Resilient Emergency Evacuation using Opportunistic Communications

Gokce Gorbil and Erol Gelenbe

Abstract We describe an emergency evacuation support system (ESS) that employs short-range wireless communications among mobile devices carried by civilians. Emergency information is disseminated via opportunistic contacts between communication nodes (CNs), and each CN provides adaptive step-by-step navigation directions for its user during evacuation. Using mobile devices and opportunistic communications (oppcomms) allow ESS to operate when other means of communication are destroyed or overloaded. In this paper, we evaluate the resilience of oppcomms as used to enable evacuation support in ESS; we specifically consider the effect of CN failures on evacuation and communication performance. Our simulation experiments of evacuation of a three-floor office building show that ESS is highly resilient to node failures, and failure ratios up to 20% are well-tolerated.

1 Introduction

Evacuation is an urgent and important component of emergency response that requires spatio-temporal decision making by the civilians affected in the emergency. The unknown impact of the event, incomplete and incorrect information on the situation, dynamic conditions of the emergency (such as a spreading hazard) and destroyed and inaccessible communication infrastructure introduce significant challenges for evacuation. We propose a resilient emergency support system (ESS) to provide evacuation support to civilians in the emergency area. ESS uses opportunistic communications [13] between pocket devices carried by people to disseminate information on the emergency. Using this 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.

Gokce Gorbil and Erol Gelenbe
Imperial College London, EEE Dept., ISN Group, SW7 2BT, London, United Kingdom, e-mail: {g.gorbil, e.gelenbe}@imperial.ac.uk

In this paper, we evaluate the resilience of opportunistic communications for evacuation support as employed in ESS. We specifically consider the effect of device failures on evacuation and communication performance. 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.

1.1 Design Assumptions

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.

We assume that the graph is known for a building. We also assume that 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).

1.2 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 [13] 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 [15] 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 [12] 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 [14]. 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.

2 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) [1]. 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.

2.1 Simulation Results

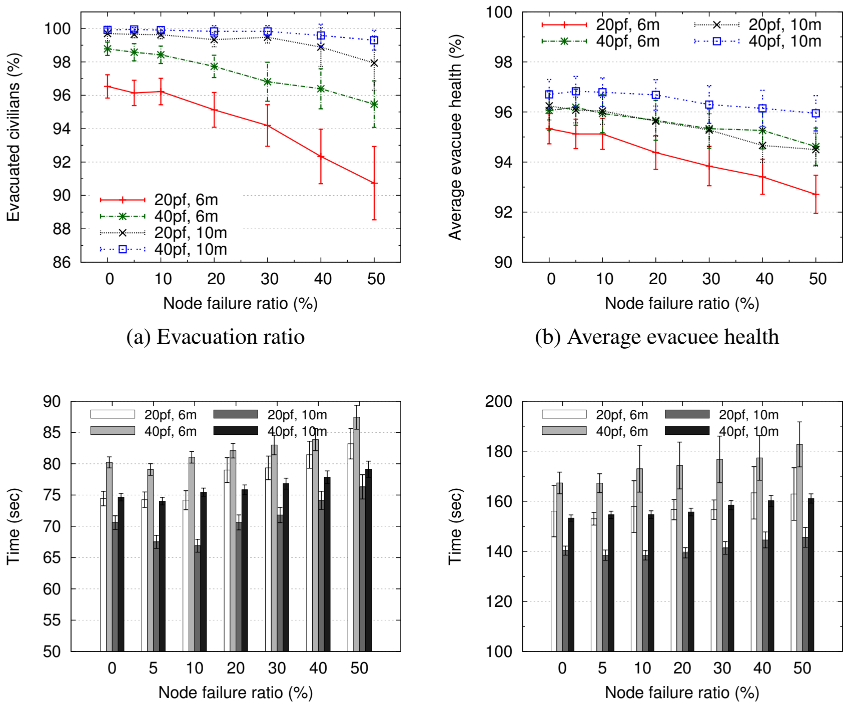
We see that evacuation ratio (Fig. 1a) is affected less from failures when nodes have more frequent contact opportunities and when connected subnetwork sizes are larger, i.e. when population density and/or communication range is high. For example, with 40pf and 10m range, evacuation ratio is practically unaffected by failures. Effect of failures on evacuation ratio increases as population density and/or communication range decreases. With more failures in the system, evacuation ratio decreases in general. We see that ESS is fairly resilient to node failures in terms of evacuation ratio and that failure ratios of up to 20% are well-tolerated. An important observation is that 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 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 node failure ratio. Our results show that evacuation times increase as failure ratio increases, except for the 20pf with 10m range case, which shows decreasing average evacuation time until 10% failure ratio. The effect of failures on evacuation time comes from two factors: (i) with more failures, people are alerted later of the fire and therefore start to evacuate later, and (ii) more people need to change paths during evacuation because of incomplete or outdated information, which both increase evacuation time.

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

---

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



(a) Evacuation ratio (b) Average evacuee health

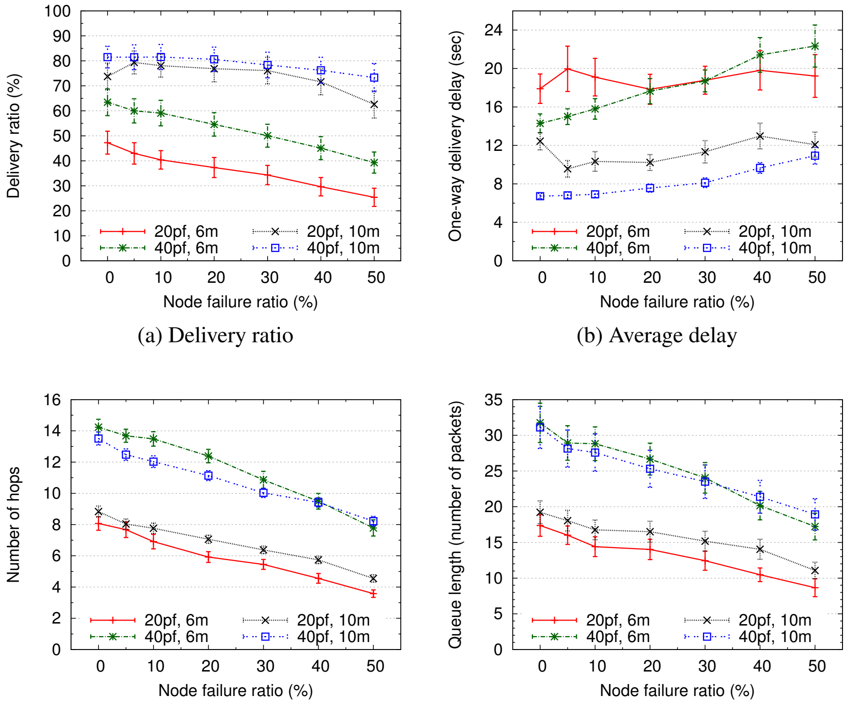
(c) Average evacuation time (d) Worst-case evacuation time

Fig. 1 Effect of node failures on evacuation performance

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

[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

Fig. 2 Effect of node failures on communication performance

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.

3 Conclusions and Future Work

We have described an emergency evacuation support system (ESS) that employs opportunistic communications between pocket devices carried by people to disseminate emergency messages. Each communication node (CN) provides alerts and navigation directions to its user for evacuation based on 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, ESS is a highly resilient system which 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.

An ESS is a complex distributed system that provides spatio-temporal analyses and decisions to improve the outcomes for human beings that are affected by a small or large scale emergency [10]. Thus in this area we encounter all the classical and long-standing research questions related to distributed systems, including the incomplete and incorrect information on the distributed situation [4], and the inconsistent state information due to synchronisations and delays [5]. The distributed decision algorithms, for instance including the allocation of emergency teams and supporting mobile units, are also very challenging and require further work [7–9].

Our results in this paper focus only on communication issues and we have seen that the 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 way to improve resilience to node failures. We aim to investigate this approach in future work. In addition to node failures, we also need to consider deliberate attacks on the network. We believe that security of oppcomms is important due to the critical nature of emergencies and we will 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 engineering [6]. Furthermore, techniques such as CPN [2, 3, 11] not only can benefit oppcomms, but have also proved useful in guiding evacuees. These aspects too will be included in future work.

References

1. Dimakis, N., Filippoupolitis, A., Gelenbe, E.: Distributed building evacuation simulator for smart emergency management. The Computer Journal **53**(9), 1384–1400 (2010)
2. Gelenbe, E.: Cognitive packet network (CPN). U.S. Patent 6,804,201 (2004)
3. Gelenbe, E.: Steps towards self-aware networks. Communications of the ACM **52**(7), 66–75 (2009)
4. Gelenbe, E., Hébrail, G.: A probability model of uncertainty in databases. In: Proc. 2nd Int. Conf. on Data Engineering (ICDE'86), pp. 328–333 (1986)
5. Gelenbe, E., Sevcik, K.C.: Analysis of update synchronisation algorithms for multiple copy data bases. IEEE Transactions on Computers **C-28**(10), 737–747 (1979)
6. Gelenbe, E., Stafylopatis, A.: Global behavior of homogeneous random neural systems. Applied Mathematical Modelling **15**(10), 534–541 (1991)
7. Gelenbe, E., Timotheou, S., Nicholson, D.: Fast distributed near-optimum assignment of assets to tasks. The Computer Journal **53**(9), 1360–1369 (2010)

8. Gelenbe, E., Timotheou, S., Nicholson, D.: A random neural network approach to an assets to tasks assignment problem. SPIE Signal Processing, Sensor Fusion, and Target Recognition XIX **7697**(1), 76,970Q (2010)
9. Gelenbe, E., Timotheou, S., Nicholson, D.: Random neural network for emergency management. In: Proc. Workshop on Grand Challenges in Modeling, Simulation and Analysis for Homeland Security (MSAHS'10) (2010)
10. Gelenbe, E., Wu, F.J.: Large scale simulation for human evacuation and rescue. Computers and Mathematics with Applications (2012). DOI 10.1016/j.camwa.2012.03.056
11. Gelenbe, E., Xu, Z., Seref, E.: Cognitive packet networks. In: Proc. 11th Int. Conf. on Tools with Artificial Intelligence (ICTAI'99), pp. 47–54 (1999)
12. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Computer Science **5**(0), 39–47 (2011)
13. Pelusi, L., Passarella, A., Conti, M.: Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks. IEEE Communications Magazine **44**(11), 134–141 (2006)
14. Song, L., Kotz, D.F.: Evaluating opportunistic routing protocols with large realistic contact traces. In: Proc. 2nd ACM Workshop on Challenged Networks, pp. 35–42. ACM (2007)
15. Vahdat, A., Becker, D.: Epidemic routing for partially-connected ad hoc networks. Tech. Report CS-2000-06, Duke University, Dept. of Computer Science (2000)