beacons a node has received in the last 20 seconds. We change this time interval intuitively based on the vehicles' speed, network density and re-election overhead. As depicted in Figure 10(b), the beacon receiving rate of the nodes changes while the position of the vehicle changes. The status of the nodes are also shown in Figure 10(a), where the nodes with higher beacon rate are always selected as sink. As the vehicle passes by a node, that node will most likely be selected as a sink; since HELLO messages were set to be exchanges every 5 seconds.

Sink Election/Simulation Our solution was evaluated in Matlab, but by using the same mobility traces produced by the setup described above. Vehicles broadcast beacons every second. We define the contact fraction metric as the number of beacons received in the last 60 seconds divided by the maximum receivable. Figure 10(c) shows that the contact fraction averaged over sinks is always higher than those of the non-sinks, at all speeds. The average residual battery charge exhibits similar characteristics as shown in Fig. 10(d). The reason that faster speeds give better results is because of the lower probability of selecting nodes with shorter contact times. Since the scoring function is a function of both residual charge and beacon rate, the nodes with shorter contact fraction do not get a higher score, even though they have residual battery as high as others.

8 AnonNet Status and Future Roadmap

We have presented AnonNet - a mobile, wireles, delay tolerant network tailored for disaster response built with requirements from first responders. The design provides for a robust, reliable, efficient system which incorporates heterogeneous technologies and is entirely battery powered. Seismic sensing systems can classify data with 73.3% accuracy on real rubble piles, based on mote based FFT and reports it to responders via a prompt on their smart phones. Data waypoints act as optimized data caches which improve the throughput of the system as a whole. Support for third party technologies using open standards enables error free integration and deployment.

AnonNet is an initial approximation of a system that can be deployed in disasters. There is much that needs to be done in terms of energy efficiency, improving latency and adding new functionality like chemical hazard sensors or acoustic victim detection that can locate victims from whispers. We look forward to seamless integration of a wide variety of cloud based services with AnonNet. Such services provide for cheap data storage, processing, and quick deployment. SIP based voice services can deliver simple audio and video streams from iOS devices.

9 References

[1] Japan hit by tsunami after massive earthquake. http://www.bbc.co.uk/news/world-asia-pacific-12709850.

[2] 2010 haiti earthquake (wikipedia). http://en.wikipedia.org/wiki/2010_Haiti_earthquake.

[3] Federal emergency management agency. http://www.fema.gov.

[4] Army to deploy iphones in combat. http://abcnews.go.com/Technology/army-prepares-deploy-smartphones-iphones-combat/story?id=12395650.

[5] US&R Task Force Equipment. http://www.fema.gov/emergency/usr/equipment.shtm.

[6] Project 25 technology interest group. http://www.project25.org/.

[7] Project 25 interoperable communications for public safety agencies. http://www.motorola.com/web/Business/Solutions/Business Solutions/Mission Critical Communications/ASTRO 25 Trunked Solutions/_Document/Project 25 Whitepaper.pdf.

[8] G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, and M. Welsh. Monitoring volcanic eruptions with a wireless sensor network. In *EWSN*, 2005.

[9] S.G. Iyengar, P.K. Varshney, and T. Damarla. On the detection of footsteps based on acoustic and seismic sensing. In *ACSSC*, 2007.

[10] G.P. Mazarakis and J.N. Avaritsiotis. A prototype sensor node for footstep detection. In *EWSN*, 2005.

[11] Matteo Ceriotti, Luca Mottola, Gian Pietro Picco, Amy L. Murphy, Stefan Guna, Michele Corra, Matteo Pozzi, Daniele Zonta, and Paolo Zanon. Monitoring heritage buildings with wireless sensor networks: The torre aquila deployment. In *IPSN*, 2009.

[12] A. Pakhomov and T. Goldburt. Seismic signal and noise assessment for footstep detection range estimation in different environments. In *Proc. SPIE*, volume 5417, pages 87–98.

[13] Steven W. Brown, Ms William, G. Griswold, Barry Demchak, Ba Leslie, and A. Lenert. Middleware for reliable mobile medical workflow support in disaster settings, 2006.

[14] M. Arisoylu, R. Mishra, R. Rao, and L. A. Lenert. 802.11 wireless infrastructure to enhance medical response to disasters. *AMIA Annu Symp Proc*, pages 1–5, 2005.

[15] J. P. Killeen, T. C. Chan, C. Buono, W. G. Griswold, and L. A. Lenert. A wireless first responder handheld device for rapid triage, patient assessment and documentation during mass casualty incidents. *AMIA Annu Symp Proc*, pages 429–433, 2006.

[16] L. A. Lenert, D. A. Palmer, T. C. Chan, and R. Rao. An Intelligent 802.11 Triage Tag for medical response to disasters. *AMIA Annu Symp Proc*, pages 440–444, 2005.

[17] Krishna Kant Chintalapudi and Lakshmi Venkatraman. On the design of mac protocols for low-latency hard real-time discrete control applications over 802.15.4 hardware. In *IPSN*, 2008.

[18] Gang Zhou, Jian Lu, Chieh-Yih Wan, M.D. Yarvis, and J.A. Stankovic. Bodyqos: Adaptive and radio-agnostic qos for body sensor networks. In *Infocom*, 2008.

[19] I-Hong Hou and P. R. Kumar. Admission control and scheduling for qos guarantees for variable-bit-rate applications on wireless channels. In *MobiHoc*, 2009.

[20] Zhen Ren, Gang Zhou, Andrew Pyles, Matthew Keally, Weizhen Mao, and Haining Wang. Bodyt2: Throughput and time delay performance assurance for heterogeneous bsns. In *Infocom*, 2011.

[21] Kevin Fall, Gianluca Iannaccone, Jayanthkumar Kannan, Fernando Silveira, and Nina Taft. A disruption-tolerant architecture for secure and efficient disaster response communications. In *International Con-*

ference on Information Systems for Crisis Response and Management, 2010.

[22] Hamed Soroush, Nilanjan Banerjee, Aruna Balasubramanian, Mark D. Corner, Brian Neil Levine, and Brian Lynn. DOME: A Diverse Outdoor Mobile Testbed. In *HotPlanet*, 2009.

[23] Vladimir Dyo, Stephen A. Ellwood, David W. Macdonald, Andrew Markham, Cecilia Mascolo, Bence Pásztor, Salvatore Scellato, Niki Trigoni, Ricklef Wohlers, and Kharsim Yousef. Evolution and sustainability of a wildlife monitoring sensor network. In *SenSys*, 2010.

[24] S. Mehrotra, C. Butts, D. Kalashnikov, N. Venkatasubramanian, R. Rao, G. Chockalingam, R. Eguchi, B. Adams, and C. Huyck. Project rescue: Challenges in responding to the unexpected. In *SEISC*, 2004.

[25] Raheleh B. Dilmaghani and Ramesh R. Rao. An ad hoc network infrastructure: Communication and information sharing for emergency response. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication*, pages 442–447, 2008.

[26] B.S. Manoj and Alexandra Hubenko Baker. Communication challenges in emergency response. *Commun. ACM*, 50:51–53, March 2007.

[27] Raheleh B. Dilmaghani, B. S. Manoj, Babak Jafarian, and Ramesh R. Rao. Performance evaluation of rescue mesh: A metro-scale hybrid wireless network. In *Proceedings of WiMesh Workshop, SECON*, 2005.

[28] Bo Xing, S. Mehrotra, and N. Venkatasubramanian. RADcast: Enabling reliability guarantees for content dissemination in ad hoc networks. In *Infocom*, 2009.

[29] Network-centric warfare and wireless communications. http://www.meshdynamics.com/documents/MD_MILITARY_MESH.pdf.

[30] Wenrui Zhao, Yang Chen, Mostafa Ammar, Mark Corner, Brian Levine, and Ellen Zegura. Capacity enhancement using throwboxes in dtns. In *MASS*, 2006.

[31] Nilanjan Banerjee, Mark D. Corner, Don Towsley, and Brian N. Levine. Relays, base stations, and meshes: enhancing mobile networks with infrastructure. In *Mobicom*, 2008.

[32] N. Banerjee, M.D. Corner, and B.N. Levine. An energy-efficient architecture for dtn throwboxes. In *INFOCOM*, 2007.

[33] M. Ibrahim, P. Nain, and I. Carreras. Analysis of relay protocols for throwbox-equipped dtns. In *WiOPT*, 2009.

[34] M. Farukh Munir, A.A. Kherani, and F. Filali. Stability and delay analysis for multi-hop single-sink wireless sensor networks. In *PerCom*, 2008.

[35] M. Younis, M. Bangad, and K. Akkaya. Base-station repositioning for optimized performance of sensor networks. In *VTC*, 2003.

[36] D. Kim, W. Wang, N. Sohaee, C. Ma, W. Wu, W. Lee, and D.-Z. Du. Minimum data-latency-bound k-sink placement problem in wireless sensor networks. *IEEE/ACM ToN*, 2011.

[37] Myounggyu Won, Mike George, and Radu Stoleru. Towards robustness and energy efficiency of cut detection in wireless sensor networks. *Elsevier Ad Hoc Networks*, 9(3):249–264, 2011.

[38] Kevin Fall. A delay-tolerant network architecture for challenged internets. In *Proceedings of Conference on Applications, technologies, architectures, and protocols for computer communications*, 2003.

[39] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss. Delay-Tolerant Networking Architecture. RFC 4838 (Informational), April 2007.

[40] K. Scott and S. Burleigh. Bundle Protocol Specification. RFC 5050 (Experimental), November 2007.

[41] J. Polastre, R. Szewczyk, and D. Culler. Telos: enabling ultra-low power wireless research. In *IPSN*, 2005.

[42] Aruna Balasubramanian, Ratul Mahajan, Arun Venkataramani, Brian Neil Levine, and John Zahorjan. Interactive wifi connectivity for moving vehicles. In *SIGCOMM*, 2008.