Emergency Cyber-Physical-Human Systems

Erol Gelenbe, *FIEEE* and Gökçe Görbil
Department of Electrical & Electronic Eng.
Imperial College London, SW1P 4AZ, UK
Email: {e.gelenbe, g.gorbil}@imperial.ac.uk

Fang-Jing Wu
Nanyang Technological University
Singapore
f.wu@ntu.edu.sg

Abstract

Emergency management systems (EMS) are important and complex examples of Cyber-Physical-Human systems that are deployed so as to optimise the outcome of an emergency from a human perspective. They use sensor networks, networked decision nodes and communications with evacuees and first responders to optimise the overall Quality of Service to benefit primarily human beings in terms of survival, health and safety, and the the protection of nature, property and valuable infrastructures. The use of technology for emergency management also has side effects in terms of failures and malicious attacks of the ICT system, so that the outcome will be affected by how well the ICT system operates under stress. Thus this paper surveys research on wireless sensor-assisted EMS, including networking, distributed control, and knowledge discovery. An evaluation of increased effectiveness and liabilities that wireless communications introduce is conducted when adversaries exacerbate the emergency by malicious attacks through the wireless system.

1. Introduction and Vision

Cyber-technical systems exploit wireless technologies, sensing, and distributed decision making and control, at the confluence of ubiquitous computing, networking technologies, and wireless sensor networks (WSNs). This paper focuses on a class of such systems, the Emergency Management Systems (EMS) that enable intelligent and fast response to emergencies such as fires, earthquakes, or terrorist attacks. Emergency response has motivated considerable research in communications, information acquirement and dissemination, knowledge discovery, resource allocation and management, heterogeneous system integration and asynchronous control. The key functionality of EMS is to find safe paths for evacuees and to navigatw them towards safety in a timely fashion. Thus we will start our survey with this aspect and detail the role of sensing and communications within this scope. Then we will consider simulation tools that have been developed specifically for EMS, often as a way to provide predictive guidance for decision making. Finally we will address the issue of the breakdown in communication networks during an emergency, and discuss the use of opportunistic communications (Oppcomms) as an alternative that requires a limited infrastructure. Potential attacks on Opcomms during and emergency, and defense techniques will be discussed. Their impact will then be briefly evaluated using simulations with regard to the outcome of human evacuation and safety. Finally we offer a few conclusions.

2. Distributed Evacuation Systems

The physical architecture related to sensing, communications and decision making, and the distributed structure intrinsic to the evacuees and the first-responders, naturally leads to a distributed design for emergency management systems. Such systems can be structured in a two-tiered architecture composed of a distributed decision system and a sensing system. The upper-tier distributed decision system is a middleware that connects the sensing clients and the user clients. Note that all sensor nodes do not form a connected WSN and are only responsible for reporting in-situ and real-time information to the decision system. In [10] the sensing component is composed of a set of sensor nodes, while the decision component is composed of a set of lightweight decision nodes (DNs), inspired from adaptive QoS-aware algorithms for packet routing [22], [13] that use the Random Neural Network [2], [15]. The idea is to replace the ”packet” in a network by an ”evacuee”, the QoS in the packet network is replaced by a measure combining delay to the safe exit and the safety of the path, and the DNs play

978-1-4673-1544-9/12/$31.00 ©2012 IEEE

the role of routers for the evacuees. For a recent survey of experimental results concerning QoS-aware routing algorithms in packet networks see [14]. To make this scheme workable in an evacuation scenario, each evacuee is equipped with a user portable device (e.g., a smart phone) which communicates with the DNs directions. The potential paths that evacuees can follow in the physical system mimic the paths in the network, and the DNs are physically placed at decision points of an undirected graph which represents the displacements that evacuees can make as they move in the building. The work in [11] extends [10] to more realistic emergency scenarios, where the hazard intensity reported by each sensor aggregates its own value with that of neighboring sensors. However DNs may fail or be destroyed during an emergency, so that in [25] *opportunistic communications* are suggested for the design an elastic evacuation system, where a set of mobile decision nodes (MDN) that are carried by the evacuees and possibly by emergency personnel are used to complement or partially replace the DNs. Each MDN maintains a navigation graph [10]. The work in [23] considers a *hybrid decision component*, where both static decision nodes and mobile decision nodes may coexist for increased reliability. In [27], the concept of functional separation is adapted to partitioning the sensing system into two sensing units, the *emergency sensing unit* and the *position sensing unit*. In [30], a WSN is adopted to monitor hazards in the environment, and only one exit is assumed. Each user is equipped with a sensor node to communicate with the WSN for requesting an emergency evacuation path to the exit. The concept of *artificial potential fields* which has been long used in mission planning [18], [28] is adopted to compute evacuation paths in a distributed manner. Geometric navigation exploits geometric graphs to plan evacuation paths as far from hazards as possible. For instance in [5] *Delaunay triangulations* [35] are used to partition a WSN into several triangular areas for planning area-to-area navigation paths, as shown in Fig. 1; each sensor knows its location and will cooperate to compute a planar graph [31] in a distributed manner.

However, location information of both sensors and users may not always be available, so [29] maintains a road map in each user device to compute navigation paths. While most of the research focuses on finding paths based on real-time information, prediction based navigation uses the prediction of how long a hazard will take to reach the sensor, to compute the evacuation path with the longest escape time before the hazard reaches it. In [4] safe evacuation paths are maintained in two graphs, the *hazard graph* and

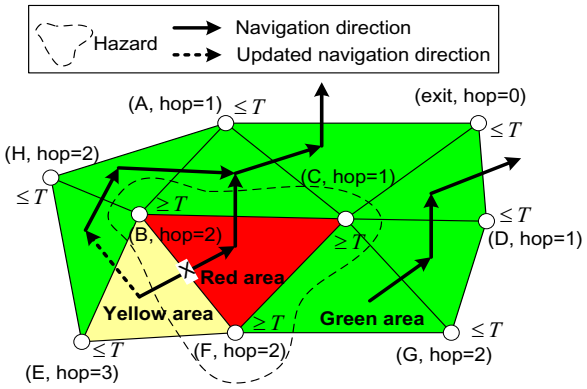

Figure 1. An example of area-to-area navigation paths.

the *navigation graph*. The inherent limitations of simple homogeneous WSNs lead to *heterogenous cyber-physical emergency evacuation systems* that combine a sensing system with a decision support system.

Prediction can be also accomplished using agent-based simulators specialised to EMS [3], [1]. The physical world can be modelled as a directed graph [12] where the set of vertices represents *Points of Interest (PoI)*, each corresponding to a location and an edge represents a path for the motion of human beings between two locations. Simulators such as DEFACTO [36], SimSITE[32], and DBES [6] are distributed for faster executon. SimSITE [32] is also a 3D visualization simulator to facilitate training of first-aid responders. DBES [6] follows HLA and extends [12] to a distributed framework that decomposes the simulated environment into modules. Some papers also consider the social interactions among evacuees [33].

3. Reliable Secure Communications

The algorithms we have cannot operate without communications. Yet communications are often one of the first infrastructures that fail during emergencies. Thus in this section we focus on what can be done in such circumstances. As a setting consider an EMS similarly to the one described in [26], [24] for densely populated urban areas. Consider a multi-floor building equipped with **fixed sensor nodes (SNs)** while the people having **mobile communication nodes (CNs)**. SNs are pre-deployed at fixed locations and each SN has a sensing unit that senses its immediate area and short range (¡ 5m) wireless communication capability. SNs *do not* perform data storage, processing or decision making and are only utilized for monitoring and civilian localization. Each person has a hand-

or pocket-held device, with storage and processing capacity equivalent to that of a mobile phone, capable of short-range (∼10m) communication. The CNs form a network in an opportunistic manner (Oppcomms) as devices come into contact. If necessary, certain CNs may be placed in fixed locations, e.g. on walls, for additional coverage. Oppcomms can disseminate messages to gather and convey information for situational awareness. The Oppcomms use multiple hop "store-carry-forward" [34] among fixed and mobile CNs using human mobility. Because the network may be disconnected for long periods of time, CNs may store messages for lengths of time, and delivery of messages is not guaranteed. We assume that each CN (a) has a graph representation of the building, and (b) is able to carry out the computations that we will describe for emergency management, (c) and can sense other CNs in its vicinity, and communicate with them via Opcomms. Each SN has a unique ID, a local clock and a location tag for its position in the building. SNs periodically sense their surroundings and each significant measurement is kept in the form of a **measurement message (MM)** and passed on to nearby CNs. Active CNs periodically produce a beacon message in the form of a localization request; any SN in the vicinity that receives the beacon replies with a **localization message (LM)** that is used by the CN to position itself approximately in the graph representation of the building. In order to preserve SN energy, CNs may inactivate the localization procedure until they are alerted about an emergency. An MM is converted by the CN into an **emergency message (EM)** containing the location of the SN for the corresponding MM, the hazard intensity, source CN ID and observation timestamp of the SN. Each EM is then disseminated among CNs using Oppcomms. The first received MM or EM is an indication of a (new) hazard, and the CN alerts its user and starts the evacuation process for that user. The CNs use epidemic routing (ER) [38] to disseminate EMs to provide "one-to-all" dissemination. Since each CN stores the graph representation of the building, it updates it locally using the MMs and EMs and computes the shortest path (SP) from its current location to the nearest exit, so that the human being equipped with the CN can be safely directed. As new messages are received, the SP is updated combining the physical distance with the hazard level. The system we have described also needs to be protected against attacks from malicious atackers.

All non-malicious CNs and SNs are assumed to operate correctly. When a defense mechanism is not employed, normal nodes trust all CNs and assume that all EMs contain correct information. We assume that each malicious node knows the identities of all malicious nodes, and follows the attack model as described below. A malicious node can (i) drop-all received legitimate packets (sent by non-malicious nodes), and (ii) create and inject incorrect packets. Thus a malicious node creates and disseminates malicious messages with false information resulting in a flooding-type attack and also misdirects CNs into providing wrong evacuation paths. In order to vary the rate of false message injection, an attacker may probabilistically creates a false EM for each location change, and a resulting false EM can falsify information on any message field: source CN ID, hazard intensity, hazard location and timestamp. In the sequel we assume that a malicious node that creates a false EM, uses correct values for the location and timestamp (as received from nearby SNs via either MMs or LMs) to emulate authenticity, but falsifies the intensity and CN ID. Malicious nodes may also tamper with legitimate messages received from other nodes. However the proposed defense mechanism discussed below prevents malicious nodes from using incorrect IDs for their messages, and from modifying messages received from other nodes.

3.1. A Defense Mechanism

To counter the effects described above, a collaborative defense mechanism that combines identity-based signatures (IBS) [37] and content-based message verification can be used to detect malicious packets and nodes. Packet dropping and collective blacklisting is employed to prevent identified attackers from participating in Oppcomms. IBS is a useful solution for node authentication and message integrity in Oppcomms, that uses identity-based cryptography (IBC) which is an asymmetric Cryptosystem with a unique identifier, such as a network address, to generate its public key. Therefore, the public key of an entity can be generated by any node that knows its ID. The private key of an entity is generated by the private key generator (PKG) and it is only known to the entity and the PKG. Depending on whether generic devices (such as smartphones) or dedicated devices (such as specialized ZigBee nodes which are only used for emergency support) are used as CNs, private key generation proceeds as follows. For generic devices, the user of a device is required to download the necessary software and building graph file onto her device before the device can act as a CN. The trusted third party providing the software and graph file acts as the PKG and the device is assigned a private key based on its device. Dedicated devices that come preloaded with the

necessary software and files also include their private key, which are assigned by the third party that installs the device software. All interaction with the PKG is offline and a device is not recognized as a CN until it has the required software and data, which include the private key. CNs do not interact with the PKG after this initial installation step and therefore the presence of the PKG is not required during EMS operation. During key generation, the PKG assures a one-to-one correspondence between a CN and its ID (and therefore public key). Keys set-up in this way are used in IBS to prevent Sybil [8] and node replication attacks. The creator (source) of an EM signs the message with its private key. A receiver can then use the source ID to generate its public key and verify the authenticity and integrity of the message via its signature. Any message that fails verification is ignored and dropped. This scheme allows easy detection of a spoofed source ID and EMs that have been modified in transit. We do not primarily use IBS as an initial authentication mechanism since any device. is allowed to install the necessary software and be part of the ESS. Notice that IBS cannot prevent insider attacks where CNs are compromised at a later stage. Therefore, in addition to IBS, CNs employ content-based message checking to identify CNs acting maliciously under the attack model described above. Each CN uses its own observations (i.e. MMs which are directly received from SNs) and EMs received from other CNs to verify the content of each received EM. A CN would expect each EM to contain information that would be consistent with the nature of the hazard and previously received EMs. For example, for a fire, the hazard intensity would be expected to stay the same or increase at a location as time passes, unless there are firefighters in the building). EMs that contain data values that contradict each other or what would normally be expected can then be detected and flagged as suspicious by the CN. Since MMs always contain correct values, any EM that contradicts with an MM (i.e. self-observation) is immediately identified as malicious. When an inconsistency is detected between two EMs, any one of them could be malicious. In this case, the number of EMs received from the sources of each message in question are used to identify the malicious node. This is based on the observation that malicious nodes would normally generate more EMs than normal nodes due to the flooding-type attack. Therefore, the source that has generated many more EMs is identified as an attacker. In the detection mechanism, the source of a malicious EM can be safely identified as the actual attacker since malicious CNs cannot modify EMs of other individuals or spoof their IDs due to the use of IBS. It is not guaranteed that all malicious messages and nodes will be identified since the gathering of evidence (e.g. multiple contradicting EMs regarding the same location) is dependent on the mobility pattern of users and takes some time. Detection can also produce false negatives where a normal node is mistakenly identified as malicious. We present simulation results on the performance of detection in the next section. Collective blacklisting is used to inform other CNs of detected attackers and to block them from participating in oppcomms. EMs are exchanged between CNs in the form of bundles, where a bundle contains one or more EMs that are sent to the other CN as determined by epidemic routing. Each bundle contains the list of node IDs that are known to be attackers by the sending CN. This blacklist contains attackers known to all source CNs of EMs in the bundle since the sending CN updates its own blacklist based on received EMs. When a new malicious node is identified, the identifying CN adds the ID of the malicious node to its own blacklist, which is then embedded in a **blacklist message (BM)**. Each BM contains the source node ID, blacklist, and the proof of why the new node was added to the blacklist. This proof is in the form of the original messages used to identify the node as malicious. Inclusion of the proof allows receivers to decide for themselves whether the addition is valid and allows the detection of false or bogus BMs that are created by malicious nodes. Each BM is signed by the source CN as a measure of protection. A BM is piggybacked on a packet bundle when there are EMs to be sent by the BM source. If there are no EMs to be sent, then a bundle is sent that contains only the BM to enable quick dissemination of identified attackers. The detected malicious nodes are prevented from participating in oppcomms by ignoring and dropping all messages originating from them. These attackers can still send malicious EMs via direct contacts, but such messages are ignored and immediately dropped by the receivers, preventing their further propagation among CNs.

3.2. Evaluation of Defense through Simulation

We have emulated and EMS using the multi-agent distributed building evacuation simulator (DBES) [7] for the real-life three-floor office building of Fig. 2. The bottom floor contains two exits and is $24m \times 45m$; the other floors are $24m \times 60m$. The simulated evacuees follow a probabilistic model of "normal motion" that-includes sitting at a desk, then after a while going into some other part of the floor, until they are notified of the emergency; this is intended to simulate their

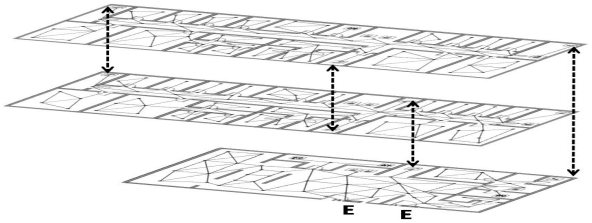

Figure 2. Model of the building used in our simulations.

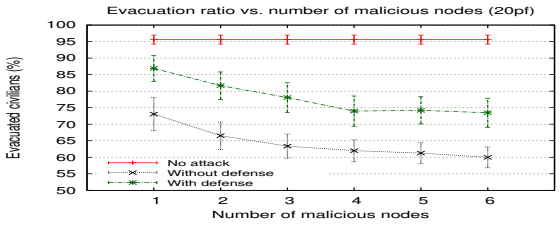

Figure 3. Ratio of successful evacuatees vs. number of attackers.

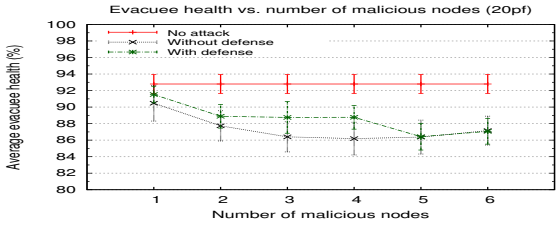

Figure 4. Average health of evacuees vs. number of attackers.

movement pattern during working hours. The walking speed for a human being is taken to be $1m/sec$ within a floors and $0.7m/sec$ when descending or ascending stairs (the ascension should normally be somewhat slower). The simulations take physical congestion into account during human movement.

In the simulations, we assume that in addition to the graph representation of the building, and the weights of the edges, each CN can store 100 messages (EMs and BMs). The average EM and BM sizes are 40 bytes and 100 bytes respectively without signatures, and 128-bit signatures are used, which adds 16 bytes to each signed message. The maximum CN data transfer rate is 100 Kbits/sec and the maximum effective CN communication range is 6m. We assume that CNs cannot communicate between floors. A SN is located at each graph vertex in the building; the SN data transfer rate is assumed to be 20 Kbits/sec and the maximum effective SN communication range is 5m. We simulate a fire and its associated effects such as smoke, which spreads following a Bernoulli trial model [9]. It starts at the intersection of two corridors on the second floor, which is a critical location due to its proximity to the main staircase that provides access to other floors. The simulations assume that all conventional means of digital communication have broken down in the building during the emergency and that the central alarm has failed due to a central power failure. The EMS then acts as a fire alarm and provides directions for evacuation to the building occupants. In our experiments, the fire starts at simulation start ($time = 0$). Each collected simulation data point is presented with its 95% confidence interval and is the mean of 50 independent simulation runs, where the initial distribution of attacker and normal user locations is different for each run. When there are at most two attackers, they are located in the second floor; when there are more than two, locations are chosen randomly from the second and third floors. The malicious message creation probability for each location is set to 0.8 for each of the attackers.

We first present results regarding the effect of the attack and defenses mechanism on the outcome of the evacuation. Figure 3 shows the evacuation ratio vs. number of attackers. Evacuation ratio is the number of successfully evacuated non-malicious users to the number of all non-malicious users. The building occupancy is set as 20 people per floor (ppf) (including the attackers). The results indicate that even a single attacker is able to greatly affect the outcome; as the number of attackers increases, the evacuation ratio decreases. However, the defense mechanism significantly improves the evacuation ratio, although the performance without any attackers cannot be attained even with defense. Figure 4 shows the average percentage health of all successfully evacuated non-malicious users in the same simulations. Similar results are observed, although the impact of both the attacks and the defense is smaller compared to the evacuation ratio. This is because the health metric only takes into account successfully evacuated users, while casualties are not counted.

Figure 5 shows the false positive ratio of malicious packet (and node) detection versus the number of attackers, i.e. the ratio of packets (and nodes) incorrectly detected as malicious to all packets (and nodes) detected as malicious. The false positive ratio is low, ranging from 0.3% to 1.5% and the highest ratio is observed when the number of attackers is one (as would be expected due to the lack of useful statistics. Figure 6 shows two metrics: (i) the ratio of malicious packets correctly detected to all malicious

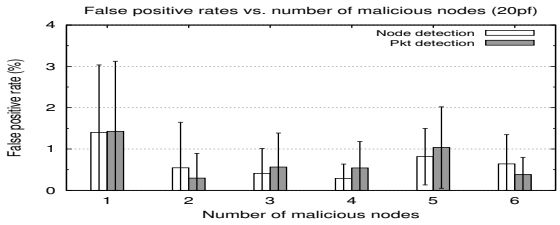

Figure 5. False positive rate of malicious packet detection.

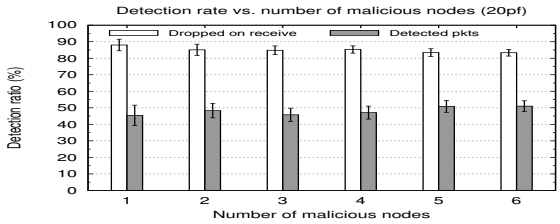

Figure 6. Performance of malicious packet detection for the defense mechanism.

packets received, and (ii) the ratio of malicious packets correctly detected before they were used by the receiving CN to update its local graph. Most of the detected malicious packets have been identified before they were used to update graphs and therefore do not directly affect evacuation directions given to the users. However, we observe that only about half of the total malicious packets disseminated among CNs are correctly identified as malicious. This illustrates the difficulty of correct detection of malicious users with intermittent connectivity and without enough time for collection of history and related information.

4. Conclusions and Future Work

Although we have tried to conduct a comprehensive review of EMS, several significant areas require much more attention. Since EMSs are intrinsically distributed and more on distributed algorithms for such systems [19] is needed. Information collected via sensing is often innacurate and requires interpretation [17]. A related problem is how one may interpret biased information [16]. The optimum allocation problems are themselves NP-hard and need to be taken in real time based on incomplete or partial information [21], and merit more attention. Another topic which has been neglected is the use of probability modeling [20] where one seeks evaluations which are necessarily statistical. Such methods can reduce lengthy computer simulations and provide computationally fast mathematical prediction of overall performance. We think that such methods will become more prevalent as the study of EMSs gains prominence and joins the mainstream of human based cyber-physical systems.

References

[1] Robocuprescue. http://www.rescuesystem.org/robocuprescue/.

[2] Volkan Atalay and Erol Gelenbe. Parallel algorithm for colour texture generation using the random neural network model. *International Journal of Pattern Recognition and Artificial Intelligence*, 6(2–3):437–446, 1992.

[3] Vidhya Balasubramanian, Daniel Massaguer, Sharad Mehrotra, and Nalini Venkatasubramanian. DrillSim: A simulation framework for emergency response drills. *Intelligence and Security Informatics*, 3975:237–248, 2006.

[4] Matthew Barnes, Hugh Leather, and D. K. Arvind. Emergency evacuation using wireless sensor networks. In *IEEE Conf. Local Computer Networks*, pages 851–857, 2007.

[5] Po-Yu Chen, Wen-Tsuen Chen, and Yi-Tsung Shen. A distributed area-based guiding navigation protocol for wireless sensor networks. In *IEEE Int'l Conf. Parallel and Distributed Systems*, pages 647–654, 2008.

[6] Nikolaos Dimakis, Avgoustinos Filippoupolitis, and Erol Gelenbe. Distributed building evacuation simulator for smart emergency management. *The Computer Journal*, 53(9):1384–1400, 2010.

[7] Nikolaos Dimakis, Avgoustinos Filippoupolitis, and Erol Gelenbe. Distributed building evacuation simulator for smart emergency management. *The Computer Journal*, 53(9):1384–1400, 2010.

[8] John Douceur. The Sybil attack. In *Peer-to-Peer Systems*, LNCS, pages 251–260. 2002.

[9] D. Elms, A. Buchanan, and J. Dusing. Modeling fire spread in buildings. *Fire Technology*, 20(1):11–19, 1984.

[10] Avgoustinos Filippoupolitis and Erol Gelenbe. A distributed decision support system for building evacuation. In *IEEE Int'l Conf. Human System Interactions*, pages 320–327, 2009.

[11] Avgoustinos Filippoupolitis and Erol Gelenbe. An emergency response system for intelligent buildings. In *Sustainability in Energy and Buildings*, 2011 (to appear).

[12] Avgoustinos Filippoupolitis, Laurence Hey, Georgios Loukas, Erol Gelenbe, and Stelios Timotheou. Emergency response simulation using wireless sensor networks. In *Int'l Conf. Ambient Media and Systems*, pages 21:1–21:7, 2008.

[13] Erol Gelenbe. Cognitive packet network (CPN). U.S. Patent 6,804,20, October 11 2004.

[14] Erol Gelenbe. Steps towards self-aware networks. *Communications of the ACM*, 52:66–75, 2 2009.

[15] Erol Gelenbe and Jean-Michel Fourneau. Random neural networks with multiple classes of signals. *Neural Computation*, 11(4):953–963, 1999.

[16] Erol Gelenbe and Georges Hébrail. A probability model of uncertainty in data bases. In *ICDE*, pages 328–333. IEEE Computer Society, 1986.

[17] Erol Gelenbe and Laurence Hey. Quality of information: An emprical approach. In *Proc. 5th IEEE Inter. Conf. on Mobile Ad-Hoc and Sensor Systems*, pages 730–735, Oct. 2008.

[18] Erol Gelenbe, Khaled Hussain, and Varol Kaptan. Simulating autonomous agents in augmented reality. *Journal of Systems and Software*, 74(3):255–268, February 2005.

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

[20] Erol Gelenbe and Andreas Stafylopatis. Global behaviour of homogeneous random neural systems. *Applied Mathematical Modelling*, 15(10):534–541, 1991.

[21] Erol Gelenbe, Stelios Timotheou, and David Nicholson. Fast distributed near-optimum assignment of assets to tasks. *The Computer Journal*, 53(9):1360–1369, 2010.

[22] Erol Gelenbe, Zhiguang Xu, and Esin Seref. Cognitive packet networks. In *IEEE 11th International Conference on Tools with Artificial Intelligence (ICTAI)*, pages 47–54, November 1999.

[23] Gokce Gorbil, Avgoustinos Filippoupolitis, and Erol Gelenbe. Intelligent navigation systems for building evacuation. *Computer and Information Sciences, Lecture Notes in Electrical Engineering*, 2011 (to appear).

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

[25] Gokce Gorbil and Erol Gelenbe. Opportunistic communications for emergency support systems. In *Int'l Conf. Ambient Systems, Networks and Technologies*, pages 1–9, 2011.

[26] Gokce Gorbil and Erol Gelenbe. Opportunistic communications for emergency support systems. *Procedia Computer Science*, 5:39–47, 2011.

[27] Yutaka Inoue, Akio Sashima, Takeshi Ikeda, and Koichi Kurumatani. Indoor emergency evacuation service on autonomous navigation system using mobile phone. In *Int'l Symp. Universal Communication*, pages 79–85, 2008.

[28] Varol Kaptan and Erol Gelenbe. Fusing terrain and goals: agent control in urban environments. In *Multisource Information Fusion: Architectures, Algorithms, and Applications 2006*, volume 6242, pages 71–79. SPIE, April 2006.

[29] Mo Li, Yunhao Liu, Jiliang Wang, and Zheng Yang. Sensor network navigation without locations. In *IEEE INFOCOM*, pages 2419–2427, 2009.

[30] Qun Li, Michael De Rosa, and Daniela Rus. Distributed algorithms for guiding navigation across a sensor network. In *ACM Int'l Conf. Mobile Computing and Networking*, pages 313–325, 2003.

[31] Xiang-Yang Li, Gruia Calinescu, Peng-Jun Wan, and Yu Wang. Localized Delaunay triangulation with application in ad hoc wireless networks. *IEEE Trans. Parallel and Distributed Systems*, 14(10):1035–1047, 2003.

[32] Ke Liu, Xiaojun Shen, Abdulmotaleb El Saddik, Azzedine Boukerche, and Nicolas D. Georganas. SimSITE: The HLA/RTI based emergency preparedness and response training simulation. In *IEEE Symp. Distributed Simulation and Real-Time Applications*, pages 59–63, 2007.

[33] Yuu Nakajima, Hironori Shiina, Shohei Yamane, and Toru Ishida. Disaster evacuation guide: Using a massively multiagent server and GPS mobile phones. In *IEEE Int'l Symp. Applications and the Internet*, 2007.

[34] Luciana Pelusi, Andrea Passarella, and Marco Conti. Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks. *IEEE Communications Magazine*, 44(11):134–141, Nov. 2006.

[35] Franco P. Preparata and Michael Ian Shamos. *Computational Geometry: An Introduction*. Springer-Verlag, 1985.

[36] Nathan Schurr, Janusz Marecki, Milind Tambe, Paul Scerri, Nikhil Kasinadhuni, and J.P. Lewis. The future of disaster response: Humans working with multiagent teams using DEFACTO. In *AAAI Spring Symp. AI Technologies for Homeland Security*, 2005.

[37] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology (CRYPTO'84)*, LNCS, pages 47–53. 1984.

[38] Amin Vahdat and David Becker. Epidemic routing for partially-connected ad hoc networks. Tech. Report CS-2000-06, Duke Univ. CS Dept., Apr. 2000.