Journal of Network and Computer Applications 36 (2013) 870–880

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Evaluating opportunistic networks in disaster scenarios

Abraham Martín-Campillo [a,*], Jon Crowcroft [b], Eiko Yoneki [b], Ramon Martí [a]

[a] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, Bellaterra, Spain
[b] Computer Laboratory, University of Cambridge, Cambridge, UK

ARTICLE INFO

Article history:
Received 16 April 2012
Received in revised form
31 October 2012
Accepted 9 November 2012
Available online 27 November 2012

Keywords:
Opportunistic networks
Opportunistic forwarding
Performance evaluation
Emergency scenarios

ABSTRACT

Forwarding data in scenarios where devices have sporadic connectivity is a challenge. An example scenario is a disaster area, where forwarding information generated in the incident location, like victims' medical data, to a coordination point is critical for quick, accurate and coordinated intervention. New applications are being developed based on mobile devices and wireless opportunistic networks as a solution to destroyed or overused communication networks. But the performance of opportunistic routing methods applied to emergency scenarios is unknown today. In this paper, we compare and contrast the efficiency of the most significant opportunistic routing protocols through simulations in realistic disaster scenarios in order to show how the different characteristics of an emergency scenario impact in the behaviour of each one of them.

1. Introduction

Recovery from an emergency situation is always a complex task, particularly in mass casualty disasters. In these scenarios, a quick and coordinated response must be given to improve the efficiency of rescue teams and save as many lives as possible. Furthermore, the emergency situation may be ongoing for some time, hence systems may have to stay usable for extended periods.

The need for these systems is real and the last mass casualty incidents in the recent years have made new applications (Mass casualties, 2009; Geo-pictures, 2010; Hikaru et al., 2011-02-28; Martín-Campillo et al., 2010; Google crisis response; Aschenbruck et al., 2004), designed to satisfy these needs, to appear. These applications ease the work of first responders providing a faster triage of the victims (medical status acquisition), better coordination, and better communication in situations without network infrastructure.

From the communication point of view, in many cases, existing network infrastructure is destroyed by the very nature of the disaster, or it is overloaded or saturated due to a heavy use. This results in the lack of a network through which transmit and share information generated within the emergency. An usual workaround for the problem is the use of Mobile Ad hoc Networks (MANET). This is the case of IMPROVISA (Improvisa) that proposes to solve this difficulty by distributing antennas in the disaster area. Although possible, this may not be feasible in large-scale emergencies. Other authors Martín-Campillo et al. (2010) suggest the use of a wireless opportunistic network (Conti and Kumar, 2010) based on mobile devices carried by emergency personnel to forward the data created and collected in the disaster area to a coordination point.

The use of opportunistic networks is very appropriate for emergency scenarios as they are infrastructure-less; nodes can store, carry and forward messages; and the routes from the sender and the destination are build dynamically. This makes opportunistic networks tolerant to delays and disruptions, and nodes can communicate each other even if there is not any route connecting them. This is very important because in emergency situations the most important objective is to ensure that the messages and data generated in the disaster area reach their destination without any loss as they contain valuable information for the global coordination of the emergency response, as well as information about victims.

However, forwarding data in opportunistic scenarios is challenging (Ye et al., 2009; Pelusi et al., 2006). The number of victims, the quantity of data generated, or the number of nodes, are characteristics that could notably impact on the performance of routing protocols. Because of this, deciding which forwarding method to use in these scenarios is difficult (Wittie et al., 2009).

The purpose of this research is to characterise the performance of a set of routing algorithms in realistic disaster scenarios with different characteristics in order to uncover their performance and therefore their suitability to different scenarios. We have done this performance analysis carrying out several simulations using the mobility model proposed by Aschenbruck et al. (2009), and implemented in U. of Bonn (2009). We have also used the ONE simulator (Keränen et al., 2009), a simulation tool specific for

[*] Corresponding author.
E-mail addresses: abraham.martin@uab.cat (A. Martín-Campillo), jon.crowcroft@cl.cam.ac.uk (J. Crowcroft), eiko.yoneki@cl.cam.ac.uk (E. Yoneki), ramon.marti.escale@uab.cat (R. Martí).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.11.001

opportunistic networks, to simulate the forwarding process based on the traces generated.

This paper is structured as follows: first, the existing related work in disasters areas focused on mobile devices systems, forwarding mechanisms and node mobility is presented. Subsequently, the emergency scenario is depicted, followed by a description of the tests performed. Next, the results of the simulations are shown, analysed, and discussed. We close the paper with our conclusions.

2. Related work

In order to convey the nature of the problem of communications in disaster scenarios, in this section we present related work. We include: applications in emergency scenarios using its own developed network, forwarding protocols in mobile opportunistic networking, and node mobility in disaster areas.

2.1. Applications in emergency scenarios using its own developed network

Mobile devices (PDAs, smartphones, customised, etc.) are frequently used in disaster areas by rescue personnel for different purposes, including victims triage and tracking. The usual problem in emergency situations is the lack of network infrastructures in which rely the communications on. Following are some solutions that propose the use of ad hoc networks, MANETs, satellite, mesh networks, DTNs or opportunistic networks.

ARTEMIS (McGrath et al., 2003) system provides automated remote triage and emergency management information through the use of sensors. Triage information is transmitted using agents that move through a reliable messaging layer in wireless ad hoc networks.

The Mobile Agent Electronic Triage Tag System (Martí et al., 2009) creates mobile agents that store and carry triage information about victims. Mobile agents are able to move through a MANET created by mobile devices without the need of an end-to-end connection from the origin to the destination. Time To Return (TTR) is used for the mobile agent migration decision.

CodeBlue (Lorincz et al., 2004) is a system that uses sensors to triage and track victims and monitor their vital signs. The transmission of data is done using wireless sensor networks created by the sensors deployed.

TacMedCS, Tactical Medical Coordination System (Williams, 2007), is a military system to capture and display real-time casualty data in the field. In this case, a handheld unit stores the casualty data and the GPS position and uses satellite (Iridium) communication to send it. IEEE 802.11 mesh communications can also be established between the different handheld units for their collaboration.

Haggle Electronic Triage Tag (Haggle-ETT) (Martín-Campillo et al., 2010) is a system that uses Haggle (Nordström et al., 2009) and mobile devices to create electronic triage tags (ETTs) and transmit them using wireless opportunistic communications, without requiring a direct connection with the receiver, or receivers.

2.2. Forwarding in mobile opportunistic networking

Traditional network paradigms assume an existing end-to-end connection between the sender and the receiver. These networks do not accept excessive delays or disruptions, hence when this happens the delivery fails. But for some scenarios such as deep space communications, where nodes are not always in communication range, a type of network that supports intermittent communications is needed. Delay and disruption Tolerant Networking (DTN) (Farrell et al., 2006) is designed to support the disruption of connectivity and/or long delivery delays and has become popular in environments such as disasters areas or developing countries.

DTNs use the store and forward approach, as well as the store, carry, and forward approach if nodes have the ability to move. Nodes carry messages stored in their memory while moving around and forward them when they find an opportunity. One type of DTNs is opportunistic networking, where contacts are heterogeneous and unpredictable, hence nodes do not know when they will contact with another node or which node it will be. Routes from the sender to the destination of a message are built dynamically and any possible node can opportunistically be used as next hop if it is more likely to bring the message closer, or faster, to the final destination. For all these reasons forwarding data in opportunistic networks is challenging. The different forwarding mechanisms base these decisions on different type of information and different strategies. The features of the most significant forwarding algorithms are explained below.

2.2.1. Epidemic forwarding

Epidemic (Vahdat and Becker, 2000) is a well-known forwarding strategy. It is based on the very simple idea of replicating all the messages stored in a node to all the nodes that come into contact with it during its journey. This results in a higher probability of delivering the message as more nodes have a copy of each message but it can also produce network congestion. One of the variations for Epidemic forwarding is Epidemic with ACK. This modification eliminates all the copies of a message in the network when the ACK for this message (generated when it is delivered to its destination) is received. Nevertheless, the ACKs generated also produce additional traffic.

2.2.2. PRoPHET forwarding

PRoPHET forwarding (Probabilistic Routing Protocol using History of Encounters and Transitivity; Lindgren et al., 2004) uses an algorithm based on encounters to indicate how likely is each node to deliver a message to a destination in order to make forwarding decisions. The probabilities stored in a node are exchanged when they meet other nodes. Then, each node updates its values by increasing the probability for the nodes that have been found and by decreasing the probability for the rest. Based on these values, it is calculated which node is more likely to deliver the message. Finally, messages are only forwarded to another node if this one has higher delivery probability.

2.2.3. MaxProp forwarding

MaxProp forwarding (Burgess et al., 2006) is based, like PRoPHET, on the use of information about probability of future contacts with nodes when deciding if a message has to be forwarded. Unlike PRoPHET, MaxProp uses a priority queue that is used to discard messages that have little chance of being delivered to its destination and to keep those which are more likely. MaxProp uses a directed graph with weights based on encounters, with a variation of Dijkstra's algorithm to calculate the lowest path cost and, therefore, the delivery probability of each node. Furthermore, MaxProp has several other mechanisms and policies to increase delivery ratio: message prioritisation, hashed ACK, etc. One of these policies is to prioritise the forwarding of messages with lower hop count (even with low delivery likelihood), thus reducing their isolation, expanding their dissemination, and therefore increasing their chance of reaching the destination.

2.2.4. Delegation forwarding

In Delegation forwarding (Erramilli et al., 2008), each node has an associated value which is created using a metric that represents the quality of the node as relay. The metric used depends on the scenario where it will be used. Erramilli et al. (2008) propose a generalisation of forwarding methods such as BUBBLE Rap (Hui et al., 2008).

Time To Return (TTR) forwarding: In Martí et al. (2009), a routing protocol designed for disaster scenarios is proposed: Time To Return (TTR). Medical personnel in an emergency scenario are coordinated by a leader, who tells personnel where to go, or in which area to work (Martí et al., 2009), and assigns a maximum time to return to the base for security reasons. Each node has its own time to return (TTR) and therefore the forwarding protocol takes advantage of the existence of this value to use it to make forwarding decisions. If a node contacts another node with a lower TTR, it relays all its messages to this node and, if the messages have been successfully received, the sender deletes all messages relayed in order to have only one copy of them throughout the network. Hence, TTR is a single message copy forwarding mechanism.

Traditional routing algorithms usually only maintain one copy of the message in the network. When a router forwards a message to another router, it does not keep a copy of the message. In opportunistic networks it is the opposite, forwarding methods usually keep a copy of the message to increase the chances of delivering the message or deliver it faster. Nevertheless, there are some exceptions in opportunistic routing like Time To Return (TTR) forwarding.

2.3. Node mobility in disaster areas

Node movements in disaster areas cannot be completely predicted because the emergency scenario is different in each case, victims have different locations and the number of first responders working on the emergency is different. Anyway, some parts can be modelled; the disaster scenario can be divided into areas: the incident location, patients waiting for treatment area, casualties clearing stations, the rescue vehicles parking point, and the technical operational command (as can be seen in Fig. 1). These areas have different purposes and nodes move inside them and from one to another. Taking into account all these concepts about disaster areas, Aschenbruck et al. (2009) made an analysis of disaster scenarios and proposed a mobility model. We have used this mobility model, implemented in U. of Bonn (2009), to create the traces for the simulations, and The ONE simulator (Keränen et al., 2009) to simulate the forwarding process. This mobility model has been previously used in the literature (Reina et al., 2011) to evaluate a set of routing protocols in ad hoc networks.

3. Disasters recovery process

This work focuses on finding the behaviour of the most popular forwarding methods in opportunistic networks in disaster areas. In this section, the disaster scenario will be described, including its important parts, the actors involved, and the recovery process. This is important in order to understand how the routing protocols will behave in the simulations and to interpret the results.

The disaster recovery process is similar in all type of emergencies: triage, stabilisation and transportation of victims. Worst emergency scenarios usually are mass casualty incidents (MCIs), whose main characteristic is the large number of victims.

The triage of the victims is always the first and foremost phase in an emergency scenario and it is done by the first response personnel arriving at the emergency scene. Triage is the process of sorting casualties into groups based on their medical condition. Consequently, medical personnel arriving later will know which victims need more urgent attention. Victims are attended and stabilised in triage order before they are evacuated to a casualties clearing station or an hospital where they will be treated widely.

Once the triage is complete, rescue teams extract those victims who are trapped or cannot move from the the incident location to a safe place. If a casualties clearing station is installed, victims are evacuated there. If there are more than one station, a victims waiting for treatment area can exist. A casualties clearing station is a mobile (or field) hospital to treat the victims before they can be moved to a hospital. In MCIs, where it is necessary to treat lots of victims in a serious condition, casualties clearing stations are essential and have to be installed near but in a reasonable distance from the incident location to be a safe place.

Nodes move victims from the incident site to the casualties treatment area. Hence, nodes go periodically from one area to another during the disaster (acting like a data mule).

Once in a casualty clearing station, the main objective of the medical personnel there is to stabilise the patients. Once the stabilisation is done, a rescue vehicle is called to pick each victim up to transfer them to the hospital.

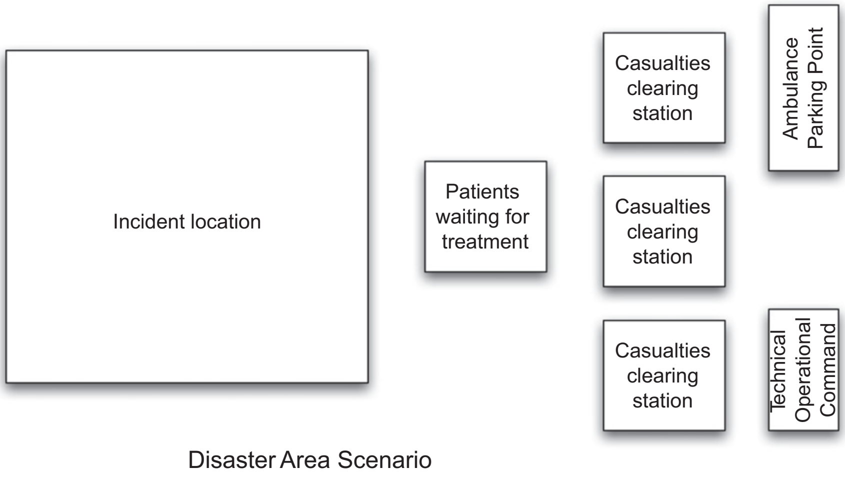
Incident location
Patients waiting for treatment
Casualties clearing station
Casualties clearing station
Casualties clearing station
Ambulance Parking Point
Technical Operational Command
Disaster Area Scenario

Fig. 1. Disaster area scenario.

The technical operational command is where the coordination team is, and where all the decisions about actions to be carried out by rescue and medical teams are taken.

3.1. Communications in the emergency scenario

Traditionally emergency communications were focused on voice, but advanced communication mechanisms are being adopted. The low price of Internet enabled mobile devices using Wi-Fi or mobile phone networks have eased this process. But in most disasters, like hurricanes, terrorist attacks, earthquakes, etc., these networks become unstable, inaccessible, overused or even destroyed, and as a consequence, emergency personnel cannot rely on the use of these existing network infrastructures and may deploy and use their own or look for other solutions.

Some of these solutions may have shortcomings. For example, if the emergency area is large, it is possible that some solutions as MANETs could not work because the impossibility of creating a fully connected network. Thus, an attempt to communicate from one point of the network to another may be unsuccessful as an end-to-end communication path is needed. Another example is the deployment of repeaters to supply an infrastructure, but this solution may require a long time to deploy.

Data generated within an emergency scenario are always considered critical and cannot be lost. Furthermore, disruptions can occur because of the emergency itself, therefore disruption tolerant networks may need to be considered. In these cases, the use of opportunistic networks (delay and disruption tolerant) may be considered as a solution. But different forwarding mechanisms can be used on top of them, and therefore, produce different results. In the next sections of this paper we analyse the behaviour of the most relevant routing solutions for its use in emergency scenarios.

Having Internet connection is very important for coordination or information purposes (e.g. with another technical operational command, hospitals, government, etc.). For this reason, it is assumed that some parts of the emergency, for instance casualties clearing stations or the technical operational command, have persistent Internet connectivity even if the network infrastructure is destroyed or unusable, e.g. using satellite connections.

4. Evaluation

Disaster scenarios are unpredictable, its area or the number of victims are data that cannot be precisely predicted. Furthermore, emergencies are heterogeneous because each disaster produced has different numbers of victims (that can be closely related to the number of messages created), different numbers of people working on the emergency, etc. As the characteristics of a disaster scenario considerably change from one to another, it is very important to carry out simulations that test the performance impact of these disaster scenarios characteristics in each forwarding protocol.

We have selected four of the most relevant opportunistic routing protocols for emergency scenarios: Epidemic, MaxProp, PRoPHET, and TTR. This evaluation, tests the selected protocols through simulations in a set of emergency scenarios with different characteristics: different values of number of nodes, number of messages, and message size, in order to evaluate their impact on the performance.

Results are expressed in charts as delivery ratio, overhead ((number of messages relayed–messages delivered)/messages delivered), and energy cost per message (number of messages relayed/messages created) metrics. We have also included several tables at the end of the paper with a summary of all the results from the simulations (average hops, throughput, or delivery delay).

4.1. Routing protocols

There are plenty of forwarding methods in the literature but we cannot test all of them, hence we have chosen those that we consider more relevant for opportunistic networks and, in this special case, for emergency scenarios.

We have chosen three popular routing methods in the literature for doing the simulations, Epidemic, PRoPHET and MaxProp, together with another forwarding method, TTR, that is special for disaster situations. In the following lines is a brief explanation of the motivation why they have been selected:

- *Epidemic*: This method has been chosen because of its message spread. It is a reference for other routing methods. It is also very well known for flooding the network because of the replication of each message to the rest of the nodes.
- *PRoPHET*: It is a probabilistic routing method that aims to improve Epidemic routing with higher delivery ratio due to the use of probabilities. This protocol is well known in opportunistic networks and it is usually used, as Epidemic, in comparisons.
- *MaxProp*: It does an estimate delivery likelihood and adds some rules to the decision as to give forwarding preference to low-hop-count messages, to free up storage of delivered messages or to not forward the same message twice to the same next hope destination. This approach is very important as it gives a congestion control mechanism to MaxProp, that is a interesting feature to test.
- *TTR*: This is a routing method specific for disaster areas, based on the use of the "Time to Return" as a forwarding decision. In contrast to the other protocols, TTR only keeps one copy of the message throughout the network: when a message is relayed, it is deleted from the sender. This makes this protocol very energy saver but also penalises its delivery ratio.

In the last few years a lot of forwarding protocols based on social networks have arisen for opportunistic networks (SimBet Daly and Haahr, 2007; PeopleRank Mtibaa et al., 2010 or BUBBLE Rap Hui et al., 2011). However, these routing methods cannot be used in emergency scenarios because they use information that is not available under disaster situations.

4.2. Simulation set-up

We use the Disaster Area mobility model proposed by Aschenbruck et al. (2009) implemented in BonnMotion U. of Bonn (2009) to create the traces used for the simulation. This mobility model defines five main areas in the emergency scenario: the incident location, the patients waiting for treatment area, the casualties clearing stations, the ambulance parking point, and the technical operational command (Fig. 1).

For the simulation, two zones have been defined: one zone 0 (incident location) and one zone 1. Zone 1 is where nodes from zone 0 go, and can be a patients waiting for treatment area, or a casualties clearing station, or both. We have defined as a destination point for the messages, a node in the entry point of the zone 1 as we consider network connection inside this zone. We have not taken into account other elements in the simulations, as the ambulance parking point, because we consider the message delivered once it arrives to the zone 1. We also consider in zone 1, a satellite, or another type of, network connection that communicates the disaster area with the exterior, an essential requirement for coordination. The duration of the simulation is of 6000 s.

Three main characteristics of an emergency scenario are tested in the simulations to see how they impact in the performance of the forwarding protocols: number of nodes (density of nodes of the scenario), number of messages created (that can also be interpreted as number of casualties) and message size.

All the nodes in the scenario share the same attributes (link speed, radio range, etc.). A link speed of 54 Mbps and a radio range of 60 m are the values defined for all the nodes. The link speed is chosen using the 802.11 g standard. The maximum radio range is a parameter that can be different depending of the device the user is using: we carried tests outdoor with obstacles using iPhones 3GS, that gave us an average result of 60 m. Regarding this value, in Section 5.1 we have tested a disaster scenario with different densities of nodes. Since having shorter radio range is similar to having less density of nodes or a larger scenario, these results can be extrapolated to know which results would be obtained for radio ranges longer, or shorter than 60 m. Messages are originated in randomly chosen nodes with a size of a message size of 128 kB (size for a text and an image) and are created throughout all the simulation time. We have also tested the performance impact of the messages size in each one of the forwarding protocols. Table 1 sums up the common simulation parameters for all the simulations.

4.3. Energy efficiency

The energy efficiency of forwarding methods in emergency scenarios is very important. This importance is mainly due to two reasons: the first one is that in these scenarios mobile devices are heavily used, and its battery is limited, so if it is drained fast the node will be off and the messages will not arrive. The second is that the duration of an emergency is unknown, hence the battery life has to be preserved against the overuse.

According to recent works (Balasubramanian et al., 2009a; Rice and Hay, 2010), Wi-Fi is one of the most energy consuming elements of a mobile phone device. “An analysis of power consumption in a smartphone” (Carroll and Heiser, 2010) states that the network can consume up to 725 mW when transferring data at full capacity. Furthermore, when a mobile device is using its Wi-Fi network in opportunistic mode, it cannot enter in PSM (Power Safe Mode) because it looks constantly for nodes and so it spends a lot of energy scanning the network and associating with the nodes met (Balasubramanian et al., 2009a). These studies measure the energy consumption based on an specific model of mobile phone. Knowing exactly how many Watts a node will consume when transferring a message, highly depends on the model of the mobile device, the network chipset, etc. For this reasons we have extracted the common values for all the forwarding methods to measure an independent value that does not depend on the mobile device the user is using.

The contacts between nodes or the messages size are elements that are common in all the forwarding protocols when we test them using the same traces and simulation parameters. Hence, the parameter that defines the energy consumed by a forwarding protocol is the number of messages relayed (Balasubramanian et al., 2009b). We define an energy cost per message as the number of messages relayed divided by the number of messages created. Therefore, we can measure and compare the cost between different forwarding methods regardless of the message size or the number of message created.

Table 1
Values for the simulation parameters.

Parameter		Value
Network	Simulation time	6000 s
	PHY data rate	54 Mbps
	Radio range	60 m
	Buffer size	7.5 MB
Mobility	Model	Disaster Area (Aschenbruck et al., 2009)
	Zone 0	700 × 600 m
	Zone 1	50 × 50 m
PRoPHET	Pinit	0.75
	β	0.25
	γ	0.98
MaxProp	Meeting Prob Max Set Size	50
	α	1

5. Simulation results

In this section we present and discuss the results obtained after performing the simulations. We want to analyse how the chosen routing methods behave in emergency scenarios with different characteristics in number of nodes, number of messages and message size. We will examine the performance impact of each characteristic in each routing method.

5.1. Number of nodes

The number of nodes is the sum of all the devices that can communicate between them in an opportunistic way. Those can be sensors, mobile devices carried by the personnel working in the emergency (medical, firefighters, etc.) or other types of devices. The density of nodes depends on many factors: personnel involved, devices available, etc. For this reason we evaluate the performance of the selected forwarding protocols with different numbers of nodes. Table 2 shows the values of the parameters for these simulations.

In terms of delivery ratio, in Fig. 2 we see that MaxProp has the highest delivery ratio. As the number of nodes grows, so do the delivery ratio and the cost per message (Fig. 4) of MaxProp,

Table 2
Values for parameters for “number of nodes” based simulations.

Parameter	Value
Message generation rate	1 message/s
Message size	128 kB

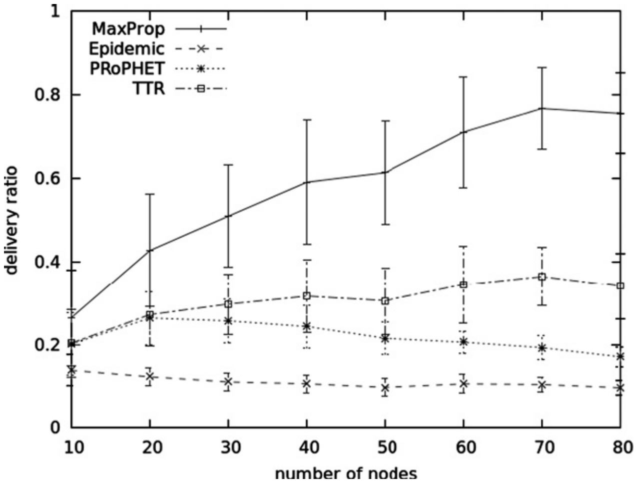

Fig. 2. Delivery ratio vs. number of nodes.

because more message relays are done. Regarding Epidemic and PRoPHET, both have a high energy cost. PRoPHET includes probabilistic information when deciding whether a message should be relayed or not, which improves the delivery ratio of Epidemic, although adding probabilities to the decision making works better for few nodes.

Using Epidemic, buffers become full and nodes are forced to drop the oldest messages to make room for new ones. This can produce the relay of messages that had previously been relayed to this node, increasing the overhead (Fig. 3) and the cost (Fig. 4). As we can see in Fig. 2, the delivery ratio of Epidemic is very low.

If we look more deeply in MaxProp results, we will find that its good results are due to two main characteristics of this routing method. MaxProp deletes those message in the buffer with lowest delivery likelihood when freeing up space for new messages. In addition, it sends messages to other nodes in specific order that takes into account message hop counts and message delivery probabilities based on previous encounters. These two characteristics provide a good congestion control and a better distribution of messages. Therefore, for MaxProp, having more nodes in the emergency scenario means better results.

For TTR, its results in delivery ratio improve those of Epidemic and PRoPHET thanks to the use of the data mules approach in emergency scenarios. Nodes go back and forth to the zone 1 where they deliver the messages. TTR takes advantage of that by using this information in the forwarding decision and thus forwarding the messages only to those nodes that have better chances of delivering the message sooner. However, its single-message policy (TTR passes the message, instead of duplicating it, to the neighbour) makes this forwarding protocol lose opportunities to relay messages to better nodes, producing a delivery ratio far below MaxProp.

Comparing overheads in Fig. 3, Epidemic is the routing method that produces more transmissions per delivered message while TTR is the one that produces less. Analysing the results we can also say that as the number of nodes grows, so does the number of messages relayed in all routing methods because there are more relay opportunities (nodes).

Figure 4 shows a higher cost when the number of nodes grows also because more message relays are done. TTR maintains a lower cost due to its single-copy forwarding policy that produces few message relays. In this figure, TTR shows its potential as a low cost routing protocol. The rest of methods grow linearly with a bigger slope.

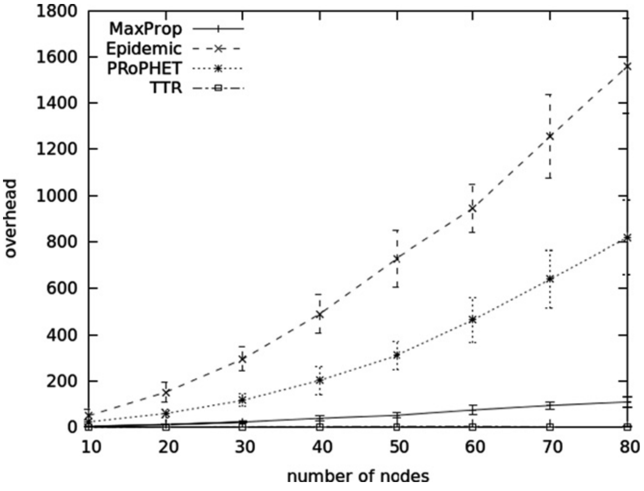

Fig. 3. Overhead vs. number of nodes.

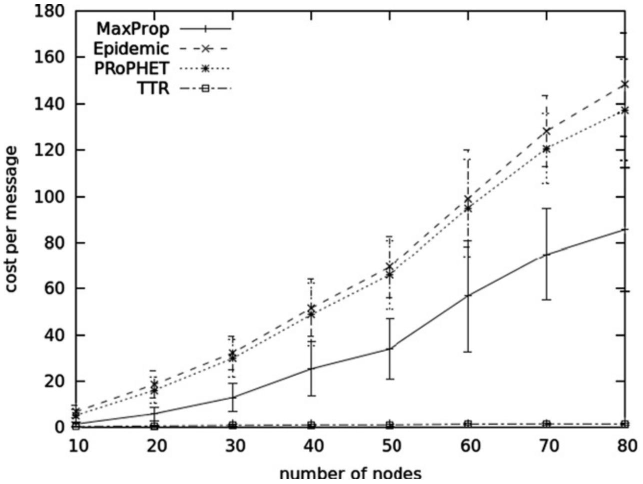

Fig. 4. Cost per message vs. number of nodes.

5.2. Number of messages

In an emergency scenario, a message can be generated by a mobile device of personnel working in the disaster area to inform about a victim found, triage information, an update in their health status or other information about the scenario. Sensors attached to victims can also generate several number of messages (Lorincz et al., 2004), hence we can say that it would probably exist a correlation between the number of victims in an incident location and the number of messages generated. In this third set of simulations the focus is on the analysis of how the number of message impacts the routing protocols performance. Table 3 shows the specific parameters for these simulations.

For the delivery ratio, see Fig. 5, the results show that MaxProp performs much better than any other method, achieving almost 100% of messages delivered for low number of messages. PRoPHET also behaves very well for low number of messages and its delivery ratio decreases as the number of messages increases.

Table 3
Values for parameters for "number of messages" based simulations.

Parameter	Value
Number of nodes	50
Message size	128 kB

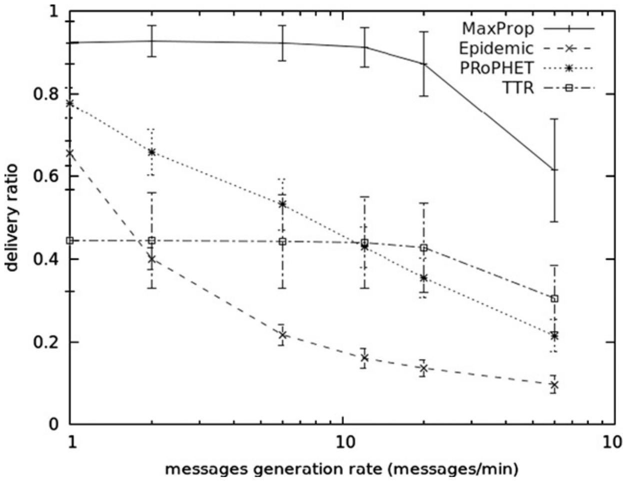

Fig. 5. Delivery ratio vs. number of messages generated per minute.

This last behaviour is the same for all the methods, their performance decrease when the number of message increases, as the buffers of more nodes become full. The protocols without congestion control are more affected than MaxProp as it can be seen in Fig. 5. TTR is less affected by the change of the number of messages created because the nodes have fewer messages to relay due to its single-copy policy and buffers do not become full. Although the delivery ratio performance is less affected by the increase of the number of messages, its delivery ratio is also low.

Figure 7 shows for Epidemic and PRoPHET that the cost per message decrease when the message rate increase because there are more messages created but the number of messages relays do not increase in the same percentage. The number of relays per message for MaxProp and TTR are constant for different message generation rate.

The cost of delivering a message (Fig. 6) decreases when the message generation rate is higher more messages are delivered (not the delivery ratio) but the number of messages relays do not increase in the same percentage.

We can observe in Figs. 6 and 7, and Tables 7 and 8 that a lot of relays are done for low number of messages in Epidemic as well as in PRoPHET.

5.3. *Message size*

In this set of simulations we test how message size impacts. Table 4 shows the specific parameters for these simulations.

In Fig. 8 we observe that the delivery ratio for each routing method decreases when the message size increases. The performance drop is more severe for the Epidemic and PRoPHET methods. These two protocols and MaxProp produce a high delivery ratio for small messages, but Epidemic and PRoPHET are more affected by the increment of the message size. In case of small messages where the buffers are not full, all the messages can be copied and, therefore, the forwarding strategy is less important because all nodes can have a copy of the message. For large messages, MaxProp is also the best method. When the size of the messages grows, a good congestion control and forwarding strategy is very important as Fig. 8 shows.

Regarding the overhead, in Fig. 9 we see how it increments due to the decrease of the delivery ratio. But for Epidemic, when the message size is bigger than 128 kB, the number of messages relayed decreases faster than the number of messages delivered,

Table 4
Values for parameters for "message size" based simulations.

Parameter	Value
Message generation rate	1 message/s
Number of nodes	50

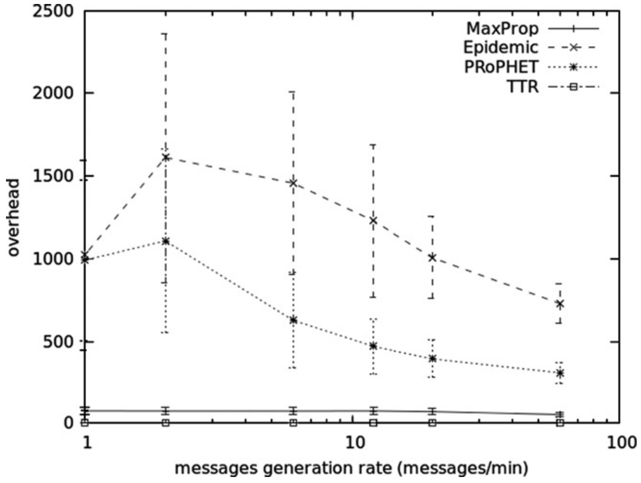

Fig. 6. Overhead vs. number of messages generated per minute.

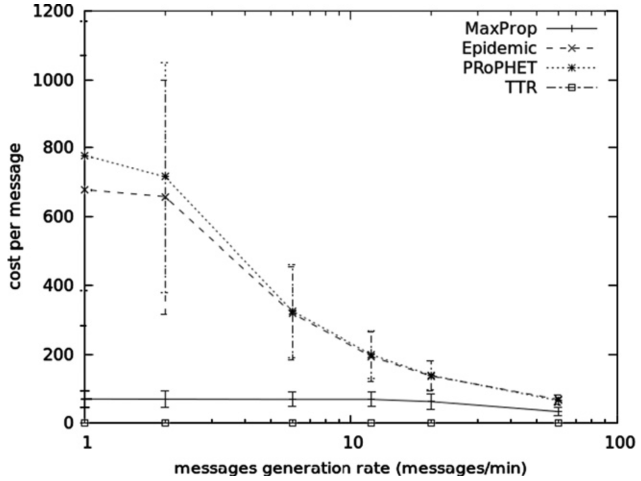

Fig. 7. Cost per message vs. number of messages generated per minute.

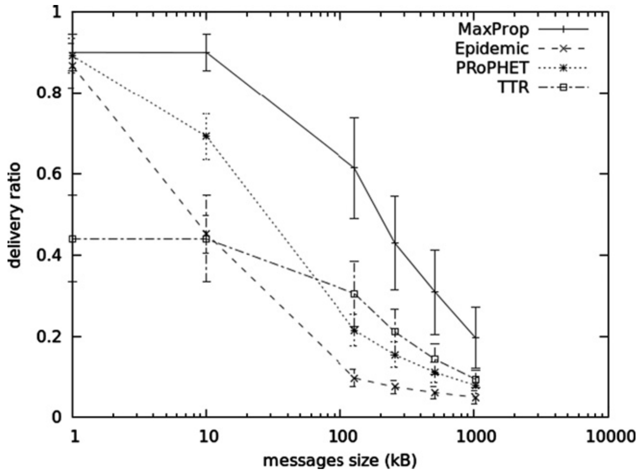

Fig. 8. Delivery ratio vs. message size.

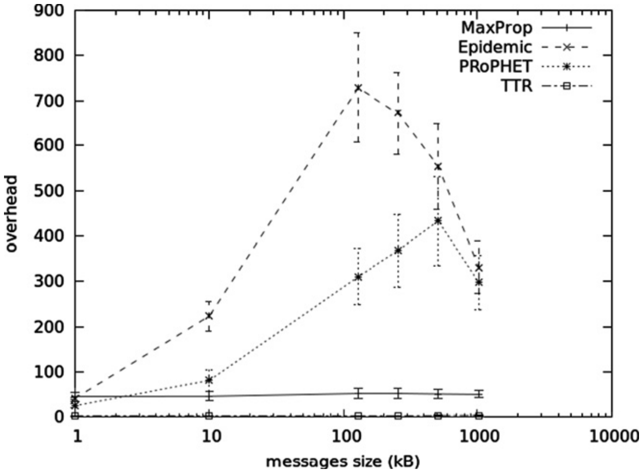

Fig. 9. Overhead vs. message size.

causing the decrement of its overhead. As in other charts, MaxProp and TTR are less affected.

In terms of cost per message we see in Fig. 10 the same problems mentioned above. In this case, MaxProp also reduces the cost per message, doing less relays per message. Regarding TTR, it is also affected by the message size, although it only carries one copy of the message in all the network.

6. Discussion

In this section we want to discuss the results obtained in the previous section. From these results we can say that MaxProp has a very good performance in terms of delivery ratio for almost all emergency scenarios regardless of its characteristics. It is the method with most messages delivered. All other methods are significantly worse in terms of delivery ratio with a few exceptions.

However, if we consider overhead or cost, then the results are different. In this case, the routing method with best results is always TTR as it keeps only one copy of the message throughout the network and it is designed for emergency scenarios. This means that TTR is the most efficient (less overhead) forwarding method and the one that consumes less energy (less cost). In terms of delivery ratio, TTR has better results than Epidemic and PRoPHET in scenarios with high number of messages or big messages where these approaches produce network congestion. In scenarios with few or lightweight messages (where buffers can store a lot of messages), the Epidemic approaches have better results than the TTR one.

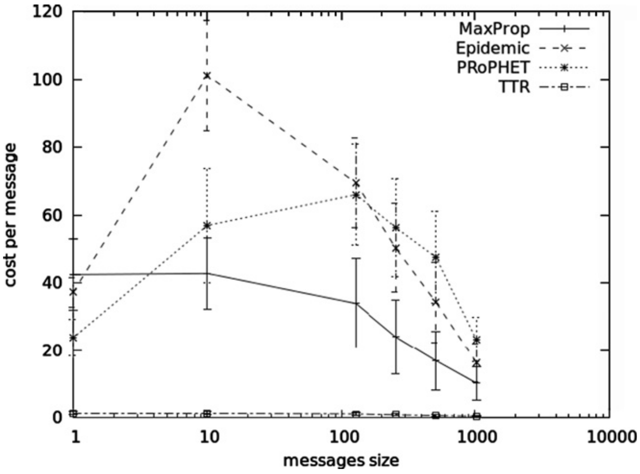

Fig. 10. Cost per message vs. message size.

Taking into account these results, in an emergency scenario where we require the fastest delivery method, hence the method with highest delivery ratio in a given time, we would choose MaxProp. However, choosing MaxProp will produce a high power consumption and will drain the battery fast. In some cases the battery will not last until the end of the emergency resulting in loss of messages and nodes. Emergency scenarios with a high density of nodes in the incident location or with a lot of messages created will cause a high energy cost for MaxProp. If one of these cases is foreseen, a more energy efficient forwarding method should be used. If TTR is used, the battery of the nodes will last much longer. This would have as a consequence a poorer delivery ratio but the node will not be switched off during the emergency that can cause a delay in the delivery of the messages carried by that node.

We must remember that all nodes will eventually come back to the coordination point once the emergency will come to an end, hence all messages will be delivered at some point and no one will be lost. Hence, the fastest delivery method is the one that delivers more messages while the emergency is ongoing.

The following summarises the key aspects of each of the routing protocols:

MaxProp

++ Excellent delivery ratio in almost any situation thanks to its congestion control protocol and forwarding decision algorithm.

+ Satisfactory energy cost performance for low number of nodes or messages.

– Elevated consumption for scenarios with high number of nodes or small size messages.

TTR

++ Very good energy cost in all situations thanks to its single message copy policy.

+ Good delivery ratio in scenarios with high number of nodes or number of messages.

– Poor delivery ratio in scenarios with small message size or low number of messages.

ProPHET and Epidemic

+ Good delivery ratio in scenarios with small size messages or low messages generation rate where no congestion is produced.

+ Good cost in scenarios with small size messages.

–– Elevated energy cost and overhead except for small size messages simulations.

Table 5
Results summary for 10 and 30 nodes.

Number of nodes	**10**				**30**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	25.71	33.81	17.64	25.97	32.82	65.18	14.09	38.03
Delivery ratio	0.20	0.26	0.14	0.20	0.26	0.51	0.11	0.30
Overhead	24.42	4.78	51.19	0.88	117.48	23.46	295.55	2.06
Cost per message created	5.29	1.55	6.88	0.40	29.95	13.00	32.31	0.94
Avg hops count	1.49	1.31	3.02	1.40	2.88	2.36	7.21	2.40
Delivery Delay CDF (60 s)	0.06	0.07	0.05	0.07	0.06	0.11	0.05	0.08
Delivery Delay CDF (600 s)	0.19	0.22	0.14	0.20	0.17	0.37	0.10	0.26
Delivery Delay CDF (1800 s)	0.20	0.26	0.15	0.21	0.25	0.47	0.12	0.30
Delivery Delay CDF (3000 s)	0.20	0.26	0.15	0.21	0.26	0.50	0.13	0.30
Delivery Delay CDF (4200 s)	0.20	0.27	0.15	0.21	0.26	0.51	0.13	0.30
Delivery Delay CDF (5400 s)	0.20	0.27	0.15	0.21	0.26	0.52	0.13	0.30

Finally, tables with a summary of specific values extracted from the different simulations presented in figures from 2 to 10 are included. Tables 5 and 6 show a summary with the values of the tests for different number of nodes (10, 30, 50 and 70). Tables 7 and 8 show the summary for different message generation rates per minute (1, 2, 6 and 12). And finally, Tables 9 and 10 show the summary for different message sizes (1 kB, 10 kB, 256 kB and 512 kB).

7. Conclusions

Recently there has been a growing interest in emergency management systems, and the victims triage process or the coordination of rescue teams are key aspects of these systems. Many of them rely on the availability of a network infrastructure, which in a real emergency scenario may be damaged or overused and unavailable, as we have seen in recent events such as the hurricane Sandy in the East Coast of the United States or the earthquake in Japan. There are several approaches to solve this problem: to create a fully-connected mobile ad hoc network between all the mobile devices used in the disaster area; to deploy a full-coverage network (scattering repeaters) in the disaster area; or to use opportunistic delay and disruption tolerant networks to provide a network of not fully connected nodes. The last option does not require time to deploy repeaters before using the solution and it can also be employed in wide disaster areas where an ad hoc network cannot be fully connected with only a few nodes. For the opportunistic networking approach, there are several forwarding methods that can be used, and it may not be obvious how to decide which provides the best performance for a given scenario.

Table 6
Results summary for 50 and 70 nodes.

Number of nodes	**50**				**70**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	27.48	78.50	12.43	39.07	24.63	98.16	13.29	46.59
Delivery ratio	0.21	0.61	0.10	0.31	0.19	0.77	0.10	0.36
Overhead	310.45	52.54	728.82	2.77	639.97	95.09	1254.62	3.39
Cost per message created	66.08	33.94	69.44	1.17	120.72	74.98	128.13	1.62
Avg hops count	4.13	3.27	10.90	3.03	5.12	4.21	12.12	3.75
Delivery Delay CDF (60 s)	0.05	0.12	0.04	0.07	0.05	0.16	0.05	0.09
Delivery Delay CDF (600 s)	0.12	0.42	0.09	0.26	0.12	0.54	0.10	0.31
Delivery Delay CDF (1800 s)	0.19	0.55	0.11	0.30	0.18	0.69	0.12	0.36
Delivery Delay CDF (3000 s)	0.21	0.59	0.12	0.31	0.19	0.74	0.13	0.37
Delivery Delay CDF (4200 s)	0.21	0.61	0.12	0.31	0.20	0.76	0.13	0.37
Delivery Delay CDF (5400 s)	0.21	0.62	0.12	0.31	0.20	0.77	0.13	0.37

Table 7
Results summary for one messages/min and two messages/min.

Message gen. rate	**1 message/min**				**2 messages/min**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	1.66	1.97	1.40	0.95	2.81	3.96	1.71	1.89
Delivery ratio	0.78	0.92	0.65	0.44	0.66	0.93	0.40	0.44
Overhead	990.14	74.88	1019.88	2.47	1106.71	74.12	1609.86	2.48
Cost per message created	777.50	70.85	677.79	1.59	715.09	70.29	657.40	1.58
Avg hops count	4.47	6.72	6.44	3.43	4.47	6.72	6.75	3.43
Delivery Delay CDF (60 s)	0.09	0.21	0.12	0.09	0.07	0.20	0.08	0.08
Delivery Delay CDF (600 s)	0.46	0.69	0.48	0.32	0.32	0.68	0.29	0.32
Delivery Delay CDF (1800 s)	0.71	0.90	0.66	0.45	0.59	0.90	0.41	0.44
Delivery Delay CDF (3000 s)	0.76	0.94	0.68	0.46	0.65	0.94	0.43	0.45
Delivery Delay CDF (4200 s)	0.77	0.95	0.69	0.47	0.67	0.95	0.43	0.46
Delivery Delay CDF (5400 s)	0.78	0.95	0.69	0.47	0.67	0.95	0.43	0.46

Table 8
Results summary for six messages/min and 12 messages/min.

Message gen. rate	**6 messages/min**				**12 messages/min**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	6.79	11.81	2.78	5.66	10.96	23.37	4.10	11.24
Delivery ratio	0.53	0.92	0.22	0.44	0.43	0.91	0.16	0.44
Overhead	627.70	73.61	1455.06	2.41	469.99	74.51	1227.58	2.37
Cost permessage created	326.46	69.41	319.63	1.55	199.40	69.57	193.83	1.52
Avg hops count	4.45	6.48	8.01	3.36	4.32	5.71	9.29	3.31
Delivery Delay CDF (60 s)	0.06	0.19	0.06	0.08	0.06	0.18	0.05	0.08
Delivery Delay CDF (600 s)	0.23	0.66	0.17	0.31	0.20	0.64	0.13	0.31
Delivery Delay CDF (1800 s)	0.44	0.88	0.23	0.43	0.36	0.85	0.17	0.42
Delivery Delay CDF (3000 s)	0.50	0.92	0.24	0.45	0.41	0.91	0.18	0.44
Delivery Delay CDF (4200 s)	0.53	0.94	0.25	0.45	0.44	0.92	0.19	0.44
Delivery Delay CDF (5400 s)	0.53	0.94	0.25	0.45	0.44	0.93	0.19	0.45

Table 9
Results summary for 1 kB and 10 kB messages.

Message size	**1 kB**				**10 kB**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	0.89	0.90	0.87	0.44	6.91	9.00	4.51	4.40
Delivery ratio	0.89	0.90	0.87	0.44	0.69	0.90	0.45	0.44
Overhead	25.54	45.93	41.85	2.21	81.60	46.29	223.81	2.21
Cost per message created	23.81	42.52	37.26	1.45	57.00	42.83	101.17	1.45
Avg hops count	3.02	4.70	4.63	3.17	2.56	4.71	3.13	3.17
Delivery Delay CDF (60 s)	0.08	0.14	0.14	0.08	0.06	0.14	0.06	0.07
Delivery Delay CDF (600 s)	0.53	0.62	0.59	0.33	0.34	0.61	0.28	0.31
Delivery Delay CDF (1800 s)	0.81	0.86	0.82	0.45	0.61	0.85	0.42	0.43
Delivery Delay CDF (3000 s)	0.86	0.91	0.88	0.46	0.68	0.90	0.47	0.45
Delivery Delay CDF (4200 s)	0.89	0.93	0.89	0.47	0.70	0.92	0.48	0.46
Delivery Delay CDF (5400 s)	0.89	0.93	0.90	0.47	0.71	0.92	0.48	0.46

Table 10
Results summary for 256 kB and 512 kB messages.

Message size	**256 kB**				**512 kB**			
Protocol	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**	**PRoPHET**	**MaxProp**	**Epidemic**	**TTR**
Throughput (kBps)	39.60	109.86	19.20	53.89	56.87	157.95	31.41	73.20
Delivery ratio	0.15	0.43	0.08	0.21	0.11	0.31	0.06	0.14
Overhead	367.66	52.70	671.59	3.26	432.96	51.46	553.42	3.72
Cost per message created	56.41	24.06	50.35	0.92	47.59	16.91	34.33	0.69
Avg hops count	4.05	3.05	10.51	2.77	3.72	2.88	9.14	2.39
Delivery Delay CDF (60 s)	0.05	0.12	0.04	0.07	0.05	0.12	0.04	0.07
Delivery Delay CDF(600 s)	0.11	0.33	0.08	0.20	0.10	0.26	0.07	0.14
Delivery Delay CDF (1800 s)	0.15	0.40	0.09	0.21	0.12	0.30	0.07	0.15
Delivery Delay CDF (3000 s)	0.15	0.42	0.09	0.21	0.12	0.31	0.07	0.15
Delivery Delay CDF (4200 s)	0.15	0.43	0.09	0.21	0.12	0.31	0.07	0.15
Delivery Delay CDF (5400 s)	0.15	0.43	0.09	0.21	0.12	0.31	0.07	0.15

In this paper we have presented the results of an analysis of opportunistic routing performance in emergency situations using opportunistic networks. We take into account parameters regarding the characteristics of the emergency scenario (number of people involved, number of victims, etc.) to see how they impact on the performance of routing methods, with regards to suitability for various performance requirements such as delivery rate or lifetime.

From our analysis, we draw two main conclusions. First we find that MaxProp forwarding is the best method in terms of delivery performance in almost all scenarios. Its performance surpasses the other protocols by a more or less wide margin in almost all the simulations, no matter the number of nodes in the emergency or the number of messages generated. Second, we note the low overhead and cost of the TTR forwarding. While the delivery performance results of TTR are far below the performance of MaxProp its energy performance deserves consideration if the characteristics of the emergency scenario requires it. In long emergency situations, or scenarios with a high density of nodes, or a lot of messages, an energy efficient forwarding method is required for not exhausting the node's battery.

Acknowledgments

This research has been partially funded by the Spanish Ministerio de Educación y Ciencia (FPU Grant AP2008-03149) and Ministerio de Ciencia e Innovacĩon (TIN2010-15764 project), by the Catalan DURSI Grant 2009SGR1224 and by EU RECOGNITION project (FP7-ICT 257756).

References

Aschenbruck N, Frank M, Martini P, Tolle J. Human mobility in manet disaster area simulation—a realistic approach. In: Proceedings of the 29th annual IEEE international conference on local computer networks, LCN'04, IEEE Computer Society, Washington, DC, USA. 2004. p. 668–75 http://dx.doi.org/10.1109/LCN.2004.64. URL ⟨http://dx.doi.org/10.1109/LCN.2004.64⟩.

Aschenbruck N, Gerhards-Padilla E, Martini P. Modeling mobility in disaster area scenarios. Performance Evaluation 2009;66(12):773–90, http://dx.doi.org/10.1016/j.peva.2009.07.009 URL ⟨ ⟨http://dx.doi.org/10.1016/j.peva.2009.07.009⟩*http : //doi.acm.org*/10.1145/1644893.1644927⟩.

Balasubramanian N, Balasubramanian A, Venkataramani A. Energy consumption in mobile phones: a measurement study and implications for network applications. In: Proceedings of the ninth ACM SIGCOMM conference on Internet measurement conference, IMC '09. ACM, New York, NY, USA, 2009. p. 280–93 http://dx.doi.org/10.1145/1644893.1644927 URL ⟨http://doi.acm.org/10.1145/1644893.1644927⟩.

Burgess J, Gallagher B, Jensen D, Levine BN. MaxProp: routing for vehicle-based disruption-tolerant networks. In: Proceedings of the IEEE INFOCOM, 2006; URL ⟨http://goo.gl/hZOAw⟩.

Carroll A, Heiser G. An analysis of power consumption in a smartphone. In: Proceedings of the 2010 USENIX conference on USENIX annual technical conference, USENIXATC'10, USENIX Association. Berkeley, CA, USA, 2010. p. 21–21 URL ⟨http://portal.acm.org/citation.cfm?id=1855840.1855861⟩.

Conti M, Kumar M. Opportunities in opportunistic computing. Computer 2010;43:42–50, http://dx.doi.org/10.1109/MC.2010.19.

Daly EM, Haahr M. Social network analysis for routing in disconnected delay-tolerant manets. In: Proceedings of the eighth ACM international symposium on Mobile ad hoc networking and computing, MobiHoc '07. ACM, New York, NY, USA, 2007. p. 32–40 http://dx.doi.org/10.1145/1288107.1288113 URL ⟨http://doi.acm.org/10.1145/1288107.1288113⟩.

Erramilli V, Crovella M, Chaintreau A, Diot C. Delegation forwarding. In: MobiHoc '08: proceedings of the ninth ACM international symposium on mobile ad hoc networking and computing. ACM, New York, NY, USA, 2008. p. 251–60 http://dx.doi.org/10.1145/1374618.1374653.

Farrell S, Cahill V, Geraghty D, Humphreys I, McDonald P. When tcp breaks: delay- and disruption-tolerant networking. IEEE Internet Computing 2006;10(4): 72–8 http://dx.doi.org/10.1109/MIC.2006.91.

〈http://www.geopictures.eu/〉, Geo-pictures; 2010.

Google crisis response. URL 〈http://www.google.com/crisisresponse/〉.

Hikaru I, Kenji M, Yoichiro U, Kazuo I, Noriharu M. Study on the evaluation of applicability of smart phones in a disaster recovery system. In: Proceedings of the IEICE general conference, vol. 2; 2011-02-28. p. S61–S62 URL 〈http://ci.nii.ac.jp/naid/110008577631/en/〉.

Hui P, Crowcroft J, Yoneki E. Bubble rap: social-based forwarding in delay tolerant networks. In: MobiHoc '08: proceedings of the ninth ACM international symposium on Mobile ad hoc networking and computing, ACM, New York, NY, USA, 2008. p. 241–50 http://dx.doi.org/10.1145/1374618.1374652.

Hui P, Crowcroft J, Yoneki E. Bubble rap: social-based forwarding in delay-tolerant networks. IEEE Transactions on Mobile Computing 2011;10(11):1576–89, http://dx.doi.org/10.1109/TMC.2010.246.

Improvisa—infraestructura minimalista para la provisión de servicios en redes ad-hoc (minimalist infrastructure for service provisioning in ad-hoc networks) 〈http://www.gsi.dit.upm.es/improvisa/english.htm〉.

Keränen A, Ott J, Kärkkäinen T. The one simulator for dtn protocol evaluation. In: Proceedings of the second international conference on simulation tools and techniques, Simutools '09, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, 2009. p. 55:1–55:10 http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5674 URL 〈http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5674〉.

Lindgren A, Doria A, Schelén O. Probabilistic routing in intermittently connected networks. In: SAPIR, Lecture Notes in Computer Science, vol. 3126. Springer, 2004. p. 239–54 URL 〈http://www.springerlink.com/content/9xt3904hd05fxmjf〉.

Lorincz K, Malan D, Fulford-Jones T, Nawoj A, Clavel A, Shnayder V, et al. Sensor networks for emergency response: challenges and opportunities. Pervasive Computing, IEEE 2004;3(4):16–23.

Martí R, Robles S, Martín-Campillo A, Cucurull J. Providing early resource allocation during emergencies: the mobile triage tag. Journal of Network and Computer Applications 2009;32(6):1167–82.

Martín-Campillo A, Crowcroft J, Yoneki E, Martí R, Martínez C. Using haggle to create an electronic triage tag. In: The second international workshop on mobile opportunistic networking—ACM/SIGMOBILE MobiOpp 2010, ACM Press; 2010. p. 167–170.

〈http://www.mashproject.com/〉, Mass casualties and health care following the release of toxic chemicals and radioactive material (mash); 2009.

McGrath S, Grigg E, Wendelken S, Blike G, Rosa MD, Fiske A, et al. ARTEMIS: a vision for remote triage and emergency management information integration. Dartmouth University; 2003. p. 9.

Mtibaa A, May M, Diot C, Ammar M. Peoplerank: social opportunistic forwarding. In: INFOCOM, 2010 Proceedings IEEE. 2010. p. 1–5 http://dx.doi.org/10.1109/INFCOM.2010.5462261.

Nordström E, Gunningberg P, Rohner C. A search-based network architecture for mobile devices. Technical report. Uppsala University; 2009.

Pelusi L, Passarella A, Conti M. Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. Communications Magazine, IEEE 2006;44(11):134–41, http://dx.doi.org/10.1109/MCOM.2006.248176.

Reina DG, Toral SL, Barrero F, Bessis N, Asimakopoulou E. Evaluation of ad hoc networks in disaster scenarios. In: Proceedings of the 2011 third international conference on intelligent networking and collaborative systems, INCOS '11. IEEE Computer Society, Washington, DC, USA; 2011. p. 759–64 http://dx.doi.org/10.1109/INCoS.2011.86 URL 〈http://dx.doi.org/10.1109/INCoS.2011.86〉.

Rice A, Hay S. Measuring mobile phone energy consumption for 802.11 wireless networking. Pervasive and Mobile Computing 2010;6(6):593–606, http://dx.doi.org/10.1016/j.pmcj.2010.07.005 special Issue PerCom 2010. URL 〈 〈http://goo.gl/AjQZH〉*http : //issg.cs.duke.edu/epidemic/epidemic.pdf*〉.

Williams D. Tactical medical coordination system (tacmedcs), Naval Health Research Center, San Diego, CA. Technical report. Febraury 2004–June 2007; November 2007.

Wittie MP, Harras KA, Almeroth KC, Belding EM. On the implications of routing metric staleness in delay tolerant networks. Computer and Communications 2009;32:1699–709, http://dx.doi.org/10.1016/j.comcom.2009.02.006.

Ye Q, Cheng L, Chuah MC, Davison BD. Performance comparison of different multicast routing strategies in disruption tolerant networks. Computer Communications 2009;32(16):1731–41, http://dx.doi.org/10.1016/j.comcom.2009.02.007 special issue of computer communications on delay and disruption tolerant networking.