4-30-2019

A Communication Architecture for Crowd Management in Emergency and Disruptive Scenarios

Alfredo J. Perez

Sherali Zeadally

A Communication Architecture for Crowd Management in Emergency and Disruptive Scenarios

Alfredo J. Perez and Sherali Zeadally

The authors propose the Communication Architecture for Crowd Management (CACROM), which can support crowd management under emergency and disruptive scenarios. They identify, describe, and discuss the various components of the proposed architecture, and they briefly discuss open challenges in the design of crowd management systems for emergency and disruptive scenarios.

Digital Object Identifier: 10.1109/MCOM.2019.1800626

Abstract

Crowd management aims to develop sup- port infrastructures that can effectively manage crowds at any time. In emergency and disruptive scenarios this concept can minimize the risk to human life and to the infrastructure. We propose the Communication Architecture for Crowd Management (CACROM), which can support crowd management under emergency and disruptive scenarios. We identify, describe, and discuss the various components of the proposed architecture, and we briefly discuss open challenges in the design of crowd management systems for emergency and disruptive scenarios.

Introduction

Emergency and disruptive scenarios, either generated by man-made activities (e.g., human stampedes, terrorism) or acts of nature (e.g., hurricanes, earthquakes,

wildfires) require an effective response to minimize the risk to human life and to the infrastructure. To this end, crowd management and crowd control

[1] are concepts that allow the community and event planners to develop support infrastructures and action plans that can be effective when managing crowds.

According to Berlonghi [1], crowd management includes all the measures taken to facilitate the normal movement of people during an event, whereas crowd control includes measures to handle crowds once they have gotten out of control at a particular event. Based on these definitions, activities for crowd management include noise control, communications with the crowd, planning for the different possible scenarios during the event, and tracking of locations in which the crowd gathers (and their purpose). Examples of activities for crowd control include arrests, ejections, use of force, and any type of law enforcement task to keep the rule of law at the event. In the end, the goal of both concepts is to effectively handle crowds to successfully accomplish the event without incident, or, if an incident happens, to minimize the risk to human life and to the infra- structure. The typical elements of crowd management include:

An event: This is any type of activity that takes place at a particular location with a time to start and a time to end.

A crowd: A collection of people. Crowds can be classified into different types (i.e., disruptive crowd, ambulatory) based on their behavior and/ or activities at the event.

Event planners: People or institutions in charge of the event. Event planners are responsible for performing crowd management at the event, and should be prepared to support and enforce crowd control if needed.

Support infrastructure: This includes the elements, equipment, systems, and plans that event planners utilize to perform crowd management. The support infrastructure may include simulations to develop plans for potential scenarios before, during, and after the event concludes (i.e., to safely disperse crowds after the event).

Tragic events (e.g., Hurricane Katrina in New Orleans), the death of a U.S. worker during a post-Thanksgiving's Day Black Friday sales event, Hajj stampedes,

and other situations at events that have led to the loss of human life have prompted security, law enforcement agencies, and business to employ crowd management. In fact, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has developed a guideline to follow when special sales and pro- motional events take place, and law enforcement agencies use crowd management any time an event will gather large crowds.

Crowd Management Approaches

Type of approach	Example of approach	Application examples	Strengths	Weaknesses
Modeling and simulation-based approaches	Differential equations Probability distributions and expectations Complex systems modeling	U.S. National Infrastructure Simulation and Analysis Center (NISAC)	A priori modeling of events and possible scenarios before they occur	Models may be hard to validate, which may lead to unrealistic scenarios
Infrastructure-based approaches	Closed-circuit television (CCTV) Real-time aerial imagery Radio frequency identification (RFID) Static wireless sensor networks	The Hajj annual pilgrimage to Mecca	Real-time monitoring of crowds at events Real-time identification of problematic crowds and scenarios Estimation of crowd management variables such as crowd density and crowd velocity is possible	Require the investment of infrastructure at event, which may be costly Environmental conditions may affect data collection (CCTV)

Crowd-based approaches	Mobile crowdsensing and social network monitoring	Monitoring of public events in the United Kingdom, the Nether- lands, and Switzerland	Real-time monitoring of individual and crowds at events	Require crowd participation at the events
			Real-time identification of problematic crowds and scenarios	Crowd devices may generate faulty data on purpose
			Estimation of crowd management variables such as crowd density and crowd velocity is possible	May create privacy concerns for crowd members

Crowd management has been studied as an inter- disciplinary area that includes psychology, computer science/information technology, criminal justice, and civil engineering, among other fields [2]. From the information and communication perspective, we classify the approaches used for crowd management as follows.

Table 1. Summary of crowd management approaches from an information and communication perspective.

Modeling and simulation-based approaches: Modeling and simulation-based approaches are used in crowd management to model the behavior of crowds at an event to discover critical situations under different scenarios before they occur. These approaches make use of techniques such as differential equations, probability distributions, and complex systems modeling [3].

Infrastructure-based approaches: In this category, event planners make use of systems deployed at the venue. Such systems may include closed-circuit television (CCTV), real-time aerial imagery (e.g., drones, satellites), and radio frequency identification (RFID) using event tickets and/or event-distributed id tags to collect real- time data about crowds at the event [4].

Crowd-based approaches: In this category event planners make use of crowdsourced systems such as mobile sensing systems (i.e., the use of smartphones) and social networking web- sites (e.g., Twitter) to monitor and collect

data about crowds at the event. Crowdsourced data may include location data, multimedia data (e.g., sound and video), and text-based data collected from social networks about the event [5].

Crowd management systems provide situation- al awareness to event planners during an event. To this end, crowd management systems allow event planners to observe an area of interest and estimate variables needed to characterize crowds such as crowd size, crowd density (i.e., the number of people per unit area in the event), crowd velocity and direction (i.e., where the people are moving and how fast they are doing it), and crowd behavior (e.g., pacific, disruptive, violent) [5]. Thus, crowd management systems use different streams of data (e.g., CCTV feeds, crowd- sourced data such as location or social media data) to estimate these variables with different accuracies depending on the estimation method and technology used. For example, counting people using CCTV is more difficult to perform (and has a higher estimation error) than using crowd- sourced data (e.g., mobile phone location data) for the same purpose. Table 1 summarizes the strengths, weaknesses, and application scenarios where these recently proposed approaches have been applied.

Crowd Management for Emergency And Disruptive Scenarios

The techniques described in the previous section (with the exception of modeling and simulation-based approaches) require telecommunications support to be effective in order to perform crowd management during emergency and disruptive scenarios. Depending on the nature of the emergency/disruptive scenario (i.e., a small-scale incident such as a mass shooting, or a large-scale event such as an earthquake, a blizzard, or the passing of a hurricane), the tele- communication infrastructure could be affected by the scenario. In addition, methods such as infrastructure-based approaches and crowd-based approaches use different types of data (e.g., text- based/binary data such as location data, multi- media data, and real-time data) which require different quality of service (QoS). When the communication networks' operations are disrupted or fail, these

systems may not work as expected. In large-scale emergency events, the telecommunication infrastructure can be affected as follows.

Failure at the core of the network: In this category, the core infrastructure of the network is affected by the scenario because of power out- ages [6, 7], physical damage to the communication infrastructure itself (e.g., wired infrastructure flooded, or cellular antennas taken down because strong winds or earthquakes), and failure due to high traffic load in the network during and after the emergency event.

Failure of the edge devices in the network: In this category, the telecommunication infrastructure fails at the edge of the network because battery-powered end-user devices (i.e., smart- phones) deplete their power supply, or no power is available at the end device because of a power grid failure (e.g., a house). To highlight this issue, Kongsiriwattana *et al.* [7] conducted a survey on battery depletion and found that a large amount of respondents deplete the battery of their smart- phones within 24 hours (32 percent within 14 hours, and 46 percent within 24 hours).

Based on the telecommunication failures mentioned above, to perform crowd management for prolonged, large-scale emergency scenarios using the various techniques described in the section above, the communication infrastructure

must have backup power supplies (at both the core network and the edge devices' infrastructure), communication protocols must minimize power consumption (to save power at both parts of the network), and if crowd-based approaches are used through mobile crowdsensing applications in battery-powered devices, the latter must be designed with mechanisms to minimize power consumption.

The Communication Architecture for Crowd Management

In light of the above discussions and analysis of techniques, in this section, we describe our pro- posed Communication Architecture for Crowd Management (CACROM), which is an architecture for crowd management in large-scale emergency and disruptive scenarios. As Fig. 1 shows, the CACROM architecture

consists of three tiers: the power segment, the communication segment, and the crowd data collection and notification segment.

Power Segment

The power segment includes the power supplies required to maintain the CACROM-based devices and systems in execution. These power supplies can be divided into two groups.

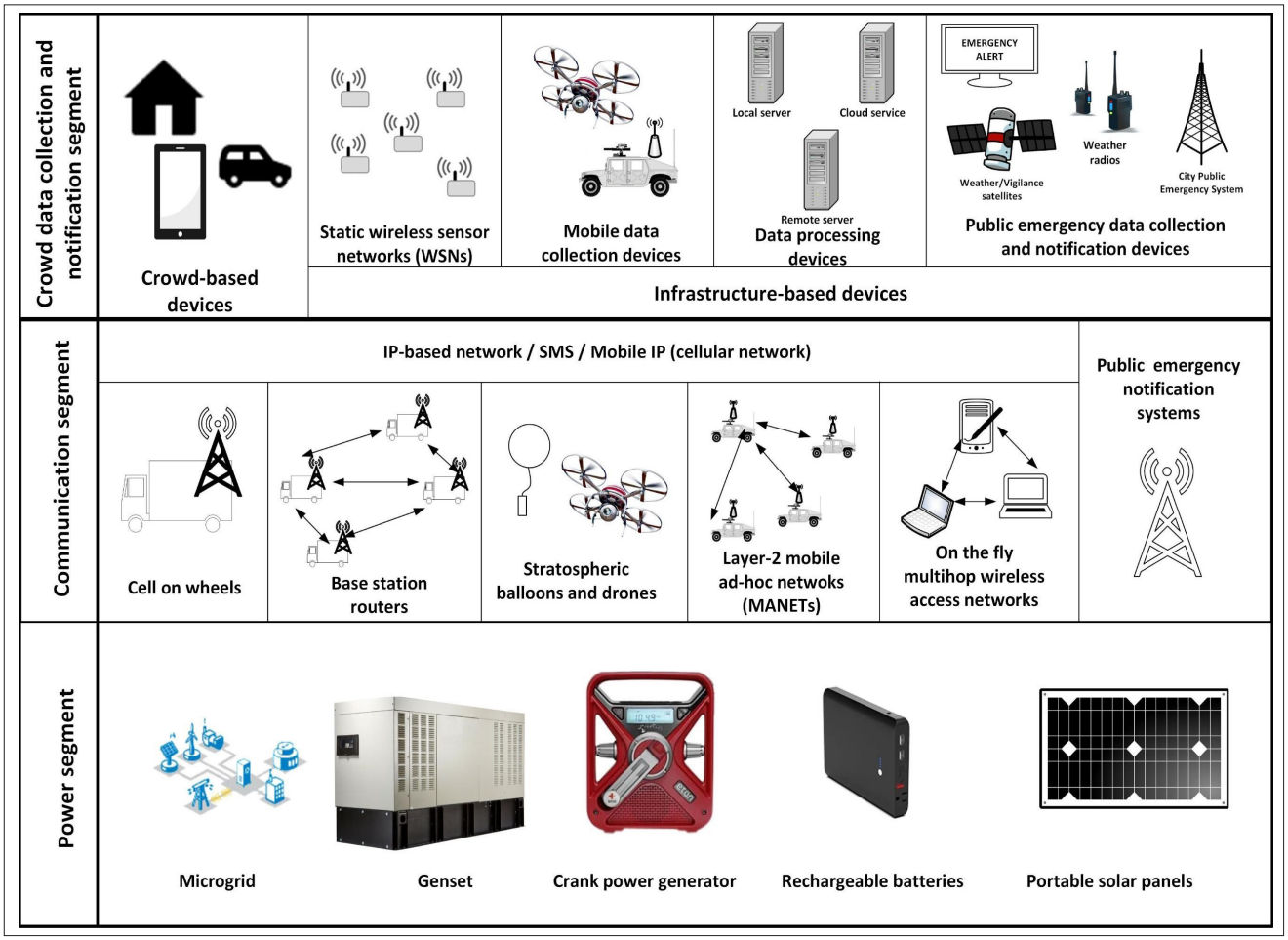

Figure 1. The CACROM architecture.

Power supplies for core network equipment: The goal in this category is to supply power for core equipment during a large-scale emergency event through gensets (diesel-based generators) placed above ground, microgrids, solar panels, or a combination of renewable power supplies.

Power supplies for crowd data collection: The goal in this group is to maintain power supplies to enable crowd data collection devices during a large-scale event. Some examples of technologies in this category include pre-charged rechargeable batteries, crank generators, portable solar photovoltaics, gas generators, and/or microgeneration.

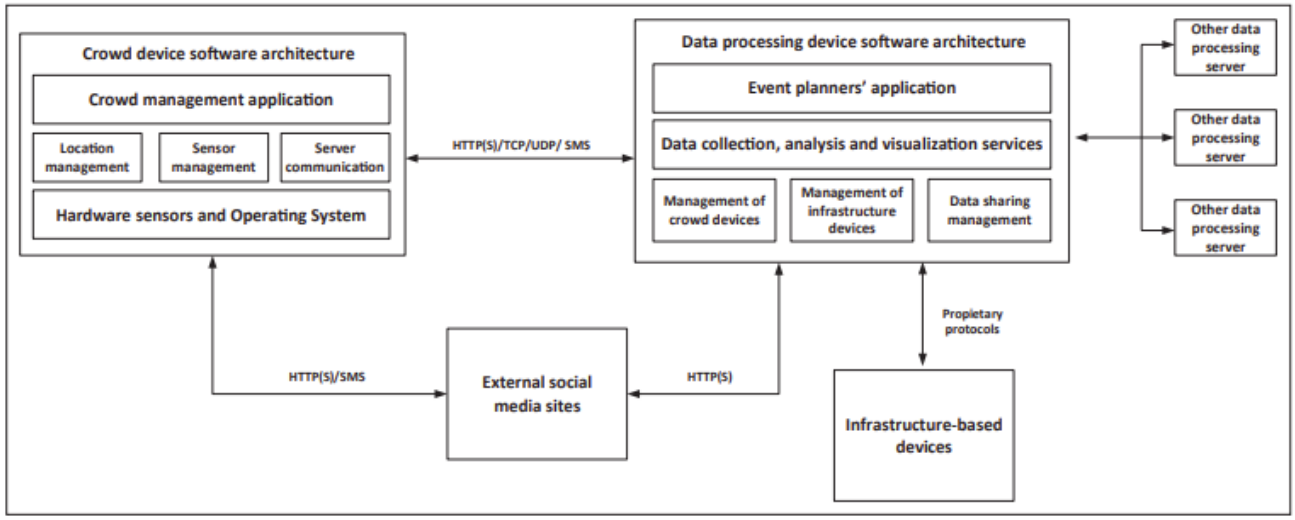

Figure 2. The crowd data collection and notification segment's software architecture

Communication Segment

In the CACROM architecture the communication infrastructure consists of IP-based networks — that is, residential Internet service providers (ISPs), mobile IP, and short messaging systems (SMS) — connected through communication technologies such as cellular networks, household Inter- net access, mobile ad hoc networks (MANETs), and current public emergency notification systems such as the Federal Emergency Management Agency's (FEMA's) Integrated Public Alert and Warning System (IPAWS), which sends alert information to crowds. The utilization of SMS in large-scale emergency events was effective in the aftermath of the Haiti earthquake in 2010 where an SMS infrastructure was quickly established and helped to provide humanitarian relief coordination during the event [8].

As cellular networks with fixed base stations and household Internet access may fail because of physical damage to the communication equipment, the

CACROM communication segment could be deployed by using the following technologies:

Cell on Wheels (COWs): In this approach only the cellular antennas are portable, and they can be deployed through land-based vehicles. The drawback of this approach is that it may rely on fixed communication networks to connect the antennas with the rest of the cellular network, which could fail based on the emergency situation. This approach was used in the aftermath of Hurricane Katrina in New Orleans [9].

Portable cellular systems using base station routers: In this approach the cellular system is deployed by using a collection of base station routers (BSRs) in which each router is a fully equipped communication node that contains all the infrastructure required by a cell. It is differentiated from the COW approach in that the full cell site is self-contained, whereas in the COW only the base station (i.e., antenna) is mobile. BSR nodes create a mobile ad hoc network among themselves via microwave links [10], and crowd users connect using their cell phones without any modification to their devices.

Internet connectivity with stratospheric balloons/drones: In this approach stratospheric balloons or drones are used to provide Internet access. An example of this approach is project Loon, which uses stratospheric balloons and a set of easy-to-install ground stations that serve as ISPs to crowd users. According to Alphabet, Loon was deployed with support from AT&T and T-Mo- bile to bring the Internet to more than 200,000 people in the aftermath of Hurricane Maria in Puerto Rico. A similar approach was demonstrated in project Titan's and Facebook's connectivity lab in which Internet service access is provided via drones. A disadvantage of these systems is that when the balloons or drones fail, they may generate emergency situations for people on the ground.

Layer-2 mobile ad hoc networks (MANETs): In this approach MANET nodes are deployed to create wireless backbone communication over greater distances. MANET nodes can provide Wi-Fi access point functionality to crowd users and event managers, and these nodes can be deployed via terrestrial vehicles, first responders on foot, aerial vehicles (e.g., unmanned aerial devices), or a

combination of these. These net- works are called layer-2 MANETs [11] because, from the point of view of the crowd users and event managers, the communication is end-to-end (i.e., without requiring the crowd devices to per- form routing). An example of this technology is Persistent Systems' WaveRelay, which is currently used by the U.S. Federal Bureau of Investigation (FBI).

On-the-fly establishment of multihop wire- less access networks (OEMAN): In this approach crowd user devices connect to the Internet after the emergency/disaster scenario in order to per- form mesh/ad hoc routing functionality [12]. As new devices connect to the network, they continue to extend the network's coverage. Even though these types of networks are similar to layer-2 MANETs, they differ in that layer-2 MANET equipment is only responsible for routing, but in this approach crowd devices may collect data and perform routing as well. A drawback of OEMANs on crowd devices is power consumption because crowd devices may deplete their batteries faster as a result of performing routing tasks.

A combination of the communication technologies at a large emergency or disruptive scenario can be deployed, based on the availability of the technologies at the particular geographical location and the scale of the event.

Crowd Data Collection And Notification Segment

This segment corresponds to the devices and the software architecture needed to collect and process data from the crowd. Here, the goal is to collect data as needed from the event planners and crowd users while minimizing power usage at crowd-based devices and to minimize the amount of traffic in the communication tier. The devices used by this segment can be classified as follows.

Crowd-based devices: These are the devices owned by the crowd users. They include mobile phones, smartphones, static sensors in homes, Internet of Things (IoT) devices, and connected vehicles. Notification devices such as televisions and radios are also included under this category. The goal of these devices is to collect data need- ed by event planners, which may include location data (e.g., GPS data), sensor data (e.g., health and weather-related data, air pollution), images, sound, text, and video.

[1]

Infrastructure-based devices: These are the devices that are deployed by event planners or those that already were deployed as part of the infrastructure to collect data and process the data collected from the crowd. Devices under this category include static wireless sensor networks (WSNs) (e.g., weather stations, water gauge devices), mobile data collection devices such as drones and land-based vehicles deployed by event planners (to collect video), data processing devices such as servers, remote servers, and cloud services (e.g., social networking platforms), and public emergency data collection and notification devices (e.g., traffic cameras, satellites, billboards, public loudspeaker towers/sirens).

Figure 2 depicts the software architecture during crowd data collection, and it includes the protocols used to collect data on an end-to-end basis from the crowd, and the infrastructure-based and external systems such as social networking sites. The software architecture in CACROM is divided in two parts:

1. Crowd device software architecture
2. Data processing device software architecture

The components of the crowd device's soft- ware architecture are used by a crowd management application that collects data from smartphones and external sensors via Bluetooth (or Wi-Fi). In addition, the components can per- form some type of local processing, and they can communicate with event planners' servers and external social networking sites (if available). The components of the crowd-device software architecture include the following.

Hardware sensors and operating system: They support the communication between the sensors connected and end-user devices such as the smartphone. The sensors may be connected directly to the smartphone, or the smartphone collects data via Bluetooth or Wi-Fi from them.

---

[1] The components of the crowd device's software architecture are used by a crowd management application that collects data from smartphones and external sensors via Bluetooth (or Wi-Fi). In addition, the components can perform some type of local processing, and they can communicate with event planner's servers and external social networking sites (if available).

Location management: This component collects and evaluates if it is worthwhile to spend power to obtain location data. It also decides if the location data should be forwarded to the event planner's data processing devices (saving computing resources such as processor time and network bandwidth). This module is important because it helps to reduce the power consumption of the device since the GPS sensor consumes a great amount of power from the smartphones' batteries. Mechanisms in this component include the location-aware state machine and the critical point algorithm, which diminish the amount of data sent by the smartphone to the servers. The location-aware state machine algorithm works by deactivating the GPS sensor when it is not needed, and the critical point algorithm selects which location data to send to the server based on preconfigured rules [14].

Sensor management: In this component the crowd device collects the sensor data, performs local feature detection/analysis at the smart- phone, and sends notifications to the event planners to crowd devices upon detection of scenarios of interest.

Server communication: This component transfers data from the crowd's smartphone devices to the event managers' data processing devices and external social networking applications. It makes use of HTTP, HTTPS, TCP, UDP, and SMS, which are used by the smartphone's crowd management application according to the emergency scenario. For example, if event planners need continuous, real-time location data collection, the crowd management application may send the location data via UDP. However if reliability is needed, TCP, HTTP, or HTTPS may be used. SMS can be used to share short messages that may include sporadic location data or text-based information. This component may also support security (e.g., encryption) and privacy mechanisms.

The components of the data processing device's software architecture are used by event planners' data presentation services (i.e., graphical user interface systems and applications) to visualize and collect data from crowd-based devices, infrastructure-based devices, and external systems such as social networking sites. In addition, the event planner's application can process data and provide feedback

to the crowd and to public security/law enforcement personnel (including rescue personnel). These components include:

- Management of crowd devices: It implements the functionality needed to collect data from crowd devices and feedback crowd devices if needed by the event planners by using crowd devices or public emergency notification systems.
- Management of infrastructure-based devices: It provides mechanisms that collect data from infrastructure-based devices and external systems such as social networking plat- forms.
- Data sharing management: It provides the functionality to scale the crowd management system if needed. It can be used as a gateway to connect to other data processing devices that are part of the crowd management system by using either federated or peer-to-peer protocols.
- Data collection, analysis, and visualization services' component: It allows event planners to perform analysis and visualize the data from various sources.

Discussion And Open Issues for Crowd Management Architectures for Emergency And Disruptive Scenarios

Crowd management systems for emergency and disaster scenarios can be evaluated by using various factors such as cost of deployment, bandwidth utilization, power consumption, and accuracy in the estimation of crowd parameters. It is worth mentioning that, under an emergency scenario, some of these factors may compete with each other in the sense that improving one factor may deteriorate another factor of the system. For example, for crowd management systems based on infrastructure-based approaches, while they may be reliable in their estimation of crowd parameters (since they rely on trust- ed devices deployed by event managers), such solutions can be costly from the monetary perspective because they may require a static infrastructure that cannot be used in another area, and it may be destroyed in a disaster event. In contrast, crowd-based approaches may be cheaper to deploy since they rely on crowd devices, but their estimation of crowd parameters may be unreliable because of untrusted data that could be submitted on purpose to exacerbate the disaster. With respect to the network bandwidth consumption in

these systems, it depends on the type of data collected by the crowdsensing system (e.g., real-time video and multimedia data require different QoS compared to the QoS required for location data). Event managers should consider these factors when deploying crowd management systems in emergency and disaster scenarios.

In the rest of this section we highlight aspects in each of the three segments of the CACROM architecture that should be taken into account in the design of future architectures for crowd management for emergency and disruptive scenarios. We also discuss open issues that require further research in the development of these architectures.

Power Segment

Usually, power is considered reliable in communication architectures. However, large-scale emergency events such as the recent Hurricane Maria have shown that power loss in centralized grid systems have a great impact not only on the crowd but also on emergency management personnel and communication equipment. We pro- posed and designed CACROM to highlight the need for power as an important design requirement in communication architectures under emergency scenarios, and the fact that distributed generation (i.e., microgrids) provides a better response to emergencies. This requires not only novel design approaches for resilient power grids, but also the need for educating the public about the importance of keeping backup power that can be brought in during large-scale emergencies.

Communications Segment

The utilization of IP-based networks in CACROM has the major benefit that no special equipment (or modification) is required by the crowd to be part of the crowd management system. However, this approach also requires the availability of an infrastructure similar to the one used every day, which may not be available during an emergency situation. Moreover, different types of data such as multimedia and/or real-time data have different QoS requirements compared to the QoS requirements of crowdsourced data (e.g., location data). Careful management

of the available net- work bandwidth, especially in disaster scenarios wherein the communication segment may be partially damaged, is needed for crowd management systems to be useful and efficient.

Crowd Data Collection And Notification Segment

Location data is important in crowd management systems because many aspects about crowds (e.g., crowd density) can be obtained from this type of data. However, the continuous use of location sensors such as GPS quickly exhausts smartphones' battery power. CACROM provides two mechanisms to minimize the power consumption when using location data. In particular, the critical point algorithm [13] can send 80 percent less location data through the network while still providing enough information to per- form analysis. This saves both network bandwidth and battery power.

Open Research Issues for Crowd Management

We highlight the following open research issues that require further work for crowd management architectures in emergency and disruptive scenarios.

Security: CACROM makes use of devices that are in possession of crowd members to collect data. Therefore, they could use their devices to submit fake data on purpose to exacerbate the emergency and provide further risk to human life or to public/private property. Some solutions that can address this problem exist in the realm of ubiquitous sensor networks and crowdsensing systems. Such solutions make use of techniques such as estimation and filtering approaches, interpolation techniques (kridging), Markov random fields, principal component analysis (PCA), clustering, Gaussian mixture models, and anomaly detection algorithms [14]. However, more research is need- ed to incorporate and develop new techniques to handle this issue in crowd management systems for emergency scenarios.

Participation: The participation of crowds in crowdsensing systems traditionally depend on some type of incentive (either through micropayments, altruistic incentives, or social incentives) that provides a reason for a crowd member to contribute data to the system. If not enough participation takes place, a crowd

management system based on the CACROM architecture may not collect sufficient data to provide an accurate representation of what is currently taking place. More research is needed to better understand crowd participation under emergency/disruptive scenarios.

Privacy: A major issue that is related to the utilization of crowd devices that collect data is privacy. According to the U.S. Department of Health and Human Services' Bulletin on HIPAA Privacy in Emergency Situations [15], disclosures about a patient's health (including identifiable data) can be done in emergency scenarios without previous consent for treatment purposes, in case of imminent danger (to the patient and to others), and to public health authorities (as permitted by the applicable state law and ethical requirements). However, other disclosures must be kept to a minimum for the intended purpose. These rules require that crowd management systems in the United States operating under emergency scenarios must abide by the Health Insurance Portability and Accountability Act (HIPAA) rules with exceptions as described by the rules specified above. As legal privacy protections depend on the juris- diction (i.e., in Europe privacy laws are managed differently), privacy challenges that need to be addressed in the future include how crowd management systems should integrate these privacy rules and the perception of the public about privacy during emergency scenarios.
2 3

Conclusion

The impact of natural and manmade catastrophic events in the last decade has fueled a growing interest in the development of systems for crowd management

---

[2] The utilization of IP-based networks in CACROM has the major benefit that no special equipment (or modification) is required by the crowd to be part of the crowd management system. However, this approach also requires the availability of an infrastructure similar to the one used every day, which may not be available during an emergency situation.

[3] If not enough participation takes place, a crowd management system based on the CACROM architecture may not collect sufficient data to provide an accurate representation what is currently taking place. More research is needed to better under- stand crowd participation under emergency/ disruptive scenarios

in emergency/disruptive scenarios. To handle crowd management in these scenarios this work has proposed the CACROM architecture. We describe and discuss the architecture, and finally provide future research issues that require further attention.

Acknowledgment

We thank the anonymous reviewers for their valuable comments and suggestions.

References

1. A. Berlonghi, “Understanding and Planning for Different Spectator Crowds,” *Safety Science*, vol. 18, no. 4, 1995, pp. 239–47.
2. D. Sharma *et al.*, “A Review on Technological Advancements in Crowd Management,” *J Ambient Intell. Human Comp.*, vol. 9, no. 3, 2018, pp. 485–95.
3. N. Bellomo *et al.*, “Human Behaviors in Evacuation Crowd Dynamics: From Modelling to ‘Big Data’ Toward Crisis Management,” *Physics of Life Reviews*, vol. 18, 2016, pp. 1–21.
4. M. Yamin and Y. Ades, “Crowd Management with RFID and Wireless Technologies,” *Proc. 1st Int’l. Conf. Networks and Commun.*, 2009, pp. 439–42.
5. T. Franke, P. Lukowitz, and U. Blanke, “Smart Crowds in Smart Cities: Real Life, City Scale Deployments of a Smartphone Based Participatory Crowd Management Platform,” *J. Internet Services and Applications*, vol. 6, no 27, 2015, pp. 1–19.
6. Kwasinski, “Lessons from Field Damage Assessments about Communication Networks Power Supply and Infra- structure Performance during Natural Disasters with a Focus on Hurricane Sandy,” *FCC Wksp. Network Resiliency*, New York, NY, Feb. 2013.
7. W. Kongsiriwattana, P. Gardner-Stephen, and M. Lloyd, “Historical Distribution of Duration of Unplanned Power Outages in Queensland: Insights for Sustaining

Telecommunications During Disasters," *Proc. 2017 IEEE Global Humanitarian Tech. Conf.*, 2017, pp. 1–8.

8. P. Meier, "The Unprecedented Role of SMS in Disaster Response: Learning from Haiti," *SAIS Rev. Int'l. Affairs*, vol. 30, no. 2, 2010, pp. 91–103.
9. Kwasinski *et al.*, "Telecommunications Power Plant Dam- age Assessment for Hurricane Katrina — Site Survey and Follow-up Results," *IEEE Sys. J.*, vol. 3, no. 3, 2009, pp. 277–87.
10. D. Abusch-Magder *et al.*, "911-NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations," *Bell Labs Tech. J.*, vol. 11, no. 4, 2007, pp. 113–33.
11. Sinsel, *Supporting the Maritime Information Dominance: Optimizing Tactical Network for Biometric Data Sharing in Maritime Interdiction Operations*, M.S. thesis, U.S. Naval Postgraduate School, 2015.
12. Q.T. Minh *et al.*, "On-the-Fly Establishment of Multihop Wireless Access Networks for Disaster Recovery," *IEEE Commun. Mag.*, vol. 52, no. 10, Oct. 2014, pp. 60–66.
13. S. J. Barbeau *et al.*, "A Location-Aware Framework for Intelligent Real-Time Mobile Applications," *IEEE Pervasive Computing*, vol. 10, no. 3, 2011, pp. 58–67.
14. J. Perez, S. Zeadally, and N. Jabeur, "Security and Privacy in Ubiquitous Sensor Networks," *J. Info. Processing Systems*, vol. 14, no. 2, 2018, pp. 286–308.
15. U.S. Dept. of Health & Human Services, "Bulletin: HIPAA Privacy in Emergency Situations," Nov. 2014; https://bit. ly/2L22MBW, accessed December 2, 2018.

Biographies

Alfredo J. Perez [M] is an assistant professor in the TSYS School of Computer Science at Columbus State University. His research interests include mobile computing/sensing, cybersecurity, and the Internet of Things. He received his B.Sc. in systems engineering from Universidad del Norte, Colombia and his

Ph.D. in computer science and engineering from the University of South Florida. He is a member of the National Academy of Inventors.

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. He received his Bachelor's degree in computer science from the University of Cambridge, England, and his doctorate degree in computer science from the University of Buckingham, England. His research interests include cybersecurity, privacy, the Internet of Things, and energy-efficient networking. He is a Fellow of the British Computer Society and the Institution of Engineering Technology, England.