City Mesh – Resilient First Responder Communication

Kamill Panitzek
TU Darmstadt
panitzek@tk.informatik.tu-darmstadt.de

Immanuel Schweizer
TU Darmstadt
schweizer@tk.informatik.tu-darmstadt.de

Dirk Bradler
TU Darmstadt
bradler@tk.informatik.tu-darmstadt.de

Max Mühlhäuser
TU Darmstadt
max@tk.informatik.tu-darmstadt.de

ABSTRACT

Communication between first responders is vital to the success of large scale disaster management. But communication technologies used by first responders today do not scale well due to heterogeneity, point-to-point connections, and centralized communication structures.

As the popularity of devices equipped with Wi-Fi grows, the number of access points (APs) in city centers increases as well. This communication infrastructure exists and should be used in city wide disasters as it is readily available in areas with high population density. In this paper, we investigate Wi-Fi access points in 5 major cities deployed in stores, bars, and restaurants. We want to answer the question if these APs can be used as a mesh networking backbone in disaster response. The main contributions of this paper are (i) the surveyed and analyzed public Wi-Fi layout of five major cities and (ii) the connectivity analysis of the city wide network topology.

Keywords

Wireless ad hoc networks, mesh networks, resilience, city area.

INTRODUCTION

Efficient communication is fundamental for disaster relief. But the communication technology in use today does not scale well with the increasingly global scale of disasters. This is due to a number of reasons: (i) as the scope of any disaster increases more first response organizations are involved which leads to a heterogeneity in devices and technology, (ii) from a technology perspective the connections today are mostly point-to-point without any way to relay or redirect data if the direct path is blocked, and (iii) new communication infrastructure cannot be added ad-hoc as parts of the infrastructure become blocked or destroyed.

A prominent example where communication technology did not scale are the 9/11 attacks. One of the major findings of reports after the disaster (Titan Corporation and United States, 2003) indicated a strong need for reliable first response communication. They state that “In the first few hours, foot messengers at times proved to be the most reliable means of communicating”. If this is a problem for the developed world, it is an even more severe problem for disaster in developing countries, e.g. the earthquake in Haiti.

We have analyzed different use cases a first response infrastructure must be able to handle (Bradler, Kangasharju and Mühlhäuser, 2008). The most important lesson learned is the need for a distributed communication infrastructure. This exposes no single point of failure leading to higher resilience. We have proposed a distributed crisis response communication system that tackles the relevant challenges and provides a reliable communication system for disaster management (Bradler, Schiller, Aitenbichler and Liebau, 2009). Our approach operates on small mobile handheld devices carried by first responders. These devices form an ad-hoc network. The network is supported by more powerful supernodes, e.g. stationary access points (APs) or

Reviewing Statement: This full paper has been fully double-blind peer reviewed for clarity, relevance, significance, validity and originality.

communication vans.

Today more and more mobile devices capable of Wi-Fi communication, e.g. smartphones, tablets, emerge. To accommodate customers in stores, bars, or restaurants, an increasing number of publicly available wireless APs is deployed. All APs could form a communication graph since they use the same basic protocols and technologies. Yet this communication power remains unusable in the case of a disaster. We investigate the basic properties of the communication graph. This answers the questions if these APs can be used as the backbone of a city-wide ad-hoc network in the case of a major disaster. We collected the Wi-Fi APs for 5 major cities (Chicago, Melbourne, Mountain View, New York, and San Francisco), investigated the density of APs, and simulated the derived city-wide ad-hoc network.

The main contributions of this paper are (i) the surveyed and analyzed public Wi-Fi layout of five major cities and (ii) the connectivity analysis of the city wide network topology.

The reminder of this paper is organized as follows. Section 2 describes wireless mesh networks. In Section 3 we present our methodology and evaluate our approach in Section 4. Section 5 concludes the paper and presents future work.

WIRELESS AD-HOC MESH NETWORK

Wireless ad-hoc mesh networks (WMNs) are distributed communication structures that configure and organize themselves. Communication nodes in WMNs form ad-hoc connections between them. In WMNs there are typically two types of nodes: the mesh router and the mesh client. Mesh routers provide the basic infrastructure for the mesh networks. They might be connected to gateways to provide internet connectivity for the mesh network. Mesh clients on the other hand connect to mesh routers and use the created mesh infrastructure to send and receive messages. Usually they are less powerful devices like laptops or smartphones. Mesh clients may also participate in the routing of the network (Akyildiz and Wang, 2005).

Wireless Mesh networking today is already part of many Linux distributions as the 802.11s amendment to wireless networking is currently available as draft (Hiertz, Max, Zhao, Denteneer, and Berlemann, 2007). The goal here is to standardize a mesh networking protocol on top of the wireless 802.11 standard used for example in home routers or access points today. This would lead to ubiquitous mesh networking capabilities. But even today there are several other solutions available already. The most common is XMesh (Teo, Singh, and McEachen, 2006) originally developed by Crossbow Technologies and now available for the TinyOS sensor platform.

Additionally there are many different routing protocols for mesh networking. The most common routing protocols are Optimized Link State Routing (OLSR) (Clausen, Jacquet, Adjih, Laouiti, Minet, Muhlethaler, Qayyum and Viennot, 2003) and Ad hoc On-Demand Distance Vector Routing (AODV) (Perkins, Belding-Royer and Das, 2003). New approaches are the “Better approach to mobile ad-hoc networking” (B.A.T.M.A.N.) (Neumann, Aichele, Lindner and Wunderlich, 2008) and Babel (Chrobozek, 2008). While B.A.T.M.A.N. is intended to replace OLSR, which it outperforms, Babel is based on destination-sequenced distance-vector routing (DSDV) and AODV. Both are state of the art routing protocols for WMNs (Abolhasan, Hagelstein and Wang, 2009). So it is indeed possible to use a given set of APs as a WMN for disaster response. But we have to gain deeper understanding of the properties of the already given AP infrastructure to really take advantage.

We need a more thorough analysis of current WMN properties. WMNs and their algorithms are usually analyzed by conducting simulations. This allows investigating the weakness of a certain WMN topology or studying the behavior of the network under certain conditions. Usually the simulation starts by placing the nodes at random positions on a rectangular plane where they form a unit disc graph. In a unit disc graph two nodes are connected iff they are no further apart than one distance unit (Clark, Colbourn and Johnson, 1990). A main shortcoming of this simulative approach is that wireless access points in reality are not randomly distributed. So the properties we are deriving might be true on random networks but not with any practical deployment. The density of wireless APs might change with population density, city architecture, or shopping behavior. None of these are reflected in current simulation models.

We have conducted a preliminary analysis of the current AP topology in 5 different city areas. This will enable a better understanding whether this infrastructure can be used as mesh backbone in disaster response and how to deploy given technology on top of non-random graphs. We will emphasize on the resilience of a given architecture as APs might be destroyed during a disaster.

Before we will introduce our first results we will briefly describe the Roofnet project from MIT (Chambers, 2002) and the Mobile ACcess project in Aachen[1] which are practical examples of WMNs and more sophisticated uses of APs.

MIT Roofnet project

The MIT Roofnet team deployed a wireless mesh network on the campus of the Massachusetts Institute of Technology in Cambridge (comp. Figure 1). This network provides broadband internet access to users in Cambridge. The protocol used to determine the routes between routers is called SrcR. Two broadcasts are used with this protocol. The first one measures the probability that a packet receives its' destination when transmitted between two nodes in radio contact. The second broadcast is used to build the routing tables. To find a route from node *s* to node *d*, node *s* broadcasts that it wants to find a route to node *d*. Every node receiving the broadcast from node *s* will add its ID to the route and forward the packet to the next node. Finally node *d* receives that packet and it will reply back along the route that was found for that particular packet. When node *s* receives the reply it can use this information to determine the best route to node *d*. To do so the Expected Transmission Count (ETX) metric is used on the route information returned from the query. Access and transport of media is handled by the Extremely Opportunistic Routing (ExOR) algorithm (Biswas and Morris, 2005).

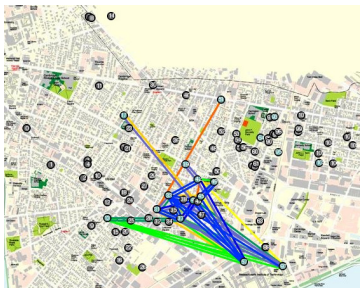

Figure 1. Roofnet MIT[2]

Mobile ACcess

Mobile ACcess in Aachen is not a WMN. It is a project of the city of Aachen and the university RWTH Aachen as well as some industrial partners to provide free mobile internet connection to participants of the project using Wi-Fi APs. Every citizen may participate to the project by sharing an AP to increase the network coverage in the city. The network also provides services for city visitors like 3D city sightseeing flight or localization. To protect the providers of such free APs from illegal usage of mobile users the data traffic of mobile users is tunneled to their own homes. This ensures that illegal internet usage is bound to the right users and their homes and internet connections. To protect the privacy of the mobile users as well the communication to the internet is encrypted. There exists a similar project by the Google Inc. in the city of Mountain View, California where the Google Company also provides free internet access by covering the city with APs.

METHODOLOGY

The number of publicly available wireless APs is increasing. This is mainly due to the fact that more mobile devices are capable of Wi-Fi connection. Smartphones, tablets, and notebooks still gain popularity forcing owners of stores, restaurants, and bars to enable wireless internet. Especially in city centers these locations occur in high density. Using the ideas of a wireless mesh network, these APs can be connected to an ad-hoc backbone infrastructure. This is especially true given the fact that 802.11s may enable mesh functionality on all routers. The communication infrastructure might then be used for first response communication. Since the AP density increases roughly with population density this technology is most useful where disaster affect a lot of people.

---

[1] Website of Mobile ACcess project in Aachen: http://www.mobile-access.org

[2] Picture taken from MIT Roofnet project website: http://pdos.csail.mit.edu/roofnet/doku.php?id=map

The projects of MIT and Aachen have shown that there exist possibilities and techniques to achieve this goal. We therefore concentrate on the given wireless APs and if they can be connected. We provide a preliminary analysis of the given infrastructure and investigate the suitability for disaster response.

We gathered location data of publicly available APs provided by the NodeDB[3] project. NodeDB is a freely accessible project where people can add and retrieve information about wireless APs into and from a global database. The information stored in this database includes location, SSID, description, status, internet connectivity, and whether the AP is for commercial use or not. The APs are visualized on a map.

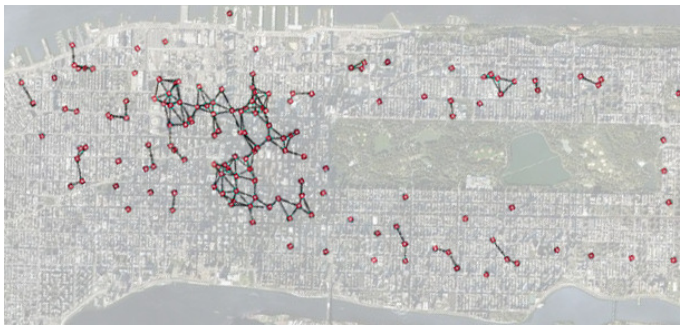

Figure 2. Derived graph of wireless APs in Manhattan, New York

Since NodeDB is an open database the completeness cannot be guaranteed. In fact we checked for Darmstadt where no publicly available AP is provided by the database. Also the Mobile ACcess project in Aachen is not covered by NodeDB. We therefore selected cities that are covered by NodeDB and have an AP density high enough to deliver meaningful results. We selected the cities of Chicago, Melbourne, Mountain View, New York, and San Francisco to analyze the AP graph. Mountain View is especially interesting as Google Inc. deployed APs in the whole city to provide internet access.

First, we extracted information about the APs in the city centers from the NodeDB project and placed them into a graph using their longitude and latitude coordinates. Connections between routers were formed using the unit disk graph as described in the introduction. Two APs are connected iff they are within a range of 300 meters[4]. Due to the high density of bars, stores, restaurants, etc. in city centers we assume important graph metrics to be different from randomly generated unit disk graphs. The city center contains more nodes and also more links between the nodes than outside regions. By looking at Manhattan we can see that places like parks (Central Park) do not have APs at all whereas the city center is strongly connected (comp. Figure 2).

Private access points

Not only stores, bars or restaurants provide wireless APs but also private households have routers providing Wi-Fi connectivity and broadband internet connection. Most of these APs are not stored in the NodeDB database and might be in much higher number than publicly available APs. If it would be possible to also have private APs participating in a city wide crisis mesh network, the network would gain in stability. Network coverage would also gratefully benefit from private APs. Projects like Aachen's Mobile ACcess have shown that citizens are interested in participating in city wide Wi-Fi networks by sharing their APs to the community. The remaining question is now how many of these private access points are there in city centers and how many people would participate to such a project. Having this information we could analyze the city mesh networks again with higher node count resulting in better network coverage.

Furthermore, there exist also computational resources resided in most private households. As first responders might not be able to carry heavy or big equipment their devices might not have high computational power. Outsourcing heavy computational tasks to standalone computers could help first responders achieving their mission. These standalone computers can be servers or computers in the crisis management headquarters or in the war room but also the computers of private households. Together with the QuaP2P[5] research group we work

[3] Website of NodeDB project: http://www.nodedb.com

[4] Belkin router details: http://www.belkin.com/IWCatProductPage.process?Product_Id=481082

[5] Website of QuaP2P Research Group: http://www.quap2p.de

on a peer-to-peer (P2P) based service platform to provide services and computational resources to a participating P2P community. For crisis management this can provide distributed applications reaching from simple maintenance of a list of missing civilians to a dynamic map of the disaster environment where first responders can add sensor information to a map about their current position and also retrieve information about regions which have not yet been searched for civilians. Private computers can help in such situations by not only providing computational resources but also storage capacity for backups or other important data.

EVALUATION

WMNs are usually created by randomly placing communication nodes in a square or rectangular field. Nodes that are inside a certain radius of another node are connected with each other. Looking at most cities we believe a random placement of nodes does not reflect the reality well enough. This is especially due to the fact that most cities have city centers or mall areas where most of the city's shops, bars, and restaurants are resided. This leads to a much higher density of publicly available AP. Examining graph theoretical properties of both, the randomly generated mesh networks and mesh networks derived from APs in major cities we show a city mesh network to differ significantly in major graph theoretical properties.

Table 1 shows information about the 5 evaluated cities. The number of APs is provided as well as the area the APs are distributed in. All cities exhibit different properties. We therefore compared the AP graphs against randomly created unit disc graphs with the same basic properties as given by the table. This helps us finding a baseline for each city and still be able to compare the cities with each other. For statistical significance, we therefore analyzed 20 randomly generated unit disk graphs, generated average values for every metric and compared the results against the according city.

	Height (m)	Width (m)	Area (km²)	#APs	#APs / km²
Chicago	2577	1998	5.15	49	9.51
Melbourne	5105	3126	15.96	115	7.20
Mountain View	5572	6613	36.85	488	13.24
New York	2964	10898	32.30	162	5.02
San Francisco	5047	5246	26.48	136	5.14

Table 1. Analyzed cities

To show the differences between the examined cities compare Figure 3 which provides a connected map of the mesh networks formed in Chicago, Mountain View and San Francisco. The derived mesh network for New York City is shown in Figure 2 above. It is important to note that in Mountain View Google tries to optimize the coverage of their network while in other cities all APs are independent of each other. We will see how this influences different metrics later.

Figure 4 demonstrates the difference between the AP graph and a randomly generated network exhibiting the same basic properties. Here the city of Melbourne is shown together with a randomly generated network. The city center contains most of the APs and the nodes are therefore strongly connected and the link count is much higher than anywhere in the random network. Also there are huge spaces in the city network without APs. Both facts are due to the geographical conditions of the city. In the random network the nodes are distributed equally over the entire area.

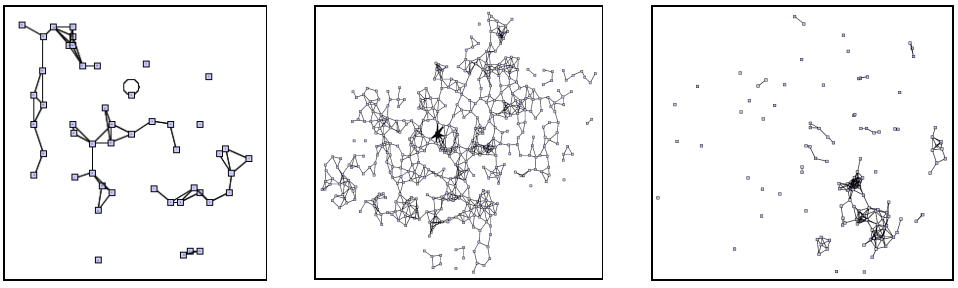

Figure 3. Wireless APs in (a) Chicago, (b) Mountain View, and (c) San Francisco

All nodes are either isolated or they are part of small to medium sized components. The random network does not contain an identifiable biggest component.

To analyze the different graph theoretical properties of the mesh networks we used the Graph-Theoretic Network Analyzer (GTNA) (Schiller, Bradler, Schweizer, Mühlhäuser and Strufe 2010). It is a Java-based framework that allows for the graph-theoretic analysis of arbitrary network topologies. It is possible to either import snapshots from network simulators or generate popular network topologies. A large set of commonly used graph metrics and network topology generators are already provided by GTNA but the framework is also easily extendible through a well-defined plug-in interface. The tool also has a plotting module which allows for a graphical visualization of the analyzed graph metrics. In our subsequent evaluation all city networks are represented by the green plots and the random networks by the red plot.

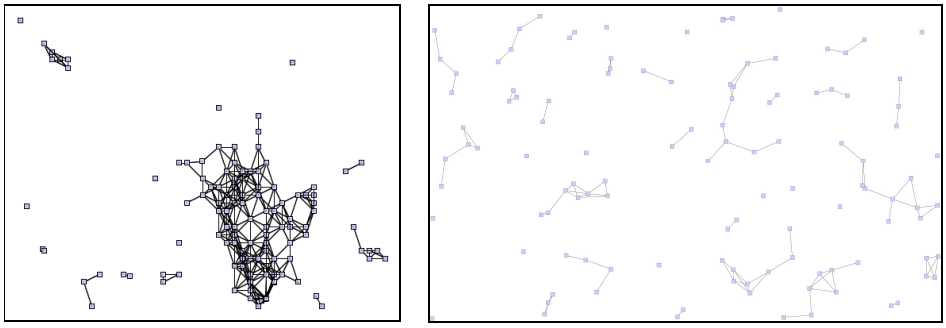

Figure 4. Mesh network of (a) Melbourne and (b) a random network

Metrics

We used different metrics to analyze and compare the cities with each other. First, we analyzed the average node degree and the degree distribution for all networks. The node degree is defined as the amount of links that are connected with one node. The average degree is then calculated as the average over all node degrees in one network. Second, we analyzed the size of the biggest component and how it behaves when removing critical nodes. The biggest component of a network is the sub-network that contains the most nodes which are all connected to that sub-network. In the biggest component there are no isolated nodes. Most critical nodes are defined as nodes with the highest node degree, also called hubs. By removing such nodes many links of the network are lost. Third, we analyzed the characteristic path length and the diameter of the network. The characteristic path length is defined as the average shortest path between all node pairs in the network. The diameter on the other hand is defined as the longest path over all shortest paths between all node pairs in the network.

Node degree

Looking at the average node degree provided in Table 2 we see that Melbourne has the highest average node degree. San Francisco and New York are very similar in their random graph due to the similar #AP / km² value from Table 1. But their actual degree values differ since the cities have different shapes (comp. Figure 3). In fact we can see that cities have unique average node degrees for that matter. The degree values of the randomly generated graphs are proportional to the #AP / km² values from Table 1. The reason for this is the fact that nodes are equally distributed when randomly generating the mesh network. The average node degree of cities on the other hand is not bound to the #AP / km² value. By looking at the networks of Melbourne and Mountain View we see that in Melbourne there are many nodes connected with each other in the city center whereas in Mountain View Google Inc. distributes the APs with the goal of reaching good network coverage in the city.

D_{avg}	Chicago	Melbourne	Mountain View	New York	San Francisco
City	5.06	13.32	9.53	5.13	7.67
Random	4.38	3.78	7.16	2.67	2.65

Table 2. Average node degree

We take a deeper look at the degree distribution of Melbourne and Mountain View (comp. Figure 4). Since the degree distribution of Melbourne is similar to the distribution of the other cities, Melbourne can represent them in this analysis. As we compare the random network against the city mesh we observe that the distribution hits a

peak value for random networks. This peak is rather low and around 1 for Melbourne and 3 for Mountain View respectively. Afterwards the probability of nodes with higher node degree decreases.

In the mesh network of Melbourne we cannot identify a real peak value and the probability of different node degrees seems to be distributed arbitrarily over all node degrees. Only the possibilities of nodes with node degree of more than 10 decrease again. This is the reason for the high average node degree in Melbourne and the discrepancy to the random network. In other cities the distribution is similar but shifted towards lower values.

In Mountain View the node degree distribution does not differ that much from the random network. Also the average values are closer to each other than in Melbourne. We believe this to be due to the high density of APs in Mountain View. There are nearly twice as much APs per km² in Mountain View than in Melbourne. Also, since Google Inc. tries to reach the best network coverage for the entire city, the APs need to be distributed equally over the whole city. This also holds true for the random network. So while in Melbourne the layout is given by the density of stores in Mountain View one company is responsible. And their target of maximal network coverage can only be reached if the AP density is equal over the whole city area. We will see later that the nodes are not randomly deployed.

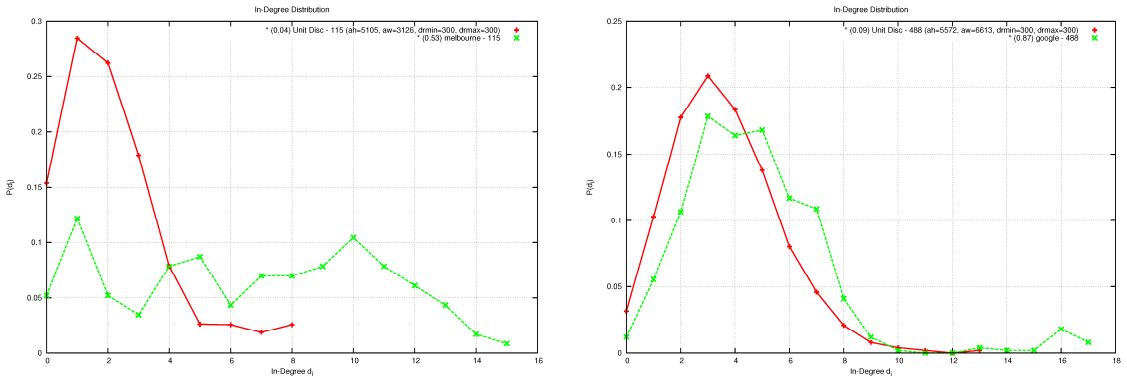

Figure 5. Degree distribution of (a) Melbourne and (b) Mountain View

Biggest component size

The size of the biggest component is of great interest concerning the connectivity and the robustness of the network. In this section we will concentrate on Melbourne and Mountain View since they exhibit the most interesting characteristics. While the network in Mountain View is planned by Google, the networks in Melbourne and the other cities emerged more occasionally. San Francisco is very similar to New York and does not present new information and Chicago is very similar to a generated random network as we will see later on. The network in Melbourne on the other hand has the highest average node degree. This is why we chose Melbourne for this analysis.

The graphs in Figure 6 show the behavior of the biggest component of a network when removing critical nodes (nodes with highest node degree). In both networks removing critical nodes decreases the size of the biggest component since most of these nodes are part of that biggest component. The most interesting fact is that the biggest component of the Mountain View network consists of nearly 460 nodes (the overall network consists of 488 nodes). That translates to almost 95% of the nodes, so there are just very few nodes isolated. This again is due to the fact that Google Inc. tries to provide high network coverage in the city and the distances between APs still allow for radio connectivity. In Melbourne on the other hand only 83 out of 115 nodes or ~72% belong to the biggest component. But this is without any central organization or control facility.

To analyze the robustness of the biggest component the nodes are sorted by their node degree in decreasing order. Then the node with highest node degree is removed from the network. It is obvious that the nodes with highest node degree are the most important nodes when it comes to network connectivity. As mentioned above such nodes are also called hubs. A random event like a disaster would probably not start with the most connected nodes while an adversary would use that tactic. So this evaluation comes as a worst case analysis of what happens if the most important nodes are destroyed.

By removing the top 20% of these nodes the network of Mountain View is still connected. That is a very high value and translates to 72 nodes that need to be destroyed. Nonetheless when we remove more nodes we can observe a drop in the size of the biggest component of the Mountain View network. This means that at this point

the biggest component is partitioned and another component smaller in size is created. On comparison the network in Melbourne is still connected with over 30% of the critical nodes removed. After that we can also observe the partitioning of the biggest component as in the network of Mountain View. If we compare both to their random baseline we can see that the biggest component is much smaller and that the drop for Melbourne is earlier at around 10% of the critical nodes.

A disaster is a dynamic scenario where the environment changes constantly and infrastructure is destroyed or blocked. Thus any communication infrastructure must be robust to node failures. Our analysis here shows that even though we remove 20% or 30% of the most important nodes the communication graph stays connected in Mountain View and Melbourne respectively. As already mentioned we focused on the most critical nodes of the network and still observed a good performance. A disaster might destroy nodes in the infrastructure more arbitrarily leading to an even better performance of the network.

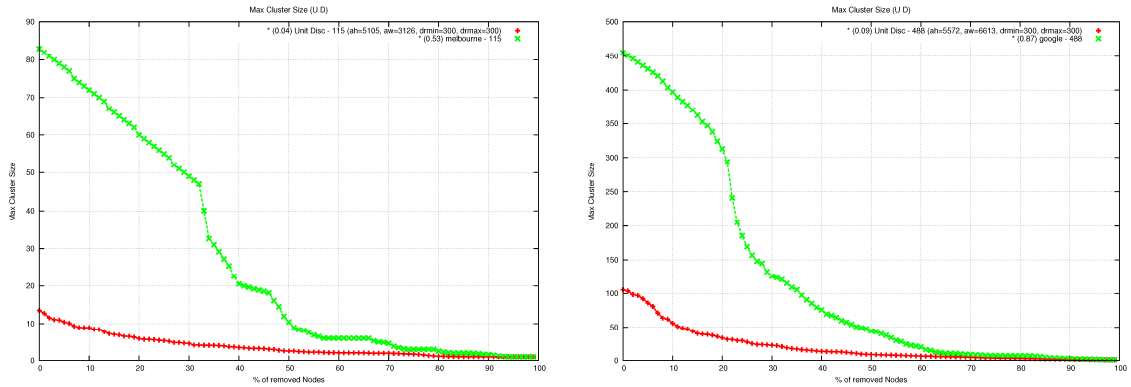

Figure 6. Size of biggest component in (a) Melbourne and (b) Mountain View

Characteristic shortest path length

The characteristic shortest path length gives a good metric about the average hop count for a message to route through the network. A network with high characteristic path length might therefore have a bad routing performance. But looking at the values presented in Table 3 it is important to keep in mind that these values also depend on the number of nodes in the network and how good they are connected. Random networks exhibit a very small characteristic shortest path length so they provide a good baseline. We therefore also calculated the ratio of the characteristic path length observed in the city to its random counterpart. A value close to one would indicate an almost perfect routing graph.

Mountain View exhibits the longest characteristic path length. While this might lead to higher message delay we have to consider that the biggest component covers almost the complete area. It is possible to communicate over much larger distances. And if we look at the ratio compared to the random counterpart it is on par with the performance of Melbourne.

If we take the ratio into account New York actually exhibits the longest average paths. This might be due to the highest skew in distribution, with a high concentration around the city center and large blank spots like the Central Park. It is also interesting to see Chicago being the leader in this evaluation. We have already mentioned Chicago to have the most random distribution. But this again confirms our early observation. The ratio is very close to 1 making it easy to route in the Chicago network.

CPL	Chicago	Melbourne	Mountain View	New York	San Francisco
City	3.14	3.71	14.29	5.84	3.74
Random	2.62	2.26	8.43	1.97	1.73
City/ Random	1.20	1.64	1.70	2.96	2.16

Table 3. Characteristic shortest path length

Table 4 shows the worst case performance for path length (the diameter) and the same trend is visible. Chicago, Melbourne and Mountain View are very close with good performance values while New York and San Francisco are worse but still good.

Diam	Chicago	Melbourne	Mountain View	New York	San Francisco
City	9.0	9.0	39.0	17.0	10.0
Random	6.7	6.9	27.85	6.3	5.15
City/ Random	1.34	1.30	1.40	2.70	1.94

Table 4. Diameter

Overall this shows that the AP networks cannot be described using random networks. However, the performance and robustness we have seen here makes them a viable choice for an ad-hoc communication backbone in disaster situations.

CONCLUSIONS AND FUTURE WORK

In this paper we explored the question if it is possible to create an ad-hoc communication backbone on top of publicly available Wi-Fi access points. We discussed that communication is important for disaster response and today's technology does not scale well with global disaster. Wi-Fi access points are already available in developed cities with high population density and might be used as a mesh network to support first response communication.

We gathered data for wireless APs, mainly in stores, bars and restaurants, in 5 major cities using the NodeDB database. We then simulated and analyzed the resulting mesh networks using the GTNA tool and compared the city mesh to randomly generated networks. We presented projects like Mobile ACcess in Aachen or the Google Wi-Fi project in Mountain View which already try to cover cities with free internet connection. These projects provide good infrastructure due to well distributed APs in the whole city resulting in nearly perfect network coverage and a well-connected and robust mesh network.

Our evaluation implies that city mesh networks cannot be modeled using networks with a random node deployment. The characteristics of a city, e.g. population density, position of shops, bars, restaurants, etc. play an important role in AP distribution. The main finding is that the mesh topology is indeed more robust than a random deployment and robust enough to cope with the removal of 20% of the most critical nodes. A network partition is therefore highly unlikely even in the event of a disaster. We have also investigated the probable routing performance by comparing the characteristic path length of the city networks to their random counterpart. We have seen that even for highly skewed networks like New York the paths are only up to three times longer. Furthermore, our observations of New York also indicates that geographic properties of cities, especially blank spots like the Central Park, are completely free of wireless APs. In the event of a disaster, communication vans or mobile antennas would have to be positioned in such spots to keep up network coverage and communication services.

In the future we want to investigate even more cities. Also it is well known that besides publicly available APs citizens usually have own routers with Wi-Fi capabilities which can also be used to assist the mesh network in crisis management. Modifications as presented in Aachen would be needed for the private routers to also participate in such crisis mesh networks. A standardized way to plug these communication nodes into the first response infrastructure needs to be proposed and evaluated in the future. As we developed a sandbox for first response communication in the past (Bradler, Schweizer, Panitzek and Mühlhäuser, 2008), we actually integrate the proposed mesh network infrastructures into our sandbox. This will let us simulate and evaluate the capabilities of these infrastructures in disaster scenarios.

REFERENCES

1. Abolhasan, M., Hagelstein, B. and Wang, J.C.P. (2009) Real-world performance of current proactive multi-hop mesh protocols, *15th Asia-Pacific Conference on Communications*.
2. Akyildiz, I. F. and Wang, X. (2005) A Survey on Wireless Mesh Networks, IEEE *Communications magazine*.
3. Biswas, S. and Morris, R. (2005) ExOR: opportunistic multi-hop routing for wireless networks, *Computer Communication Review*.
4. Bradler, D., Kangasharju, J. and Mühlhäuser, M. (2008) Systematic First Response Use Case Evaluation, *Workshop on Mobile and Distributed Approaches in Emergency Scenarios*.
5. Bradler, D., Schweizer, I., Panitzek, K. and Mühlhäuser, M. (2008) First response communication sandbox, *Proceedings of the 11th communications and networking simulation symposium.*

6. Bradler, D., Schiller, B., Aitenbichler, E. and Liebau N. (2009) Towards a Distributed Crisis Response Communication System, *In Proceedings of the 6th International ISCRAM Conference*.
7. Chambers, B.A. (2002) The grid roofnet: a rooftop ad hoc wireless network.
8. Chrobozek, J. (2008) Babel – A loop-free distance-vector routing protocol.
9. Clark, B. N., Colbourn, C. J. and Johnson, D. S. (1990) Unit Disk Graphs, *Discrete Mathematics*.
10. Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A. and Viennot, L. (2003) Optimized Link State Routing Protocol (OLSR).
11. Hiertz, G.R., Max, S., Zhao, R., Denteneer, D. and Berlemann, L. (2007) Principles of IEEE 802.11 s, *In Proceedings of the 16th International Conference on Computer Communications and Networks.*
12. Neumann, A., Aichele, C., Lindner, M. and Wunderlich, S. (2008) Better approach to mobile ad-hoc networking.
13. Perkins, C.E. and Belding-Royer, E. and Das, S. (2003) *Ad* hoc On-demand distance Vector (AODV).
14. Schiller, B., Bradler, D., Schweizer, I., Mühlhäuser, M. and Strufe, T. (2010) GTNA-A Framework for the Graph-Theoretic Network Analysis.
15. Teo, A. and Singh, G. and McEachen, JC, Evaluation of the XMesh routing protocol in wireless sensor networks, *49th IEEE International Midwest Symposium on Circuits and Systems*, 2006
16. Titan Corporation and United States (2003) Arlington County After-Action Report on the Response to the September 11 Terrorist Attack on the Pentagon.