Practical Experiences in Enabling and Ensuring Quality Sensing in Emergency Response Applications

Chris Davison[1], Daniel Massaguer[1], Lilia Paradis[2], M. Reza Rahimi[1], Bo Xing[1]
Qi Han[2], Sharad Mehrotra[1], Nalini Venkatasubramanian[1]
[1]School of Information and Computer Science, University of California, Irvine, USA
[2]Department of Mathematical and Computer Science, Colorado School of Mine, USA

***Abstract*- Situational awareness in emergency response is critical. Knowing the status of the hazards, the rescue workers, and the building occupants, etc., can greatly help the incident commander make the right decisions in responding emergencies, and as a result, save lives. Such situational awareness can be achieved by using existing sensing and communication infrastructures and/or having rescue practitioners dynamically deploy their own. Nevertheless, current sensing and communications techniques are, not fault-free. In this paper, we study, through both lab experiments and real emergency response drills, the nature of different wireless networks (sensor networks and Wi-Fi networks) in transmitting various types of data. Based on our findings, we propose a series of practical techniques that potentially enhances the reliability of data delivery over heterogeneous wireless networks, by exploiting the availability of multiple networks, the rescue workers' mobility, and the possibility of having rescue teams carry redundant sensors.**

I. INTRODUCTION

The problem of delivering information needed for mission-critical applications in a manner that enables optimal decision making, is one of the challenging problems in reliable systems development. Mission-critical information comes in various forms such as small-size data, voice and video, over possibly congested, partially available and failing networks. Reliability of this information is critical for proper decision making. However, a generic (one-size-fits-all) notion of reliability is not what is required and is not applicable either.

Improving sensing and delivery reliability in wireless sensor networks has been addressed by routing protocols such as GRAB [3], transport protocols such as ESRT [4] and CODA [5], and data management techniques such as [6]. Forward Error Correction has been validated as an effective loss mitigation scheme for multimedia steaming in both wired [8] and wireless networks [9] , [10].

This paper focuses on the role of the network and its reliability in supporting situational awareness for emergency response applications. Specifically, we look at building emergencies such as structural fires. For such type of emergencies, the quality of the data being transmitted from inside the building to the incident commander outside the building is critical. Getting the right data at the right time to the incident command post enables the incident commander to make better decisions. In this paper, we aim at understanding the reliability/latency properties of multi-modal multi-network transmissions over Zigbee [12] and Wi-Fi [11] infrastructure in the context of responding to building level emergencies. We draw conclusions into what can be expected in mission-critical scenarios viz-a-viz reliability in data collection and transfer rather than suggest a specific protocol.

We investigate the reliability of wirelessly delivering three forms of data -- small-size sensor data, voice, and video data --captured in a firefighting scenario setting. First, we establish notions (metrics) of application level reliability. Given these metrics, we experimentally determine how they are impacted by varying environmental and network situations both through controlled experiments and through larger scale drills. Second, we study reliability in a set of emergency response drills. Our experiments and tests show that existing techniques for deliveries of multiple data types over existing networks are insufficient. To this end, we further explore reliability-enhancing techniques at both infrastructure and information levels and addresses the challenges accordingly.

II. RELIABILITY OF SMALL-SIZE DATA DELIVERY OVER WIRELESS SENSOR NETWORKS

To understand the reliability of small-size sensor data delivery in wireless sensor networks, we have conducted experiments for star, straight line, and mesh network topologies. We used eight TelosB motes in the experiments for star and line topologies. Figure 1 shows reasonable delivery rate under various load scenarios in a star network. When packets were generated every 500 ms, almost every packet safely arrived at the base station. However, slight performance degradation was observed when packets were generated every 200 ms. It is interesting to note that the performance loss appeared almost equally throughout all motes. This is because all of the motes were one hop neighbors of the base station and therefore, each has an equal opportunity to communicate with the base station in congested traffic situations.

Figure 2 shows the results for the straight line topology. The results were similar but near 100% packet delivery rate was observed when packet generation period is higher than 1.0 second. The most notable difference was that performance loss did not appear as equally spread out as in star network topology. That is, the farther away from the base station, the more loss was observed. This is expected, because higher level parents assume more responsibility (more traffic load; traffic of itself and that of its descendants). It is more prone to

978-1-4244-5328-3/10/$26.00 ©2010 IEEE

high traffic load situations. Thus, the line length could significantly affect overall network performance. When designing this type of networks, one should prevent the network length from being too large.

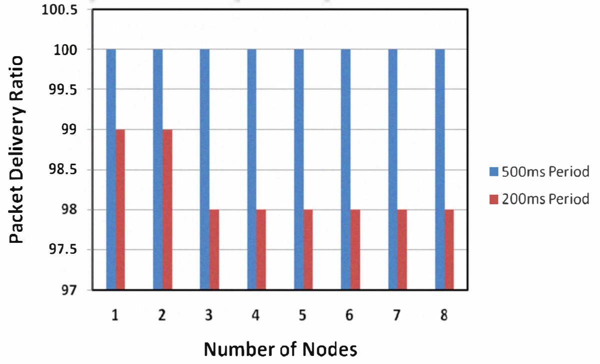

Figure 1: Packet Delivery Ratio for Star Topology with different packet generation rates.

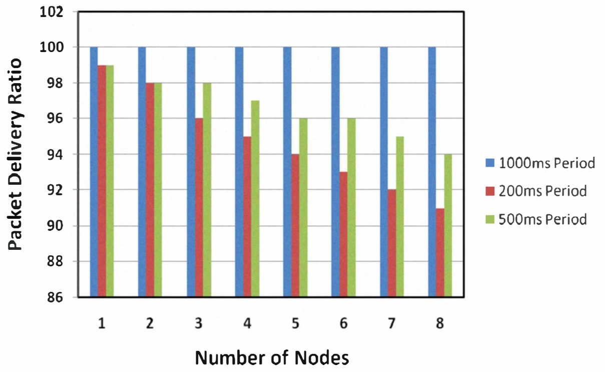

Figure 2: Packet Delivery Ratio for Straight line topology with different packet generation rates.

Unlike the star and straight line network topologies, mesh network topologies have many factors that might affect overall performance of data delivery. These include route update period, routing capability of each node, types of application, etc.. For mesh topologies, we formulated the problem as a graph coloring problem with precedence constraints and interference constraints. We designed TIGRA -- a distributed heuristic for graph coloring that takes into account application semantics and special characteristics of sensor networks [1]. TIGRA ensures that no interference occurs and spatial channel reuse is maximized by assigning a specific time slot for each node. Although the end-to-end delay incurred by sensor data collection largely depends on a specific topology, platform, and application, TIGRA provides a transmission schedule that guarantees a deterministic delay on sensor data collection.

We implemented TIGRA on an indoor testbed of 43 Tmote Sky nodes using TinyOS 2.0 [13]. Those nodes are placed in a rough grid topology. Nodes are approximately 3-4 meters apart from each other. The packet delivery ratio of TIGRA can only reach 65.5% which is significantly less than in our simulation experiments (always 100%). This suggests that even though TIGRA provides a deterministic delay in theory, in practice, reliability features must be added to the protocol before similar performance can be achieved.

III. RELIABILITY OF MULTIMEDIA DATA DELIVERY OVER WI-FI NETWORKS

Different from Zigbee sensor networks, Wi-Fi networks (including WLAN, Wi-Fi ad-hoc networks and mesh networks [2]) are typically used for delivering data types that require high transmission rate to achieve high quality rendering, such as audio/video. In this section, we explore the characteristics of audio and video data transfer over Wi-Fi networks.

A. *Speech Data*

To determine the reliability of Wi-Fi networks for speech transmission quantitatively, we conducted the following experiments. The experimental setup comprises a mobile device that records and sends an audio file over a WLAN to the server. The server runs speech recognition software on the file and converts it into text data. A third machine is used to send huge amounts of data over the WLAN to create heavy network traffic. We define two performance metrics:

1. *Quality of the speech received*: The received audio file is replayed and rated as very clear, understandable, or not clear by humans.
2. *Text-to-speech ratio*: This is calculated as the average ratio of the number of words accurately converted into text with respect to the amount of audio sent.

These metrics were measured in a series of experiments where the speaker was either stationary or mobile, and with and without the presence of ambient and network noise. Figure 3 shows the results of the tests.

	Noise		Text to Speech Ratio	Quality
	Network	Ambient		
Stationary	No	No	0.767	Very Clear
		Yes	0.589	Understandable
	Yes	No	0.533	Not Clear
		Yes	0.483	Not Clear
Mobile	No	No	0.739	Very Clear
		Yes	0.611	Understandable
	Yes	No	0.522	Not Clear
		Yes	0.467	Not Clear

Figure 3:Test results for audio transmission over Wi-Fi networks.

The experiment results indicate that the current quality and reliability of Wi-Fi networks for speech transmission is not very satisfactory due to the unpredictable and spotty coverage of the Wi-Fi infrastructure. In potentially life-threatening situations, the reliability of message delivery back to the base station is the most crucial requirement. This however cannot be achieved over existing Wi-Fi infrastructures with no extra measures being taken, due to factors such as device range, available power, bit rate, routing protocol, and any failure or uncooperative behavior of other devices.

B. *Video Data*

Sharing real-time video between mobile devices has even more stringent requirements on the underlying networking technologies because of the high bandwidth and tight latency constraints. While Wi-Fi infrastructure mode has been widely deployed and used for video streaming, the potential of Wi-Fi ad-hoc mode has not been fully explored. Instead of communicating through access points, ad-hoc mode enables mobile devices that are within each other's range to communicate directly. However, it is not clear whether Wi-Fi ad-hoc mode would really bring benefits (for instance, for video delivery) in this case and what the benefits are if any.

In this subsection, we present our experimental study on video streaming performance on real mobile devices. Our goal is to identify the tradeoffs between using Wi-Fi ad-hoc and infrastructure modes for device-to-device video delivery. In the meantime, we seek to shed light on the limitations of Wi-Fi infrastructure mode as well as the benefits of using ad-hoc mode as an alternative for mobile video streaming.

The devices we use in our experiments are the Nokia N800 Internet Tablets. The devices' Wi-Fi transmission powers are uniformly tuned to 10mW (transmission range being approximately 35 meters). For video recording and streaming on the devices, we employ the Gstreamer library. We experiment with a pre-recorded AVI video file (1-minute long). The signature video is captured by the N800's embedded camera at the frame rate of 15 frames per second. The resolution is 320*240. It is encoded using an H.263 codec at the bit rate of 96kbps. The server of a streaming session runs a Gstreamer [15] pipeline which encapsulates the H.263 video data in RTP packets and sends them to the client through UDP. The client also runs a Gstreamer pipeline, which, upon receiving the RTP packets, decodes the payload and displays the video.

We measure the streaming performance in a "roundtrip" fashion. At the server side, every RTP packet being sent out to the client is in the meantime directed to a local UDP port, where the packet's sequence number, payload size, timestamp as well as its departure time (based on the server's clock) is logged. As soon as the packet arrives at the client side, it is bounced back to the server through UDP. The server then logs the returning packet's arrival time (again, based on the server's clock). When the streaming session finishes, based on these logs, the server calculates the performance metrics.

The performance metrics are defined as follows:

1. *Latency (Round-Trip Time):* The latency of a particular RTP packet is the time elapsed from when the packet is sent out by the server till when the packet is bounced back and arrives at the server. The latency of a streaming video is the average of the latencies of all its RTP packets.
2. *Jitter*: The jitter of a particular RTP packet is the difference between the latency of this packet and the latency of its preceding packet (the packet whose sequence number is smaller by 1). The jitter of a streaming video is the average of the jitters of all its RTP packets.
3. *Loss Rate:* The loss rate of a streaming video, is the ratio of the number of packets that are not bounced back to the total number of RTP packets the video contains.

The streaming performances were defined under the following four settings:

Ad-Hoc 1 Hop: The server device and the client device communicate directly.

Ad-Hoc 2 Hops: The server device and the client device communicate through a relaying device. All the traffic between the server and the client devices will go through the relaying device.

Public AP: The server and the client devices communicate through an access point, which is accessible to all people in the building (and thus may have unknown background traffic).

Private AP: The server device and the client device communicate through an access point, which is only accessible to our experiments (and thus has no other traffic).

To have more realistic experiments, we conduct three sets of experiment*s:*

Varying Traffic Load: we vary the bit rate of the video between a server/client pair from 96kbps, 192kbps, to 480kbps.

Varying Level of Contentions and Collision: we introduce two more mobile devices and thus make two server/client pairs. We run two streaming sessions (each at 96bps bit rate) separately over the two server/client pairs in parallel.

Varying Distance: We vary the distance between a server device and a client device from 0m, 10m, to 40m, and run 5 concurrent streaming sessions (480kbps bit rate) between them.

As the results from the three experiment sets have similar indications, we only present here the results from the first experiment set. Figures 4 through 6 show our experiment results. The overall finding from our experiments is that, ad-hoc 1 hop performs slightly better than ad-hoc 2 hops, which in turn performs better than private AP; all of the above greatly outperform public AP. Public AP suffers from unknown background traffic, and its performance is very unpredictable depending on the time of a day and the day of a week. Ad-hoc 1 hop performs better than ad-hoc 2 hops because of the absence of intermediate devices, which increases the bandwidth share at each device and reduces potential contentions and collisions. The comparison between ad-hoc 2 hops and private AP is insightful in that it reveals the impact of beaconing on video streaming. Beaconing in infrastructure mode is performed solely by the access point, which makes it a performance bottleneck when the network is heavily loaded. In contrast, in ad-hoc mode, all participating devices rotate in performing the beaconing task, which mitigates the bottleneck problem, and as a result enhances video streaming performance.

In summary, our experiments show that, for delivering video between mobile devices in close proximity, Wi-Fi ad-hoc mode performs comparatively to, and in many cases outperforms infrastructure mode. The performance gain of ad-hoc mode is especially significant when the streamed video is of high bit rate, and/or multiple co-located devices are streaming videos simultaneously.

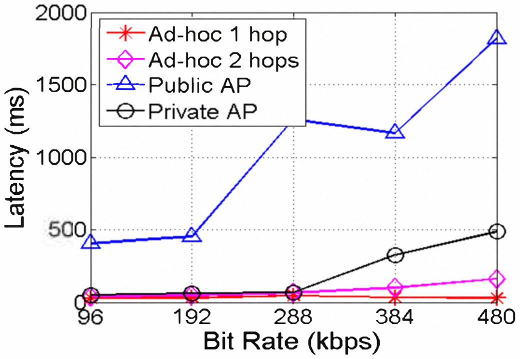

Figure 4: Latency results for video delivery over Wi-Fi network.

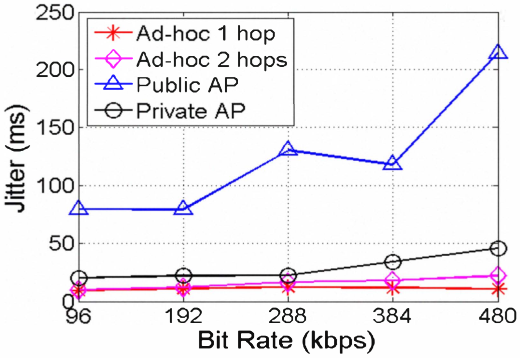

Figure 5: Jitter results for video delivery over Wi-Fi network.

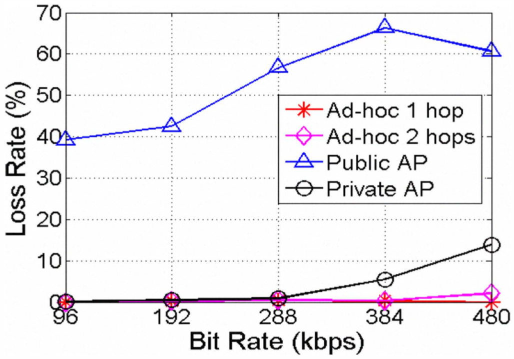

Figure 6: Loss rate results for video delivery over Wi-Fi network.

On the other hand, the service quality offered by infrastructure mode can vary tremendously and is unpredictable, depending on various factors that users might not have control of (such as infrastructure planning, background traffic). While ad-hoc mode is used for instant networking needs, its parameters are configurable by users; this provides more flexibility in fine-tuning the performance. Hence, Wi-Fi ad-hoc mode could provide a beneficial complement to infrastructure mode for mobile video delivery.

IV. Observations about Reliable Sensing from Drills

In addition to lab-based controlled experiments, we further conducted a series of emergency response drills to measure the reliability of multi-modal data using multiple networks in a more realistic scenario. The three main drills were the OCFA Live Burn drill, the Responsphere [14] HazMat Drill 1, and Responsphere HazMat Drill 2.

In these drills, network connectivity was enhanced using mesh routers, which established a Wi-Fi hot spot where we were able to upload information arriving from multiple sources. The battery-powered routers, adapted from commercial products manufactured for military applications, contain two radios: one provides a Wi-Fi bubble so first-responder sensor data can be easily uploaded, and the other supplies backhaul connectivity to the Internet in order to make the data widely available. The routers have been designed to plug into existing Ethernet connections or connect to high-speed wireless broadband using EVDO cards. All the routers—whether there are two or 50—can mesh with each other, carrying the data in "hops" from one to the next until it reaches its destination.

The antenna array is a set of two IEEE 802.11g layer 2 repeaters coupled with an EVDO layer 3 routers. The array is designed to provide maximum distance between repeaters as well as provide large Wi-Fi bubbles within the area of deployment. For all of the drills, the Wi-Fi mesh network was deployed with the same two repeaters and same layer 3 router. However, amplifiers were subsequently added as well as higher gain antennas increasing performance of the overall IP network.

For the OCFA drill as well as the Responsphere Drill 1, each firefighter carried a set of motes which would sense data such as light, sound levels, GPS coordinates, and CO levels. The base station for these motes was connected to a laptop at the Incident Command Post (ICP). The data captured from the motes was fed into the Fire Incident Command Board (FICB) to provide situational awareness to the Incident Commander (IC). During the Responsphere HazMat Drill 2, we deployed two mobile ZigBee gateways configured with the same Group ID. These gateways collected the mote data (when in range of the various static and dynamically deployed motes) and subsequently relayed that data back to the FICB.

The following observations were made from the experiments in controlled environments as well as more realistic drills.

1. *Cyber-physical system co-design is important*:
   In other words, design and deployment of nodes should consider the constraints imposed by the physical environment. A one-router mesh network was enough to support the communications between firefighters and incident commanders after taking into account environmental factors (e.g., a single structure fire). A one-router mesh network, nonetheless, was not enough for both of the Hazmat Responsphere drills which covered a larger geographical area in which multiple buildings were utilized in the drill.
2. *Mobility Reduces Reliability:*
   Due to mobility the Zigbee network took a long time to converge. While the routing topology is not stable packets got lost. Routing updates should be sent often. Wi-Fi Ad-hoc networks are sensitive to mobility since devices might easily get out of range.

3. *Packet Rate and Topology Impact Reliability:*
   Whereas one would desire to send multiple packets per second to lower the network convergence time and increase the temporal redundancy of data, sending too many packets per second also lowers reliability. Network topology also impacts reliability -- the farther from the root the most likely a packet will get lost.
4. *Failures Occur:*
   In an application such as firefighting one needs to accept that failures will happen. There is no time to diagnose the problem on-the-spot, much less to reconfigure computers, swap/recharge batteries, or change cables. Failures are aggravated by the presence of hazards such as fire: we can almost pinpoint the exact second our camera inside the building melted!
5. *Current Network Mechanisms Are Sensitive to Noise:*
   Even with theoretically correct algorithms (e.g., TIGRA) that provide 100% reliability in simulations, packets do get lost in reality. Network and ambient noise, which are *usually* unpredictable, reduce the reliability of data as well.

Based on these observations it is understood that existing techniques for delivery of multiple data types over existing networks for emergency response are insufficient.

V. TECHNIQUES TO INCREASE RELIABILITY

Aiming at enhancing the reliability of data delivery, we propose several approaches to enabling more robust data transfer in the scenarios we are targeting. We suggest techniques that can be applied at the infrastructure and/or information levels.

A. *Exploiting Multiple Technologies to form Connected Networks (Infrastructure Level)*

When network infrastructure support is needed, a straightforward approach is to set up a temporary mesh overlay, where mesh routers are placed around the area in such a way that altogether they form a connected multi-hop network. The mobile nodes communicate with each other and with the outside world by connecting to one of the mesh routers and directing all traffic to the routers. In theory, this would work perfectly in providing a network infrastructure for the communication needs of the scenario. However, in practice, it is difficult and time-consuming to discover how to place the mesh routers to fully cover a specific area. According to our deployment experiences, the number of mesh routers needed and their placements depend on various factors, such as the size of the area, the architectures in the area and the interference sources in the area. Hence, in certain scenarios, setting up mesh overlays might not meet the time constraints.

When instant network deployment is required, forming connected networks through the direct ad-hoc links between adjacent mobile nodes (mobile ad-hoc networks) is an alternative. The premise here is that the mobile nodes need to be located sufficiently densely although they can move around freely. Through autonomously forming such networks, mobile nodes establish indirect connectivity to the outside world – they send their contextual data hop by hop to the gateway nodes (which have direct connectivity to the outside world). Intermediate mobile nodes on the path serve as the relays for the information flow.

Forming ad hoc networks among wireless sensor nodes is another option that delivers sensing data from fields to control boards. The main advantage of wireless sensor networks is its low deployment cost and low power requirements. However, to establish the paths from fields to the destinations, the same requirements as in mobile ad-hoc networks need to be satisfied: the motes have to be deployed in a dense manner. In addition, because of the low bandwidth available, wireless sensor networks are typically used only for small-size data, and are not suitable for rich content data such as voice and video.

Other than using the above technologies alone, there are many possibilities for combining them and thus further enhancing reliability. For example, certain mobile nodes may be equipped with multiple interfaces (Wi-Fi, or Zigbee) and could serve as the gateway between different types of networks. Further, if all mobile nodes have multiple interfaces, different types of data (control data, contextual data, rich content data, etc.) can flow through different types of networks, which potentially reduces the network congestion level and enhances reliability, timeliness and efficiency. However, most off-the-shelf mobile devices currently have single radios; even for the devices with multiple radios, practical constraints exist probably only one radio is allowed to function at a time.

B. *Exploiting Mobility in Disconnected Networks*

In scenarios where mobile nodes are sparsely located and move around dynamically, the connectivity between one another is intermittent and highly unpredictable. As a result, it is impossible to form stably connected networks at all times. However, while nodes move around, they can potentially serve as mobile routers for the data that is destined for certain gateways. Hence, mobility can be exploited as a way to facilitate the propagation of data. Each mobile node maintains a cache which stores the data generated by it and other nodes (called bundles). When mobile nodes encounter each other, they exchange the bundles they are carrying, with the goal of increasing the probability that the bundles will be delivered to the final destinations. When a mobile node encounters a device which is the destination of a bundle in its cache, the bundle is delivered. This is exactly the well-known store-move-and-forward model that has been widely adopted in the Disruption-Tolerant Networking (DTN) research efforts [16].

Based on the above model, several core questions need to be addressed. First, replication: how many copies should be generated for each bundle? Second, forwarding: Which bundles should be forwarded upon device encounters, and in what order? Third, purging: if an incoming bundle would cause cache overflow, which bundles currently in the cache should be removed to accommodate the new bundles? The answers to these questions compose the solution to the problem. The overriding goal here is reliability, i.e., to deliver as many bundles as possible to their destinations. Meanwhile, storage efficiency (small storage on mobile nodes is consumed), transmission efficiency (small number of transmissions take place) and timeliness (short latency is incurred before bundles reach their destinations) are pursued as well.

C. Combining Connected and Disconnected Networks

In reality, there might be many scenarios in which connected networks and disconnected networks co-exist – some mobile nodes are located closely and can form a mobile ad-hoc network for a relatively long period of time, while some others are located sparsely and meet from time to time. In this case, the technologies that have been developed for mobile ad-hoc networks and those designed for disruption-tolerant networks can be integrated to leverage the characteristics of such mixed networks.

Essentially, a mobile ad-hoc network is a special case of a disruption-tolerant network, where the durations of the device encounters are relatively long-lived. With that being considered, the store-move-and-forward model should also work in mobile ad-hoc networks, and thus the mixed networks as well. In combing the two types of networks, the solutions to the sub-problems can be tailored to accommodate the characteristics of mobile ad-hoc networks. For example, when a mobile node has a path (spanning several intermediate relaying nodes) to reach the destination of a bundle, it should be forwarded the bundle, and transmits it directly to the destination through that path. In that way, both connectivity and mobility are exploited, and as a result, delivery reliability can be maximized.

VI. Conclusions

Networks can have significant impact on enabling situational awareness for emergency personnel, but not necessarily in the same way and to the same extent for all forms of data. In this paper, we studied the faulty nature of different types of wireless networks for different types of data (voice, video, and sensor data). We performed this study both in a controlled environment as well as emergency response drills. We find out that errors are always present and existing techniques are not sufficient to guarantee a certain degree of reliability. Based on our findings we proposed a set of techniques to increase reliability. Our techniques exploit the availability of different types of networks as the firefighters move and the spatio-temporal redundancy achieved by having each firefighter carry several sensors that sense the same phenomena.

VII. Acknowledgments

This work has been partially supported by the National Science Foundation (Awards IIS-0331707, CNS-0403433, and CNS-0855060) and the Federal Emergency Management Agency (Fire Prevention and Safety Research Grant). Thanks to our first responders from the Orange County Fire Authority, UCI Environmental Health and Safety, LA County Fire Department, Newport Beach Fire Department, City of Anaheim Fire Department, and our first responder technology advisors. Thanks to our technology partners at Mesh Dynamics and Deltin Corporation for their work with our researchers and helping with our drills.

References

[1] L. Paradis and Q. Han, “A Data Collection Protocol for Real-time Sensor Applications,” Pervasive and Mobile Computing (PMC), Vol. 5, No. 1, 2009.

[2] M. G. Rubinstein, I. M. Moraes, Miguel Elias M. Campista, Luis Henrique M. K. Costa, and Otto Carlos M. B. Duarte, "A Survey on Wireless Ad Hoc Networks", IFIP International Federation for Information Processing Publisher, Springer Boston , Volume 211/2006.

[3] F. Ye and G. Zhong and S. Lu and L. Zhang, "GRAdient Broadcast: A Robust Data Delivery Protocol for Large Scale Sensor Networks", ACM WINET, Vol 11, 2003.

[4] Y. Sankarasubramaniam and O. B. Akan and I. F. Akyildiz, "ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks", Proceedings of ACM MobiHoc, Vol. 11, 2003.

[5] C. Wan and S. Eisenman and A. Campbell, "CODA: Congestion Detection and Avoidance in Sensor Networks", ACM SenSys, 2003.

[6] T. Clouqueur and K. K. Saluja and P. Ramanathan, “Fault tolerance in collaborative sensor networks for target detection", IEEE Transactions on Computers, Vol. 53, 2004.

[7] L. Paradis and Q. Han, “A Survey of Fault Management in Wireless Sensor Networks,” Journal of Networks and Systems Management, Vol. 15, No. 2, June 2007.

[8] S.-W. Yuk, M.-G. Kang, B.-C. Shin, and D.-H. Cho. “An adaptive redundancy control method for erasure-code based real-time data transmission over the Internet,” IEEE Transactionson on Multimedia, 3(3):366–374, Sep 2001.

[9] V. R. Gandikota, B. R. Tamma, and C. S. R. Murthy. “Adaptive FEC-based packet loss resilience scheme for supporting voice communication over ad hoc wireless networks. IEEE Transactions on Mobile Computing, 7(10):1184–1199, 2008.

[10] Bo Xing, Sharad Mehrotra and Nalini Venkatasubramanian "RADcast: Enabling Reliability Guarantees for Content Dissemination in AdHoc Networks", The 28th Conference on Computer Communications (IEEE INFOCOM 2009). April 19 - 25, 2009. Rio de Janeiro, Brazil.

[11] Wi-Fi Alliance : http://www.wi-fi.org/index.php.

[12] Zigbee Alliance: http://www.zigbee.org/.

[13] TinyOS, http://webs.cs.berkeley.edu/tos/.

[14] Responsphere, http://www.responsphere.org/.

[15] Gstreamer, http://gstreamer.freedesktop.org/.

[16] DTNRG, http://www.dtnrg.org/