# Bilateral Routing in Emergency Response Networks

Panayiotis Kolios*, Andreas Pitsillides†, Osnat Mokryn‡

***Abstract*—An emergency response networking scenario is considered, in which immediately after the strike of a disaster, mobile terminals autonomously form an ad-hoc network. Distress nodes, use this network to disseminate help-requests as a far outcry mechanism. In turn, and upon their arrival, emergency response units opt to gain access to the withstanding ad-hoc network in order to retrieve those disseminated help requests; invaluable information that would allow timely response to those distress nodes.**

**This work is concerned with Bilateral Routing, an algorithm that best meets the requirements and constraints for help-request dissemination and retrieval in emergency scenarios. A novel explore-and-exploit dissemination strategy is detailed that clearly outperforms traditional dissemination mechanisms. The strategy takes into account both centrality and battery power of each node, to increase survivability and allow for a subsequent detection of help-requests by response units. The latter, search through reachable network nodes to retrieve new and unattended help requests. Extensive numerical results illustrate the decisive applicability of Bilateral Routing in emergency response networking scenarios.**

***Index Terms*—Ad-hoc networks, Emergency Response Networking, Bilateral Routing, Survivability, Wireless Communications**

## I. Introduction

Life threatening or not, emergency situations are both unforeseeable and unwelcome. In best case scenarios their consequences are negligible, resulting in smooth recovery, while worst cases create devastating effects to life and the environment for extended periods of time [1]. Indicatively, Sandy, the latest hurricane to hit the U.S. east coast caused loss of life and massive destructions with multimillion financial estimates of damage. Gladly, though, the occurrence of such events is infrequent and their effects mitigated by the collective actions of the aftermath Emergency Response Units (ERUs) [2]. Nevertheless, when they do happen, obtaining situational awareness is of a primary concern to ERUs.

Wireless communications based on mobile ad-hoc networks have long be proposed to offer reconnaissance services in emergency situations, and a plethora of applications have been created to aid the ERUs' planning procedures. However, and even though numerous efforts have been made to promote the operation of ad-hoc networks, their proliferation in the field is rather sluggish; due mainly to their rather poor performance in several key operations. One such primary issue urging for a solution is a robust and efficient networking strategy, aimed at emergency response scenarios.

*†P. Kolios and A. Pitsillides are with the Network Research Laboratory of the University of Cyprus, e-mail:{panayiotis.kolios, andreas.pitsillides}@ucy.ac.cy

‡O. Mokryn is with the School of Computer Science, Tel Aviv Yaffo Academic College, e-mail:ossi@mta.ac.il

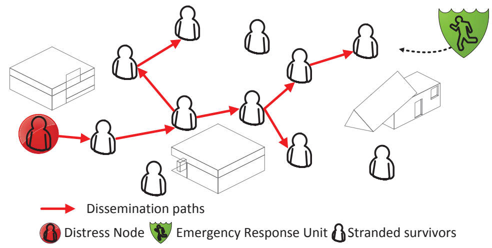



Fig. 1. Emergency Scenario

We consider here an emergency scenario in which a number of survivors are being trapped within a disaster area. These survivors are assumed to be in possession of a mobile device (most likely a featured-phone or a smartphone) which, by the time its cellular signal is lost, is able to automatically switch to ad-hoc mode and form an on-the-spot opportunistic network with others (offering services like those in HelpMe [3]).

Under these circumstances the primary concern of each individual is to be detected by the ERUs when they arrive. Hence, to assist in achieving that goal and by employing the network overlay, mobile devices spread their help requests across disjoint physical locations; an effort made to maximize their reachability and equally improve their detection probability.

The focal of this paper is thus in the design (within a mobile ad-hoc network) of an overlay routing and dissemination algorithm for help requests forwarding, in a manner that maximizes the survivability of the messages and the probability of their retrieval by ERUs, upon arrival.

This work first exemplifies the operation of a novel Emergency Response Network (ERN) formed in the aftermath of a catastrophic event where traditional networking infrastructure has been taken out of service. Within the ERN paradigm, a new routing algorithm is proposed, namely Bilateral Routing (BR), in which survivors disseminate help requests in the network to raise awareness of their situation. Initially, BR delegates help-requests to custodian nodes. Custodian nodes are chosen based on their attractiveness in terms of centrality within the network and own energy reserves. These nodes are responsible for maintaining the survivability of the help requests until rescue forces arrive. If in need, deranged custodian nodes (due, for example, to depletion of energy reserves) can activate BR once again to find a disciple. Upon arrival, ERUs attach to the ERN and look for help requests found within the network to kick-start their Search And Rescue (SAR) operations. The dissemination strategy followed by BR is described in detail in the sequel and subsequently its performance is compared to other solutions already proposed in the literature.

Figure 1 depicts the exemplified emergency setting in which several survivors have been stranded within an area. A distress node (e.g. marked distress node in the figure) generates help requests which then disseminate in the network to raise awareness of its situation (e.g. marked dissemination paths in the figure). Upon arrival to the scene, ERUs (e.g. marked emergency response unit in the figure) perform a search within the network to contact every available node. In this work, no optimized strategy is investigated for the ERUs operation. Instead the focus is placed on the request dissemination strategy. By obtaining help-requests stored at each terminal's repositories, ERUs will be in a better position to assess each and every situation and act upon that information.

Clearly it would be desirable for each generated request to be send out to every other terminal in the network to achieve maximum coverage. Such a dissemination strategy however, will most certainly aggressively deplete battery capacity of the inherently mobile terminals. Given that network survivability solely depends on the terminals' residual energy reserves, the aforementioned strategy is definitely a costly option. Moreover, with no knowledge on the arrival times of ERUs and the duration of ERUs' SAR operation, prolonging network survivability is, in fact, of utmost importance. Effectively, both competing objectives (i.e. help-request reachability and network survivability) should be maximized; the task being the matter of optimization within this work.

Our devised dissemination strategy, *Explore and Exploit*, being part of the overall BR solution is introduced in this paper. Simulation results show that our approach maximizes coverage in networks while optimizing for dense networks, to avoid redundant duplicates. More importantly, we are able to achieve the highest percentage of requests retrieval, even in very sparse topologies, indicating that this solution exhibits excellent performance in terms of survivability as well.

## II. Related Work

A number of emergency response networking solutions can be traced within the literature according to the degree of compromise of traditional communication infrastructure. At first, the work in [4] proposes the amalgamation between heterogeneous networking technologies to offer a robust solution of 100% availability. Wide and local area communication technologies are also discussed in [5] where resource priority is given to spontaneous emergency response participants. With partial operation of cellular networks after the strike of a disaster, the work in [6] details a communications service to deliver messages between stranded survivors and anyone outside the disaster area.

Within a similar setting, but only with connectivity offered to portions of the network, the work in [7]details how disconnected terminals can access the infrastructure via multihop relaying through neighboring terminals. The argument is that with only short multihop paths and with only a few terminals having direct access to base stations, significant improvements in service recovery can be provided. Our work however, considers neither full or partial operation of any deployed infrastructure. It solely depends on the ad-hoc network formed by stranded survivors and the arriving ERUs.

Departing from the realm of partial network coverage, the works in [8], [9] [10] also consider ad-hoc networking approaches; offering situational awareness, communication and coordination support and efficient information retrieval methods to emergency response units.

Delay-tolerant-networking (DTN) approaches have also been applied to the ERN scenario. The work in [11] considers how mobile relays operating in a store-carry and forwarding fashion that can link disconnected disaster-stricken areas. Priority routing in the former scenario is studied in [12] while in [13] asynchronous data exchange is considered where requests-response messages are routed through delegates of recurrent mobility patterns.

Noticeably, in all aforementioned studies the assumption is that the responder's location within the network is known. This is in fact an important assumption that is absent from the work present hereafter.

## III. Networking Architecture Modeling

The ERN scenario as outlined in section I above consists of two phases. In the first phase and just after the transient of a disaster, mobile terminals switch to ad-hoc mode and opt to build and maintain a network topology. Through this network, Help-Requesting Terminals (HRTs) disseminate help requests to selected other mobile terminals that act as custodians in an effort to improve HRTs' detection chances. In the second phase, ERUs approaching the affected area, access the ERN when found in the locality of mobile terminals and through them search the network for help-requests. Bilateral routing strives to achieve a balance between maximal HRTs' distress request detection and network survivability. Based on these premises, the ERN components operate as follows.

### *A. Mobile terminals energy-degree cardinality*

When in ad-hoc mode, mobile nodes operate in periodic on/off cycles to conserve energy. Similar to [14], the duty cycle of each node is determined solely by its own residual battery capacity. In this way, a node with less residual energy will be active for less and sleep for extended periods of time. Contrary, nodes with higher residual energy will remain active for increased time lengths and sleep for shorter periods of time. In active mode, a mobile terminal beacons its existence in the neighborhood and connections are established with those nodes that solicit communication. Beacons (similar to those used in the IEEE 802.11 standard, [15]) contain beacon intervals, a timestamp, node identification credentials and capabilities information; all of which are standardized data fields used for synchronized sniffing of neighboring nodes.

Let $\mathcal{N} = \{1, \ldots, N\}$ be the set of all stranded mobile terminals within the target emergency area. For each of these nodes, $0 \leq a(i) \leq 1$ indicates the fraction of active period in duty cycling and $1 - a(i)$ the sleep duration. The active duration is a function of the residual battery reserves, the fixed power consumption when in active standby/listening mode and when in transmit/receive mode. As in [14], the duty cycle can be dynamically adjusted to maximize lifetime. Nevertheless, this optimization is out of the scope of this work and thus a fixed value for $a(i)$ is used hereafter.

Further, let $\mathcal{Z}(i),\ i \in \mathcal{N}$ be the subset of direct (one-hop) neighbors of node $i$. Of course, the cardinality of $\mathcal{Z}(i)$ depends on the capabilities of the communications circuitry and the physical channel.

Then, the degree of a node $i \in \mathcal{N}$ is $\sum_{j\in\mathcal{Z}(i)} 1\ \ \forall i \in \mathcal{N}$, while connectivity is defined as:

$$c(i) = \gamma\, a(i) + (1-\gamma) \sum_{j\in\mathcal{Z}(i)} a(j)\ \ \forall i \in \mathcal{N} \tag{1}$$

where $\gamma$ provides a design tradeoff between the significance of one's own availability and that of its neighborhood.

The degree, as expressed above determines centrality in the network and in practice it is simply the sum of unique beacons heard by node $i$ while $a(i)$ used in (1) is obtained by monitoring the on/off intervals of beacons received. In turn, the connectivity metric expressed in (1) ranks nodes based on their own active duration, in addition to that of their neighbors. It thus, successfully merges the measure of centrality (indicating how well connected a node is in the network) and the availability of nodes in a neighborhood (indicating the extend of active duration). Importantly, both these measures can be obtained by each node separately without first establishing a connection with every other neighbor of node $i \in \mathcal{N}$.

### *B. Network dynamics*

As detailed earlier, and due to duty cycling, nodes are either active or inactive at any one instance in time. In fact, the only prerequisite is for duty cycles to conform to predetermined periodicity constrains such that any two neighboring nodes synchronize their active periods to be able to exchange messages in the network. Duty cycling, originally proposed within wireless sensor networks, has been well studied and so does synchronization (detailed above). However, due to duty cycling, a time-varying network topology is formed, in which only a portion of nodes are active at any one time. For instance, consider the exemplified scenario depicted in figure 1. By applying duty cycling, nodes switch on/off at will, altering the network topology. Figure 2a below illustrates three randomly chosen snapshots of the latter network realisation.

In effect, every stranded node is aware of its immediate neighbors but only communicates with them intermittently. Nevertheless, help-requests can be successfully propagated between nodes by probing one another when in active mode.

On the other hand, mobile response units being in constant movement only get a look of partial network topologies and thus are able to communicate with a subset of the terminals available at a particular instance in time. It is therefore important for help-requests to be propagated to those nodes that are 1) of high availability and 2) most certainly be highly connected, to ensure maximum network coverage. As detailed next, both these design principles are embedded within BR's basic operations for optimized performance.

### *C. BR operations: Explore and Exploit*

BR enables HRTs to communicate their needs in an efficient manner to custodian nodes, in a manner that prolongs the survivability and enables request detection when ERUs arrive.

**Dissemination** : A help-request is initially generated by a source terminal and then replicated to selected neighboring nodes. Those neighboring nodes that are now acting as custodians of that request, are in charge of storing the request or promoting it to better custodians. If better custodians are detected, the request is further forwarded to them.

Let us denote by $i \in \mathcal{N}$ either the source or a custodian of a help-request $e$. The BR algorithm for detecting and promoting neighboring nodes as possible forwarders is the following:

1) $i$ probes its neighboring nodes $\forall j \in \mathcal{Z}(i)$ for help-request dissemination. The probed request includes the tag $e$ that uniquely identifies the help-request.
2) In case $j$ has never heard $e$ broadcasted before, $j$ responds to $i$ and promotes itself as a candidate forwarding node; otherwise $j$ remains silent and exempts itself from $i$'s solicitation.
3) Node $i$ gathers replies and build a neighbor candidate list $\mathcal{H}(i)$ . The next custodian is then chosen from this list according to the following rule (2) :

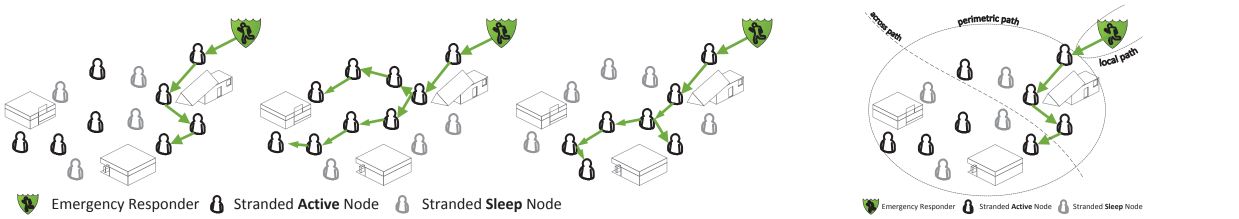
$$\arg\max_{j} \{c(j), j \in \mathcal{H}(i)\} \tag{2}$$

Specifically, probe requests and replies in steps 1) and 2), pursue an exploratory strategy where help-request copies are only forwarded towards regions that have not previously heard of the request. The exploration however is guided through well-connected nodes as indicated in step 3) where the single best-connected candidate is selected as the next custodian. In effect, the process strives to disseminate requests within the ERN but only though the best connected (higher-availability) nodes. For reference purposes (and for comparison with other schemes), the proposed dissemination strategy is hereafter called *Explore and Exploit* (EnE).

**Searching** : While on the move, ERUs are able to connect to the ERN through any of the active nodes and search for requests being deposited. Clearly, the stretch of searching is governed by the state of the instantaneous network topology which in turn affects which help-requests are being successfully discovered or missed.

Consider the dissemination operations of EnE detailed in steps 2)-3) above. Node $i$ probes its neighbors within $Z(i)$ and replies are received from the subset of neighbors that have not previously heard of the probed help-request $e$. From the built candidate list, a single node is selected as the next custodian. Clearly, when a new request is first generated by a source node $i$, every neighbor will respond to the solicit. The information overhead created by such a procedure closely resembles the overhead generated by the epidemic approach. However, subsequent probing for candidate custodians result to fewer replies and only by those nodes that have not heard of the specific help-request. As such, the communication overhead of EnE quickly diminishes, a feature that is absent in epidemic or any other basic flooding techniques.

In those optimized schemes, including spray-and-wait or spray-and-focus, that advertently constraint replication, probing is preconditioned to spread over a certain range and as such, the overhead is curbed to a fixed limit. Clearly though, this curbing greatly penalizes performance; a tradeoff better




(a) (b)

Fig. 2. The schematics in figure 2a illustrate random snapshots of the ERN, depicting the topological changes due to duty cycling of mobile terminals. Figure 2b illustrates probable SAR operations by ERUs.

addressed by EnE as shown in the sequel.

## IV. Numerical Results

To qualify the performance of EnE we conduct extensive simulation comparisons with the current state-of-the-art algorithms on a random network of various node densities. More specifically the network characteristics are as follows: The emergency region covers a circular area of diameter 2000m. Within this area, there are $N$ randomly placed stranded survivors, each in possession of a mobile device. These devices automatically build an ad-hoc network by connecting to their immediate neighbors as detailed below.

The maximum transmission range is set to $R = 400$m and the probability of link failure is modeled as $1 - \frac{log(R-d_{ij})}{log(R)}$ where $d_{ij}$ is the inter-node distance between $i, j \in \mathcal{N}$; capturing the distance-depended propagation losses.

In the results presented hereafter, a performance comparison is made between the following dissemination algorithms:

***Epidemic* [16]** : Every node exchanges help-requests with every one of its neighbors.

***Utility Flooding*** : Starting from the source node, help-requests are replicated to every neighboring node with utility higher than its predecessor. Connectivity, as detailed in (1), subsumes the role of the utility.

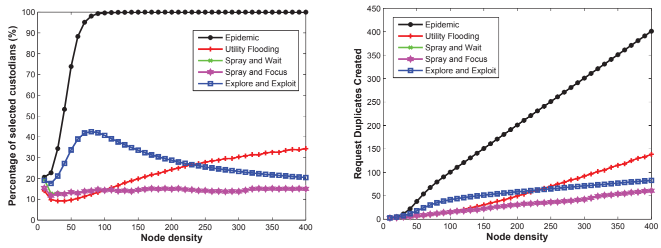
***Binary Spray and Wait (SAW)*[17]** : As the name suggests, SAW consists of the spraying and the wait phases. Initially $P$ tokens are created at the source. With every new connection established, the source or the custodian replicate the request and $\lfloor \frac{P}{2} \rfloor$ forwarding tokens are passed to the custodian until only 1 token is left at the source or the custodian. When only left with 1 token, the source and any custodians enter the waiting phase in anticipation of the arriving ERUs.

***Binary Spray and Focus (SAF)* [18]** : Similar to SAW, the spraying phase disseminates $P$ request replicas in the neighborhood of the source. However, the waiting phase whereby custodian withhold requests is replaced with the focusing phase where requests are forwarded to neighboring nodes with higher utility. As before, the utility being considered is the connectivity measure detailed in (1).

***Explore and Exploit (EnE)*** : EnE is discussed in detail in section III-C. In summary, starting from the source node, candidate custodians are those neighbors that have never heard of the probed help-request before. However, from the set candidates, the single best-connected individual is selected as the next custodian in every hop.

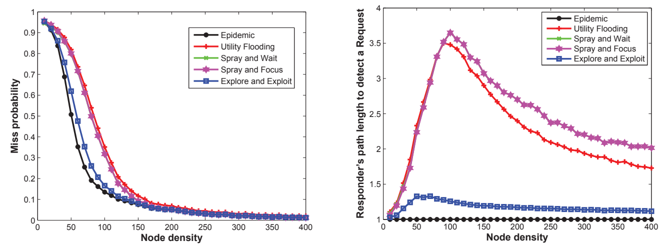
A single randomly selected stranded terminal is assumed to generate a help-request which is in turn disseminated in the network. For both SAW and SAF, the total number of tokens created is set to $P = 0.15 \times N$ (similar to [18]). For EnE $\gamma$ is simply set to 0.5.

An ERU appears at a random location and enters the network through the nearest active node found in range. We distinguish between three SAR operations as detailed in figure 2b where ERUs can only approach the emergency area from a specific location, or ERUs can only search the area perimetrically and alternatively ERUs can roam across the emergency area. However, due to space limitations the reported results are concerned only with the former case of access from a specific location. Nevertheless, the presented results resemble closely the performance for all three approaches identified.




(a) (b)

Fig. 3. Replication performance in terms of the total number of utilized nodes (fig. 3a) and the total number of generated replicas (fig. 3b).




(a) (b)

Fig. 4. Miss probability (fig.4a) and search stretch (fig. 4b) when SAR operations are confined to a specific location.

Figures 3 and 4 present results for the dissemination and recovery phase, respectively. Clearly, the more nodes acting as custodians the more energy is spent, yet the more likely it is that request are detected when ERUs arrive, and the less probability of missing requests. EnE trade-offs the two, while preserving energy.

Figure 3a first plots the percentage of nodes selected as custodians out of the total node population, for different node densities. Figure 3b plots the total number of help-request duplicates created in the network. Clearly, EnE involves the participation of a greater number of nodes compared to Utility Flooding, SAW and SAF for sparsely populated networks. In fact this is expected, since EnE tries to spread help-request copies over disjoint regions to improve coverage. Nevertheless, its diffusion is substantially lower than that of Epidemic. For an indicative node density of 75 nodes considered, only 40% of the nodes are involved in request dissemination while Epidemic spreads over all nodes (i.e. 100%). Noticeably, for node densities lower than the 75 mark, the network becomes more and more disconnected and thus all comparative strategies converge to a nominal value. Importantly though, and due to the mechanisms of EnE, for fully connected networks, an increased node density does not result in greater number of node participation. On the contrary, there is a curbing in the number of participating custodians as node density increases; clearly illustrated in the figure by the decreasing percentage of node participation for EnE. This result is also validate in plot 3b wherein the gradient of the EnE curve stabilizes to a small constant. This is opposed to the results obtained by all other strategies where request duplicates are monotonically increasing with node density at higher rates.

In effect, EnE manages to quickly diffuse help-request within the ERN to maximize coverage but sets back when such coverage is reached so that no unnecessary duplicates are forwarded.

The real benefits of EnE are presented in plot 4a of figure 4 where the probability of miss-detection of a help-request is drawn for varying node densities. Clearly, at a particular time of entry to the ERN, the responder uses a breadth-first search strategy to quickly discover all reachable nodes (and recover their request repositories) from the residual network. As such, the miss probability is defined as the probability of a request not being detected by an ERU due to the fact that the request source or custodian were not discovered. The cause of the latter miss-detection would either be due to the source/custodian being in energy-conserving sleep mode or due to unreachable nodes caused by network partitioning. Evidently, the proposed scheme closely follows the performance of Epidemic. Importantly, EnE greatly departs from the performance achieved by either Utility Flooding, SAW or SAF. Indicatively, for a density of 75 nodes, Epidemic provides an average miss-probability of approximately 0.1, EnE achieve double that value while all other comparative schemes approach a probability of 0.5. Importantly though, EnE approaches the performance of Epidemic having only utilized significantly less number of nodes (plot 3a) and with only a fraction of the duplicates made (plot 3b).

Looking into the search stretch made by ERUs to reach the desired help-requests as shown by plot 4b in figure 4, the improvements offered by EnE are also immediate. The latter scheme offers performance that closely resembles Epidemic where the help-requests are always 1-hop away from any reachable node. The difference of EnE is only marginal, as shown in the plot. All other schemes greatly depart from such an achievement.

## V. Conclusions

Bilateral Routing is detailed within this work, as a novel mechanism for help-request dissemination and detection in emergency response networks. BR discriminates between the latter two operations (i.e. dissemination and detection) where in each operation optimized strategies are followed. In the dissemination, EnE has been derived, a scheme that strives to achieve maximum network coverage but only through the fittest nodes (in terms of their residual energy). In detection, all reachable networked nodes are queried for unresolved help-request retrieval.

Performance comparisons illustrate most clearly the benefits of EnE in offering excellent support for emergency response services. Both the miss detection probability and help-request search stretch in EnE resemble the performance of Epidemic while EnE's replication performance follows closely more conservative schemes including Utility Flooding and SAF.

## References


[1] G. Phillip and R. Hodge, *Disaster area architecture: telecommunications support to disaster response and recovery*, IEEE Military Communications Conference, Vol. 2, Page(s): 833 - 837, Nov. 1995.

[2] R.E. Krock, *Lack of emergency recovery planning is a disaster waiting to happen*, IEEE Communications Magazine, Vol. 49, No. 1, Page(s):48 - 51, Jan. 2011.

[3] O. Mokryn, D. Karmi, A. Elkayam and T. Teller, *Help Me: Opportunistic Smart Rescue Application and System*, Mediterranean Ad Hoc Networking Workshop, June 2012.

[4] N. Uchida, K. Takahata, Y. Shibata and N. Shiratori, *Never Die Network Extended with Cognitive Wireless Network for Disaster Information System*, International Conference on Complex, Intelligent, and Software Intensive Systems, Page(s): 24 - 31, June 2011.

[5] L.R. Carley, M.K. Carley, *Social Network Aware Routing and Prefetching on Dual-Mode Wireless Networks*, IEEE Globecom Workshop on Complex and Communication Networks, Dec. 2010.

[6] K. Mase, *How to Deliver Your Message from/to a Disaster Area*, IEEE Communications Magazine, Vol. 49, No. 1, Page(s):52 - 57, Jan. 2011.

[7] G. Chen, A. Hu and T. Sato, *A scheme for Disaster Recovery in Wireless Networks with Dybamic ad-hoc routing*, ITU-T Kaleidoscope: Beyond the Internet? - Innovations for Future Networks and Services, Dec. 2010.

[8] S.M. George, W. Zhou, H. Chenji, W. Myounggyu, Y.O. Lee, A. Pazarloglou, R. Stoleru and P. Barooah, *DistressNet: A Wireless Ad Hoc and Sensor Network Architecture for Situation Management in Disaster Response*, IEEE Communications Magazine, Vol. 48, No. 3, Page(s):128 - 136, Mar. 2010.

[9] J. Mocito, L. Rodrigues and H. Miranda, *Communication and Coordination Support in Ad Hoc Networks for Emergency Management Scenarios*, International Wireless Communications and Mobile Computing Conference, Page(s):499 - 503, June 2010.

[10] G. Zussman and A. Segall, *Energy efficient routing in ad hoc disaster recovery networks*, Ad Hoc Networks, Vol. 1, No. 4, Page(s):405 421, Nov. 2003.

[11] Y. Sasaki and Y. Shibata, *A Disaster Information Sharing Method by The Mobile Servers in Challenged Networks*, International Conference on Advanced Information Networking and Applications Workshops, Page(s):1048 - 1053, Mar. 2012.

[12] J. Inwhee and K. Sang-Bo, *A Message Priority Routing Protocol for Delay Tolerant Networks (DTN) in Disaster Areas*, International Conference on Future Generation Information Technology, Page(s):727 - 737, Dec. 2010.

[13] C.E.Palazzi and A. Bujari, *Social-Aware Delay Tolerant Networking for Mobile-to-Mobile File Sharing*, International Journal of Communication Systems, Vol. 25, No. 10, Pages:1281 - 1299, Oct. 2012.

[14] A. Kansal, J. Hsu, S. Zahedi and M.B. Srivastava, *Power Management in Energy Harvesting Sensor Networks*, ACM Transactions on Embedded Computing Systems (TECS) - Special Section LCTES'05, Vol. 6, No. 4, Art. 32, Sept. 2007.

[15] B. O'Hara and A. Petrick, *IEEE 802.11 Handbook:A Designer's Companion*, Wiley-IEEE Standards Association, Mar. 2005.

[16] A. Vahdat and D. Becker, *Epidemic routing for partially connected ad hoc networks*, Technical Report CS-200006, Duke University, July 2000.

[17] T. Spyropoulos, K. Psounis, and C.S. Raghavendra, *Spray and wait: Efficient routing in intermittently connected mobile networks*, ACM SIGCOMM workshop on Delay Tolerant Networking, Aug. 2005.

[18] T. Spyropoulos, K. Psounis and C.S. Raghavendra, *Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility*, IEEE International Conference on Pervasive Computing and Communications Workshops, Page(s):79 - 85, Mar. 2007.