Wireless Networks in Emergency Management

Erol Gelenbe
Intelligent Systems & Networks Group
Dept. of Electrical & Electronic Engineering
Imperial College, London SW7 2AZ, UK
e.gelenbe@imperial.ac.uk

Gokce Gorbil
Intelligent Systems & Networks Group
Dept. of Electrical & Electronic Engineering
Imperial College, London SW7 2AZ, UK
g.gorbil@imperial.ac.uk

ABSTRACT

Emergencies of different types, ranging from accidents to natural disasters, are unfortunately becoming increasingly common due to the greater concentration of human populations and the existence of highly interconnected physical infrastructures that human beings increasingly rely on. Thus Emergency Management Systems are gaining in importance and they are a major and useful example of Cyber-Physical Systems where ICT, sensing and decision making come together to improve the outcomes for human beings and for nature itself. Our presentation focuses on the impact of wireless sensing, distributed decision making, and opportunistic wireless communications as tools for optimising human evacuation and improving the health outcomes for human populations during small or large scale emergencies.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*store and forward networks, wireless communication*; I.6.3 [**Simulation and Modeling**]: Applications; H.4.3 [**Information Systems Applications**]: Communications Applications

General Terms

Reliability, Performance, Experimentation

Keywords

Opportunistic communications, delay tolerant network, disaster management, building evacuation, emergency navigation.

1. INTRODUCTION

Evacuation is an urgent and important component of emergency response that requires spatio-temporal decisions to improve the outcomes for the human beings that are affected [16]. Classical problems related to large scale distributed systems, including the unknown impact of the event, incomplete and incorrect information on the situation [10], and distributed inconsistent state information [11], as well as specific issues such as the dynamical evolution of the emergency (such as a spreading hazard) and destroyed and inaccessible communication infrastructure, introduce significant challenges for a reliable and safe evacuation. The distributed decision processes themselves, including the allocation of emergency teams and supporting mobile units, are also particularly challenging [13–15].

This paper considers an approach to resilient emergency support systems (ESS) to provide evacuation support to aid human beings with the help of opportunistic communications (oppnets) [21], where pocket wireless devices can help people disseminate information and receive on the emergency so as to offer back-up communications and improve resilience. Using shared local information, each device maintains a partially updated view of the environment and provides alerts and adaptive navigation directions to its user for evacuation purposes. In this paper, we evaluate the resilience of such a system consider the effect of device failures on evacuation and communication performance.

Oppnets or delay tolerant networks have been studied extensively [4], and some work has addressed its application in emergency scenarios. Bruno et al. [1] propose that oppcomms can be used to increase the resilience of an existing communication infrastructure to enable emergency management services. They suggest that the greatest benefit of oppnets would be as a "glue" that binds together existing infrastructure that has survived the disaster, although oppnets alone are viewed to be able to provide at least some form of emergency communication. Oppcomms between mobile phones are proposed to provide adaptive emergency communications when existing cellular infrastructure has been destroyed in [20]. The authors remark that DTNs can enable information flow from civilians to emergency responders, similar to urban sensing applications, or from responders to civilians, as in alerting applications. Their work focuses on the practical issues of implementation of DTN protocols on Android smartphones. Another work that considers how oppnets formed by smartphones in the absence of cellular infrastructure can be used for the dissemination of emergency messages is [24] where generic one-way communications between a mobile source node and a mobile or fixed destination node is proposed with a modified epidemic routing protocol.

The work discussed above does not evaluate the effect of communication failures, either of the mobile devices or of the existing infrastructure. Camara et al. present an evaluation

PINGEN'12, August 26, 2012, Istanbul, Turkey.

of the effect of failures on communication performance of a DTN-based emergency notification system in [2], and propose a DTN-based emergency alert system that consists of fixed nodes called road-side units (RSUs) distributed within a road network and vehicles equipped with wireless devices. RSUs are connected to a central emergency management system (e.g. via satellite communication) and are used to send emergency alert messages from the center to all vehicles in the emergency area. Inter-vehicle communications are used to increase coverage and speed up the distribution of these messages. The authors consider the failure of RSUs in two scenarios: (i) natural disasters, where some of the RSUs fail at once due to the disaster, and (ii) deliberate attacks on the system, where RSUs are assumed to fail gradually and at random.

The work presented here builds upon previous work [6,7, 18,19]. Oppcomms were first suggested in this context to enable emergency evacuation support and evaluated the effect of parameters such as node density and communication range on evacuation and communication performance in [19], and compared with the performance of ESS with a scheme [5] that uses local communications between fixed nodes [18]. Using ESS as a back-up evacuation system in case of failures of existing systems is discussed in [6]. Thus the work presented here furthers research on the use of oppcomms for emergency support by evaluating the effect of node failures on system performance.

1.1 The system that is considered in this work

Our proposed emergency support system is targeted for densely populated urban areas and it can be deployed in both outdoor and indoor environments. In this paper, we describe ESS as deployed in a large multi-floor building. The spatial configuration of the emergency area is important for evacuation. We represent the physical area as a graph $G(V, E)$: vertices V are locations where civilians can congregate, such as rooms, corridors and doorways, and edges E are physical paths that civilians can use to move inside the building. Multiple costs are associated with each edge $(i, j) \in E$:

- the edge length $l(i, j)$, which is the physical distance between the vertices;
- the hazard level $h(i, j)$, which represents the condition of the edge in relation to its danger level for evacuation; and
- the effective edge length $L(i, j) = l(i, j) \cdot h(i, j)$, which is a joint metric representing the total cost of an edge for evacuation, including hazard and physical distance.

In our evaluation, we assume that $h(i, j)$ is the hazard intensity along the edge. The range of h can be defined based on the measured qualities of the hazard, such as temperature, light intensity, and CO_2 level. In our simulations, we use nine discrete levels to describe the hazard intensity:

$$H = \begin{cases} 1 & k = 0 \text{ (no fire on edge)} \\ k \cdot 10^3 & k = \{1, 2, \ldots, 8\} \end{cases}$$

The graph is assumed known for a building, and there are **sensor nodes (SNs)** installed at fixed positions in the building, where each SN monitors its immediate environment for a hazard. A sensor can potentially monitor multiple edges in the building graph based on its sensing capabilities and location. In our simulations, we assume that each SN monitors a single edge. Each SN is battery powered and has a unique device ID, a location tag that represents the area (i.e. edge) monitored by the sensor, and short-range wireless communication capability. When requested, an SN sends its latest measurement for its edge (i.e. its $h(i, j)$ value).

Since SNs do not need to perform complicated computational tasks, their design can be kept very simple, with little memory and low processing power for cheap production. SNs are self-powered for a variety of reasons, including but not limited to: low installation cost, ease of installation and maintenance, and resilience to power outages. Since SNs are designed as "deploy and forget" devices, meaning their maintenance will be infrequent, their energy use should be kept low. This is achieved by operating them in a sleep-duty cycle in non-emergency conditions and using very low transmission power for communications.

2. EMERGENCY SUPPORT SYSTEM (ESS)

The emergency support system (ESS) consists of **mobile communication nodes (CNs)** carried by civilians. Each CN is a simple pocket device with short-range wireless communication capability, a processor and local storage. CNs form an opportunistic network that exploits node mobility to communicate over multiple hops. Such opportunistic communications (oppcomms) are characterized by the "store-carry-forward" paradigm [21] where messages received by a CN are stored in local memory and carried with the CN as a result of human mobility. Messages stored on behalf of others are then forwarded to other CNs as they come into contact. Thus, a message is delivered to its destination via successive opportunistic contacts. Because the opportunistic network (oppnet) can be disconnected for long periods of time, CNs may need to carry messages for long durations and delivery of messages is not guaranteed.

Oppcomms are used to disseminate hazard information among CNs in the form of **emergency messages (EMs)**. Hazard information is generated by sensor nodes (SNs) deployed in the building as described above. Each significant hazard measurement is stored in a new **measurement message (MM)** created by the SN monitoring the affected area (e.g. edge). An MM contains the source ID (SN ID), location information (edge ID or (i, j)), the hazard intensity $h(i, j)$, and measurement timestamp. The latest MM created by an SN is forwarded to any CN that comes in contact with the SN. When an MM is received by a CN, it is used to update the local view of the CN as discussed below. The MM is also translated into an EM that contains the source ID (CN ID) and information from the MM (intensity, edge (i, j), timestamp). Multiple MMs are combined into a single EM when possible. In contrast to MMs, which are sent from SNs to CNs via single-hop communications, EMs are sent from CNs to CNs over multiple hops using oppcomms. Each EM is destined for all CNs.

The first MM or EM received by a CN acts as an alarm, indicating that there is a hazard and the user of the CN should evacuate the building. Each CN stores the building graph in local storage and uses received MMs and EMs to update edge costs on its local graph. An update triggers the calculation of shortest paths from the current CN location to all building exits, and the path with the lowest cost is used as an evacuation path. Any shortest path (SP) algorithm can potentially be used; CNs employ Dijkstra's SP algorithm. Since effective edge lengths ($L(i, j)$ values) are used in SP calculation, the "shortest" path minimizes exposure to the hazard while also minimizing travel distance, with priority given to the safety of the civilian.

A CN uses the latest evacuation path it has calculated to provide step-by-step directions to its user. In order to do this, the CN needs to know its location in the building. Indoor localization is achieved using the fixed SNs: each SN contains a location tag; we use the edge ID (i, j) monitored by the SN in this implementation as the SN location tag. Once notified of the emergency, each CN periodically sends a **beacon** using local broadcast. SNs that receive this beacon reply with a **localization message (LM)** that contains the source ID, location tag and timestamp. Very accurate localization is not required since the location of CNs are approximated by the graph vertices. The short communication range of CNs and SNs also decreases localization error. The location of a CN is updated as it moves in the building via LMs, and at each location update the CN updates the directions given to its user based on its current location and evacuation path.

CNs use epidemic routing [23] for the dissemination of EMs, coupled with *timestamp-priority queues*, where EMs with the earliest creation timestamps are dropped from the queue when it is full. Although epidemic routing is an early oppnet routing protocol, our evaluations [19] have shown that it is very suitable for emergency support due to its flooding based approach. Epidemic routing is known to have high message delivery ratios and low message latencies at the cost of high communication overhead [22]. However, communication overhead due to flooding does not seem to be applicable to ESS since each EM is targeted for all CNs, and good communication performance is desirable for emergency communications.

3. RESILIENCE OF OPPORTUNISTIC COMMUNICATIONS

Resilience of an emergency support system is an important property considering the critical nature of its application. Through the use of mobile devices and oppcomms, ESS operates independently of existing communication infrastructure. However, ESS is still susceptible to failures of its components. Our general intuition is that ESS would be quite resilient to failures due to the disruption tolerant nature of oppcomms. Our aim in this paper is to verify this view by evaluating the effect of node failures on evacuation and communication performance of ESS.

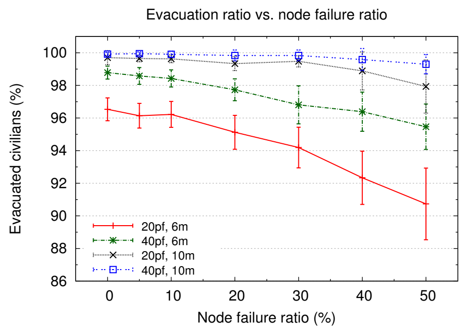
We have evaluated the resilience of ESS to CN failures with simulation experiments conducted with the Distributed Building Evacuation Simulator (DBES) [3]. We use a three-floor building model based on the EEE building at Imperial in our simulations. The ground floor is 24m x 45m and contains the two exits, the 2nd and 3rd floors are 24m x 60m. We simulate a spreading fire and associated effects such as smoke. The fire starts at the intersection of two corridors on the second floor near the staircases, and probabilistically spreads in the area along edges following a Bernoulli trial model and affects the health of civilians on adjacent vertices. Each civilian starts with a health of 100 and her health decreases as she is exposed to effects of the hazard. For each simulation, people initially start at random locations in the building following a uniform distribution on vertices. Civilians follow a probabilistic mobility model intended to simulate the movement of people during working hours when they are not evacuating. When a civilian is notified of the emergency, she follows directions provided by her CN to evacuate. Civilians move at 1.39 m/sec within floors and 0.7 m/sec at staircases. Simulations take physical congestion into account during civilian movement.

In these simulations, we assume that traditional means of communication have broken down, possibly due to the hazard. We assume that CNs cannot communicate when they are located on different floors; this may be due to physical factors that affect wireless signal strength, such as thickness of the inter-floor walls. We also assume there is no central alarm in the building (e.g. it has failed due to power failure). Therefore, ESS provides both alerting and navigation services to building occupants. All communication entities (CNs and SNs) are simulated as IEEE 802.15.4-2006 compliant devices. CN and SN data transfer rate is set to 100 kbits/sec and 20 kbits/sec, respectively. We do not explicitly simulate the PHY layer in our simulations, but we do take into account contention for the wireless medium as accessed through CSMA-CA (carrier sense multiple access with collision avoidance). CN communication range is assumed to be either 6m or 10m; SN communication range is 5m. These ranges have been chosen based on expected indoor communication range of 802.15.4 devices that transmit at 0 dB or less. In addition to the area graph and edge costs, each CN can store 100 EMs. Messages used by ESS are very short, with most message types $\leq$ 16 bytes. EMs have an average length of 52 bytes; this means that average storage requirements for oppcomms is about 5 kB per CN.

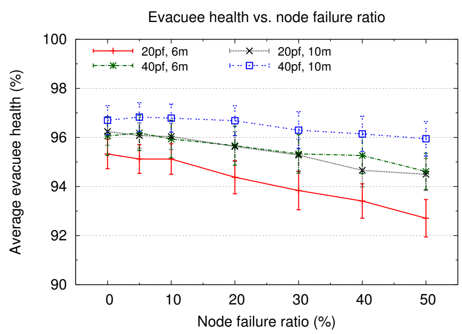
We assume that some of the CNs have failed before the emergency starts, most probably due to battery depletion. We look at four different cases in our evaluation: 20 and 40 people per floor (pf) with CN ranges of 6m and 10m. These cases allow us to evaluate the effect of CN failures in different population densities (medium and high) and with different CN ranges. Simulation results are an average of 50 simulation runs for each data point, and 95% confidence intervals are provided. Each simulation run has different initial locations for people, mobility patterns, hazard spread pattern, and CNs randomly chosen as the failed nodes. In order to isolate the effect of evacuation strategy used by users of failed CNs, we present our results where data relating to such users have been removed. In practice, such users can follow a static evacuation strategy or follow people with functional CNs.

3.1 Simulation Results

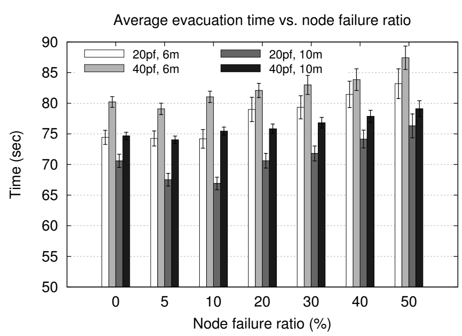
We see that the evacuation ratio (Fig. 1a) is less affected by failures when nodes have more frequent contact opportunities and when the connected subnetwork sizes are larger, i.e. when population density and/or communication range is high. For example, with 40pf and 10m range, evacuation ratio is practically unaffected by failures. The effect of failures on the evacuation ratio increases as population density and/or communication range decreases. With more failures in the system, the evacuation ratio decreases in general. We see that the ESS is fairly resilient to node failures in terms of the evacuation ratio and that failure ratios of up to 20% are well-tolerated. An important observation is that communication range has a greater effect on the resilience of ESS than population density. Average evacuee health (Fig. 1b) is generally quite high despite the failures. A general trend



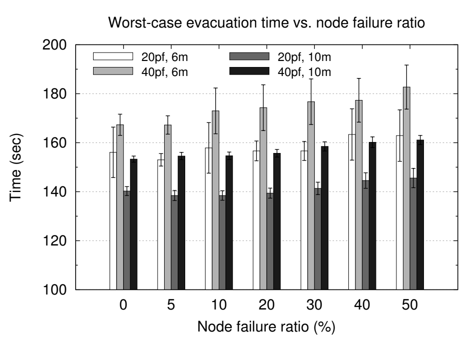
(a) Evacuation ratio



(b) Average evacuee health



(c) Average evacuation time



(d) Worst-case evacuation time

Figure 1: Effect of node failures on evacuation performance

of decreasing health is observed as failures increase but the differences in average health are very small. We again observe that networks with better connectivity (higher density or range) are more resilient and less affected by failures.

Figures 1c and 1d present average and worst-case evacuation times[1] versus the node failure ratio. Our results show that the evacuation times increase as the failure ratio increases, except for the case where we have 20pf with 10m range, which shows a decreasing average evacuation time until 10% failure ratio. The effect of failures on the evacuation time result from two factors: (i) with more failures, people are alerted later about the fire and therefore start to evacuate later, and (ii) more people need to modify their paths during the evacuation because of incomplete or outdated information, which both result in an increase in the evacuation times.

Figure 2 presents how node failures affect communication performance in ESS; these metrics are calculated using EMs only. We see that message delivery ratio (Fig. 2a) decreases as failures increase due to fewer contact opportunities. These results show that oppnets are in general more resilient to node failures than wireless networks that require end-to-end connectivity for message delivery. We observe that communication range is more effective at maintaining high delivery ratio in the face of node failures than node density. Similar behavior is observed for average message delivery delay in Fig. 2b. We observe that average message delay increases with failure ratio, with the exception of the (20pf, 6m) scenario, which does not show any significant change, but the increase is less when communication range is high (i.e. 10m). The increase in delay is more noticeable for the high density, medium range (40pf, 6m) scenario than others.

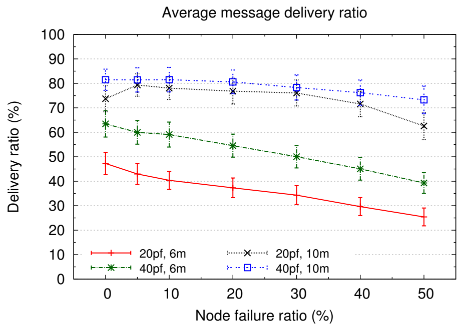
Both average message hop count (Fig. 2c) and average queue length[2] (Fig. 2d) show similar trends with increasing node failures. For both metrics, we see that results are grouped based on population density and that range has less effect than density as opposed to our previous observations with other metrics. We observe considerable decrease in both hop count and queue length as failures increase. Hop count and message delay are loosely related in oppnets due to the "store-carry-forward" message dissemination paradigm. A low hop count does not always mean a low delay since end-to-end delivery delay can be dominated by storage delay. This behavior is observed in our results: although increasing failures noticeably decreases hop count, delay increases. Hop count and queue length decrease as the number of failed nodes increases, mostly because there are fewer CNs to relay and receive messages and therefore messages reach fewer CNs.

4. CONCLUSIONS AND FUTURE WORK

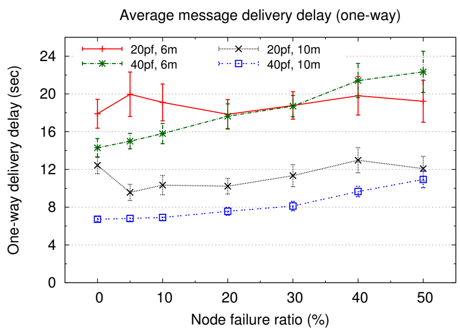
We have described an ESS that employs opportunistic communications between pocket devices carried by people to disseminate emergency messages. Each CN provides alerts and navigation directions to its user for evacuation based on

[1]The average evacuation time is the mean of the evacuation times of all successfully evacuated civilians. The worst-case evacuation time is the evacuation time of the last person to leave the building.

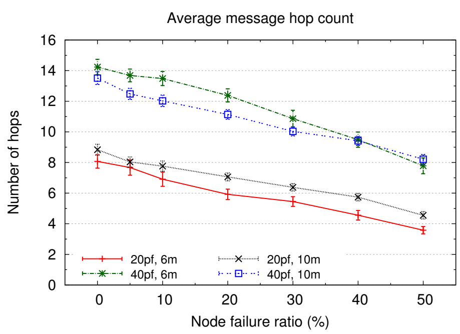
[2]Queue length is the number of EMs stored and carried by a CN for oppcomms. In ESS, CNs do not forget (drop) messages so the queue length increases monotonically until the queue is full. Average queue length is the mean of the maximum queue lengths of all CNs.



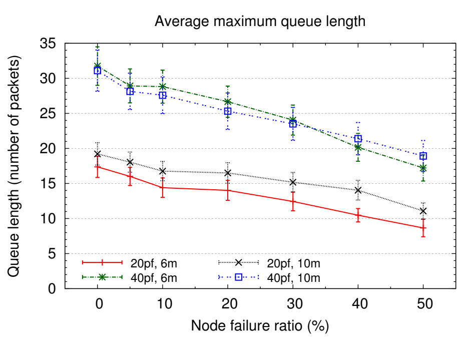
(a) Delivery ratio



(b) Average delay



(c) Average hop count



(d) Average maximum queue length

Figure 2: Effect of node failures on communication performance

its local view, which is updated via oppcomms. In indoor urban areas, fixed sensor nodes (SNs) are used to monitor the environment in real-time and for indoor localization of CNs. Due to the use of oppcomms, The ESS is highly resilient and can operate when other means of communication have broken down. ESS easily handles intermittent connectivity, link failures and node mobility. In this paper, we evaluated the resilience of ESS and oppcomms to node failures. Our simulation results have shown that ESS tolerates CN failures well, especially when connectivity is high. As CN communication range or the number of nodes in the area decreases, both network connectivity and resilience to failures decrease.

Our results indicate that communication range has a greater effect on the resilience of ESS than node density. This suggests that the dynamic adjustment of communication range can be an effective method to improve resilience against node failures, and we will investigate this approach in future work. In addition to node failures, we should consider deliberate attacks on the network, and we will further investigate the effect of network attacks in the context of emergency support in future work. Many of the problems that we have discussed would also benefit from a probability analysis as has been traditional in communication systems and other areas of information systems engineering [12]. Furthermore, techniques such as CPN [8,9,17] that adaptively route the packets of a network can both benefit oppcomms, while they have also also proved useful in guiding the evacuees. These aspects too will be included in future work.

5. REFERENCES

[1] R. Bruno, M. Conti, and A. Passarella. Opportunistic networking overlays for ICT services in crisis management. In *Proc. 5th Int. ISCRAM Conference*, pages 689–701, May 2008.

[2] D. Camara, C. Bonnet, and F. Filali. Propagation of public safety warning messages: A delay tolerant network approach. In *Proc. 2010 IEEE Wireless Communications and Networking Conference*, pages 1–6, April 2010.

[3] N. Dimakis, A. Filippoupolitis, and E. Gelenbe. Distributed building evacuation simulator for smart emergency management. *The Computer Journal*, 53(9):1384–1400, 2010.

[4] K. Fall. A delay-tolerant network architecture for challenged internets. In *Proc. 2003 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 27–34. ACM, 2003.

[5] A. Filippoupolitis and E. Gelenbe. A distributed decision support system for building evacuation. In *Proc. 2nd IEEE Int. Conf. on Human System Interaction*, pages 323–330, May 2009.

[6] A. Filippoupolitis, G. Gorbil, and E. Gelenbe. Autonomous navigation systems for emergency management in buildings. In *Proc. 2011 IEEE GLOBECOM Workshops*, pages 1056–1061, December 2011.

[7] A. Filippoupolitis, L. Hey, G. Loukas, E. Gelenbe, and S. Timotheou. Emergency response simulation using wireless sensor networks. In *Int'l Conf. Ambient Media and Systems*, pages 21:1–21:7, 2008.

[8] E. Gelenbe. Cognitive packet network (CPN). U.S. Patent 6,804,201, October 2004.

[9] E. Gelenbe. Steps towards self-aware networks. *Communications of the ACM*, 52(7):66–75, July 2009.

[10] E. Gelenbe and G. Hébrail. A probability model of uncertainty in databases. In *ICDE*, pages 328–333. IEEE Computer Society, 1986.

[11] E. Gelenbe and K. C. Sevcik. Analysis of update synchronisation algorithms for multiple copy data bases. *IEEE Transactions on Computers*, C-28(10):737–747, October 1979.

[12] E. Gelenbe and A. Stafylopatis. Global behavior of homogeneous random neural systems. *Applied Mathematical Modelling*, 15(10):534–541, October 1991.

[13] E. Gelenbe, S. Timotheou, and D. Nicholson. Fast distributed near-optimum assignment of assets to tasks. *The Computer Journal*, 53(9):1360–1369, 2010.

[14] E. Gelenbe, S. Timotheou, and D. Nicholson. A random neural network approach to an assets to tasks assignment problem. In *SPIE Symp. Defence, Security and Sensing, Track of Signal Processing, Sensor Fusion, and Target Recognition XIX*, page 76970Q, 2010.

[15] E. Gelenbe, S. Timotheou, and D. Nicholson. Random neural network for emergency management. In *The Workshop on Grand Challenges in Modeling, Simulation and Analysis for Homeland Security*, 2010.

[16] E. Gelenbe and F.-J. Wu. Large scale simulation for human evacuation and rescue. *Computers and Mathematics with Applications, Accepted for publication*, 2012.

[17] E. Gelenbe, Z. Xu, and E. Seref. Cognitive packet networks. In *ICTAI*, pages 47–54, 1999.

[18] G. Gorbil, A. Filippoupolitis, and E. Gelenbe. Intelligent navigation systems for building evacuation. In *Computer and Information Sciences II*, Lecture Notes in Electrical Engineering, pages 339–345. Springer London, 2012.

[19] G. Gorbil and E. Gelenbe. Opportunistic communications for emergency support systems. *Procedia Computer Science*, 5(0):39–47, 2011.

[20] P. Jiang, J. Bigham, and E. Bodanese. Adaptive service provisioning for emergency communications with DTN. In *Proc. 2011 IEEE Wireless Communications and Networking Conference*, pages 2125–2130, March 2011.

[21] L. Pelusi, A. Passarella, and M. Conti. Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks. *IEEE Communications Magazine*, 44(11):134–141, November 2006.

[22] L. Song and D. F. Kotz. Evaluating opportunistic routing protocols with large realistic contact traces. In *Proc. 2nd ACM Workshop on Challenged Networks*, pages 35–42. ACM, 2007.

[23] A. Vahdat and D. Becker. Epidemic routing for partially-connected ad hoc networks. Tech. Report CS-2000-06, Duke University, Dept. of Computer Science, April 2000.

[24] X. Wu, M. Mazurowski, Z. Chen, and N. Meratnia. Emergency message dissemination system for smartphones during natural disasters. In *Proc. 11th Int. Conf. on ITS Telecommunications*, pages 258–263, August 2011.