Enhancing Robustness of First Responder Communication in Urban Environments

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

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

Tobias Bönning
TU Darmstadt
boenning@rbg.informatik.tu-darmstadt.de

Gero Seipel
TU Darmstadt
seipel_g@rbg.informatik.tu-darmstadt.de

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

ABSTRACT

Communication is crucial for first responders. Crisis management is nearly impossible without good means of communication. Unfortunately the communication technology used by first responders today does not scale well. Also most of the given infrastructure, such as cell towers, might be destroyed.

In recent research ad-hoc and peer-to-peer based communication has been proposed to solve the problem of resilient communication. Most mobile devices are equipped with wireless transceivers that make them suitable to participate in ad-hoc networks. But node density might be too small for a connected topology.

In this paper we, therefore, discuss the implications of an emergency switch for private wireless routers allowing them to transition to an emergency mode to create a supportive wireless mesh network. To analyze if such a network would result in a resilient topology real data from wireless routers in a city is gathered. We calculate the locations of private and public routers from GPS traces and compare the resulting networks with each other.

Keywords

Wireless Mesh Network, Urban Area, Private Wireless Routers, First Response, Resiliency, Analysis

INTRODUCTION

In 2011 we have been reporting on the idea of using publicly available wireless routers to supplement the communication infrastructure during first response missions in urban areas (Panitzek, Bradler, Schweizer and Mühlhäuser, 2011). This would only work in city centers as most routers are privately owned in other areas. Therefore, we now shed light on the possibility of using privately owned routers as communication backbone. We compare the resulting network topologies to networks with public routers in the same urban area.

Communication between first responders, citizens and command and control personnel is viable to the success of any first response mission. In recent research ad-hoc and peer-to-peer communication has been proposed to improve communication (Bradler, Kangasharju and Mühlhäuser, 2008; Bradler, Aitenbichler, Schiller and Liebau, 2009). Using decentralized communication architectures will improve resilience as link and node failures can be mitigated by the network. This is true only if enough nodes are available as a fallback requiring minimum node density. In disaster response this is given close to the incident, the so called incident site and treatment area (Aschenbruck, Gerhards-Padilla and Martini, 2009), as most first responders will be located at these sites. It is also given close to stationary facilities like the command and control center or hospitals (hospital zone). But anywhere else in between (transport zone) the node density might be too low leaving the whole network vulnerable. A support infrastructure is needed delivering a high node density throughout the entire disaster area. It should also be readily available and working with available wireless standards.

We have made the point in 2011 that wireless routers fulfill those requirements, but routers with free access are scarce. Even though the resulting topologies build with just public routers might be suitable in city centers a

higher density is needed elsewhere. Now, we build upon that analysis by investigating privately owned routers. We assume that at some point in the future an emergency switch was to be implemented that would make all available communication resources available to first responders (Section II). This leads us to investigate the density of all routers in city areas and how they would be suitable to build a communication topology.

We extended a given Android wardriving app to gather our own dataset of all available routers in our hometown Darmstadt, Germany (Section III). A lateration method is used to estimate the positions of the wireless routers from given fingerprints. Using the unit disc graph model (Clark, Colbourn and Johnson, 1990) for wireless topologies we generate different ad-hoc mesh networks. We compare private to public networks in Section IV.

EMERGENCY MODE FOR WIRELESS ROUTERS

The amount of households equipped with internet connection reaches almost 100% in developed countries. Many of those households use wireless routers to connect multiple devices to the Internet. In apartment buildings this leads to a multitude of available wireless routers and a very high density especially in urban areas. Users can recognize this density if they search for available wireless devices at home. The routers found during the scanning process belong to neighbors in the same building or in houses on the opposite side of the road.

This infrastructure is very dense and should be available to first responders during missions in urban environments. This is why we propose an emergency switch for wireless routers. The idea is to create a wireless mesh network (Raniwala and Chiueh, 2005) on top of the given privately owned wireless routers. This infrastructure then acts as a backbone in case of a disaster. It can fill the communication gap between the incident site and the command center.

The emergency switch is meant to disable the security protocols and allow public access to the wireless router. It can only be part of the network if it is open to all users and offers its resources. Abuse of such a network must be avoided at all cost. Therefore this network should be isolated from the citizen's home network to protect people's privacy. This goal could be easily accomplished as it is already today possible to install a home network and a guest network in parallel to grant Internet access to visitors. Such functionality is included in the AVM Fritz!Box 7390[1], for instance.

A similar guest concept is used in the project Mobile ACcess of the city of Aachen, the university RWTH Aachen, and industrial partners. This project provides free mobile internet connectivity to participants of the project. Every citizen may participate to the project by sharing his or her wireless router to increase the network coverage in the city. The project also provides services for city visitors, like 3D city sightseeing flight or localization. Also, in this project the data traffic of mobile users is tunneled to their own homes to protect owners of the routers from illegal usage and law infringements. This ensures that all Internet usage is bound to the right users' identities. In addition mobile users are protected by encrypting the wireless communication.

To realize the proposed emergency switch, similar measures must be taken to protect both the citizens and the first responders during their mission. The emergency switch would enable an open guest mode that on the one hand protects people's privacy and on the other hand makes the existing communication resources available to first responders. Legal aspects must be considered and could be solved by identifying individual users of the emergency network similar to the Mobile ACcess project.

METHODOLOGY

Our goal is to analyze the wireless infrastructure in the city center of our hometown Darmstadt, Germany. But first we need to determine the locations of wireless routers in our hometown. Since the exact locations are not stored in any database, we tried to determine the locations of all routers ourselves. For this purpose we first measured signal strengths of wireless networks in a specified area of our hometown and then calculated the positions of the routers using a lateration method.

There exist several ways to learn about existing wireless routers in cities. Projects like WiGLE[2] store data about wireless networks by users driving with their cars or walking through the city while scanning for wireless networks. This procedure is referred to as wardriving and several applications exist for different kinds of hardware and operating systems. But the main problem with such data collections is that most of these data

[1] http://www.avm.de/en/Produkte/FRITZBox/FRITZ_Box_Fon_WLAN_7390/index.php

[2] http://www.wigle.net

points are located on main roads or even highways. On the other hand, in such projects routers are placed on the street instead of their real locations, because no calculations are done while wardriving. Our idea was to improve the data quality by estimating the real locations of wireless routers using lateration methods on gathered data.

To find out where wireless routers are resided throughout the city, we first have to scan for wireless networks at multiple locations in the city. For this purpose we use Android devices, since they have wireless network adapters and GPS sensors integrated. Since additional modifications to such an app must be made, we chose to use the open source app *wardrive*. We changed the application code to continuously scan for wireless routers in the vicinity and log all the information into the local database, also creating multiple entries about individual networks. Using this data we estimate the actual router location using lateration methods.

Our modified version of the *wardrive* app was installed on a Motorola Xoom Tablet. With this device we walked in slow walking speed through the predefined area of our hometown as depicted in Figure 2.a). This area includes the city center and is of roughly 0.47 km² in size. It is determined by the streets Hügelstraße, Kirchstraße, Holzstraße, Zeughausstraße, Bleichstraße, Kasinostraße, and Neckarstraße.

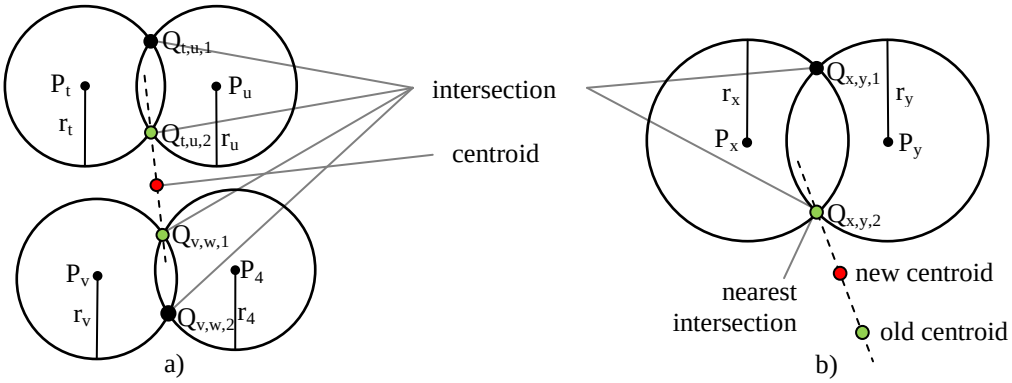

Figure 1: Multilateration

Once all data from our measurements in the city area was collected, we used lateration to estimate locations of the wireless routers. For trilateration (Savvides, Han and Strivastava, 2001) exactly three data points are needed for the calculation. But since we collected a huge amount of data points we use the multilateration approach where all measured points to one wireless router are used for the calculation, thus improving the estimation. The method is depicted in Figure 1 and starts by choosing two arbitrary points P_t and P_u with intersecting circles of the radii r_t and r_u calculated from the measured signal strength. A signal strength s is converted into a distance r by using a formula extracted from the findings of Faria (Faria, 2005) and Rappaport (Rappaport, 1996):

$$r=1/3(10^{(-s-10)/35}-1)$$

We also calculate the points in which the circles intersect and denote them $Q_{t,u,1}$ and $Q_{t,u,2}$. Then a second pair of arbitrary points P_v and P_w are picked with intersecting circles of radii r_v and r_w, respectively. For these two points we also calculate the points in which the circles intersect and denote them $Q_{v,w,1}$ and $Q_{v,w,2}$. Now we pick those two intersection points that are closest to each other and calculate the point in between, being the centroid (cf. Figure 1.a). To incorporate all other points of the measurements we pick the next two arbitrary points P_x and P_y with intersecting circles and calculate the intersection points $Q_{x,y,1}$ and $Q_{x,y,2}$ as well. Using the point closer to the old centroid we calculate the new centroid being in the middle between both points (cf. Figure 1.b). We iteratively proceed with all pairs of points with intersecting circles, thus further correcting the estimation.

PRELIMINARY EVALUATION

After applying the multilateration approach to our measurements we receive an estimated map of all wireless routers in the city center of our hometown Darmstadt. This map is depicted in Figure 2.b). In our measurements we collected 32983 points covering an area of about 467500 m² in size. We identified 1971 unique BSSIDs (unique wireless routers). Out of these 1971 routers 212 had no encryption at all (public routers) and are represented with green markers on the map below. Of the remaining encrypted routers, 129 were encrypted using WEP encryption and are represented using yellow markers, 240 and 421 used WPA and WPA2 encryption, respectively. We also found that 951 routers provided both, WPA and WPA2 encryption in parallel. All WPA and WPA2 encrypted routers are represented by the red markers on the map below. 18 routers had an unknown encryption or were ad-hoc access points most probably from people surfing in cafes with their laptops or tablets using WiFi-tethering on the mobile phone.

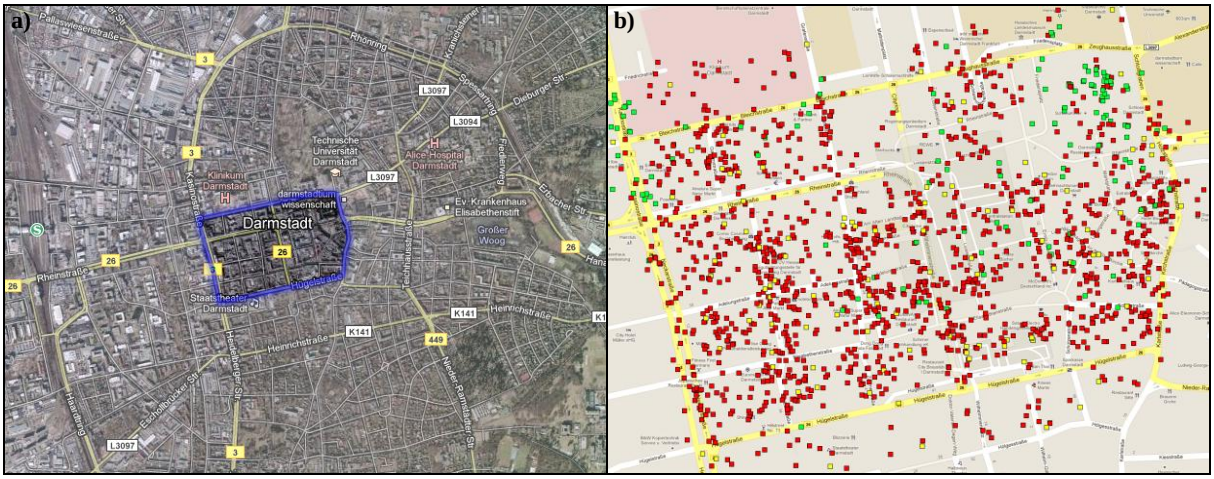

Figure 2: Map[3] of Darmstadt with a) area of measurement and b) estimated positions of wireless APs

Now, having this map of our hometown we can use this information to virtually construct mesh networks and analyze properties of these networks. For this purpose we use different communication ranges and connect two routers if they are in distance of *d* meters with $d \in \{10, 20, 30, 40, 50, 60\}$, therefore, creating six different graphs. We distinguish between encrypted (private) and non-encrypted (public) networks to compare the results to our approach proposed in 2011 (Panitzek et al., 2011). Figure 3 shows how these mesh networks would look like when constructed with *d=30* meters using all nodes (cf. Figure 2.a) or public routers only (cf. Figure 2.b).

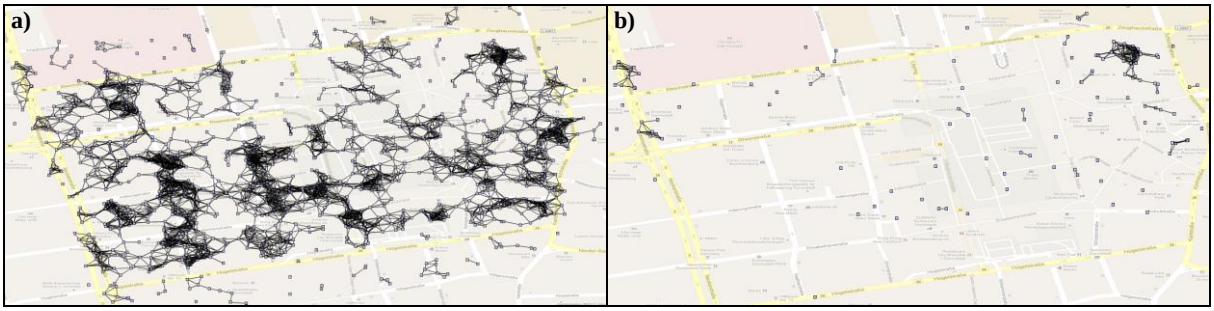

Figure 3: Constructed mesh networks in Darmstadt – a) all nodes, *d=30m* b) public nodes only, *d=30m*

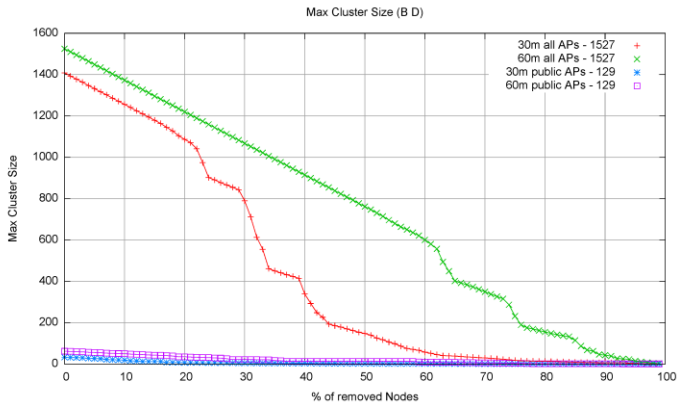

Figure 4: Compare max cluster size of public routers only to all routers

To analyze different graph theoretical properties of our constructed city mesh networks we used the Graph-Theoretic Network Analyzer (GTNA) (Schiller, Bradler, Schweizer, Mühlhäuser and Strufe, 2010). We found that networks constructed using all routers would show good performance and high resiliency to node failures. We also found that with a communication range of 30 meters a mesh network could be easily constructed in urban areas like our hometown. But due to space limitation this evaluation is omitted in this paper and we focus on the comparison between networks containing all routers and networks containing public routers only instead.

[3] Pictures of maps in this work taken from http://maps.google.com

In comparison we found that networks using only public routers have about 30% of isolated nodes when constructed with a range of *d=30* meters and about 5% isolated nodes when constructed with a range of *d=60* meters. When including all nodes only 2% of all nodes are isolated in networks with a range of *d=30* meters. When looking at the size of the biggest cluster (the biggest connected sub-graph) and comparing both networks with each other the discrepancy between these networks becomes obvious (cf. Figure 4). In public networks with *d=30* meters less than 20% of all nodes are connected to the biggest cluster whereas more than 71% of all nodes are connected to the biggest cluster when also including private routers into the network creation process. This shows that private routers will drastically improve not only network performance but also resiliency in an emergency mode mesh network.

CONCLUSION

In this paper we discussed the importance and the implications of an emergency switch for private wireless routers in urban environments. This switch should enable an emergency mode of operation creating a supportive wireless mesh network to assist ad-hoc communication in first response missions. For this purpose we changed an open source wardriving app for Android and gathered real data of wireless routers in our hometown. We used lateration methods to estimate locations of all routers we found during our measurements. We highlighted the drastic improvement gained with an emergency mode switch inside privately owned routers.

Using simulations we plan to evaluate these networks through different ad-hoc routing protocols in our future work. Furthermore, we plan to evaluate how battery life performs under these conditions use an energy model. We plan to integrate these networks in our first response communication sandbox (Bradler, Schweizer, Panitzek and Mühlhäuser, 2008) to evaluate the benefit of such a supportive infrastructure for first response missions.

ACKNOWLEDGMENTS

This work has been partially funded by the DFG research unit 733 QuaP2P.

REFERENCES

1. Aschenbruck, N., Gerhards-Padilla, E. and Martini, P. (2009) Modeling mobility in disaster area scenarios, *Performance Evaluation*, 66(12), 773-790.
2. Bradler, D., Aitenbichler, E., Schiller, B. and Liebau, N. (2009) Towards a Distributed Crisis Response Communication System, *Proceedings of the 6th international ISCRAM conference*.
3. Bradler, D., Kangasharju, J. and Mühlhäuser, M. (2008) Evaluation of Peer-to-Peer Overlays for First Response, *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 463-467.
4. Bradler, D., Schweizer, I., Panitzek, K. and Mühlhäuser, M. (2008) First response communication sandbox, *Proceedings of the 11th communications and networking simulation symposium*.
5. Clark, B. N., Colbourn, C. J. and Johnson, D. S. (1990) Unit disk graphs. *Discrete Mathematics*, 86(1-3), 165-177.
6. Faria, D. B. (2005) Modeling signal attenuation in IEEE 802.11 wireless LANs-vol. 1. *Computer Science Department, Stanford University*.
7. Panitzek, K., Bradler, D., Schweizer, I. and Mühlhäuser, M. (2011) City Mesh – Resilient First Responder Communication. *Proceedings of the 8th International ISCRAM Conference*, 1-10.
8. Raniwala, A. and Chiueh, T. (2005) Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network. *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2223-2234.
9. Rappaport, T. S. (1996) Wireless communications: principles and practice (Vol. 2). *Prentice Hall PTR New Jersey*.
10. Savvides, A., Han, C.-C. and Strivastava, M. B. (2001) Dynamic fine-grained localization in Ad-Hoc networks of sensors, *Proceedings of the 7th annual international conference on Mobile computing and networking - MobiCom'01*, 166-179.
11. Schiller, B., Bradler, D., Schweizer, I., Mühlhäuser, M. and Strufe, T. (2010) GTNA: a framework for the graph-theoretic network analysis, *Proceedings of the 2010 Spring Simulation Multiconference on - SpringSim'10*.