Using Available Wireless / Wired Network Infrastructure for Public Safety and Emergency Early Response

Abdelshakour Abuzneid, Khaled Elleithy
{abuzneid, elleithy, mohannad}@bridgeport.edu
Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06604

Abstract- After September eleven the idea of Public Safety became a key policy goal for every governmental, education and commercial institute. Currently, most of the buildings are equipped with infrastructure for internal and external communication and networking. By being able to utilize the existing infrastructure of wireless / wired network in a building, we can have in place an early response system to disasters. This is important to save lives and get resolution for a disaster sooner. The idea here is to eliminate or reduce additional cost for a dedicated infrastructure for early response system. Due to the growth for the need of internetworking, most of the buildings have already a good base for such a system. This article contributes to the solution of the problem by specifying a novel solution for integration WLAN and existing infrastructure to the system of public safety and emergency early response.

1. Introduction

Recently the Country was struck with many tragic events that resurface the need of a working emergency early response system. The first example was the tragic event of September eleven. The second event was the shooting in Virginia Tech. The third one was the shooting in Northern Illinois University. Three are only to name few. Unfortunately, in all these three occasions, no perfect emergency early response system was implemented on site.

11th September 2001

The recent release of the report from the Nation Commission on Terrorist Attacks upon the United States on 9/11 has posed questions about the design and use of the emergency early response system and interactive systems. However, the evacuation from the WTC complex is widely viewed as a success. Up to 99% of the building occupants below the level of impact survived. This achievement has been attributed to changes that were made both to the emergency exits and to fire evacuation-training programs following the bombing of the WTC in 1993 [1].

However, there were lots of mistakes. As an example, many occupants were advised to remain in their offices and wait rescue when the Stairwell A in the South Tower was still passable. This advice was largely based on experience from the 1993 bombing of WTC when many people were injured as a result of the evacuation [1].

American Flight 11 flew into the North Tower at 8:46:40. The aircraft cut through floor 93 to 99. Occupants began asking for guidance about whether or not to evacuate the building. Local telephone operators and the Fire Department of New York dispatchers relied on standard operation procedures for high-rise fires. The occupants were told to stay low, remain where they were and wait for emergency personnel. This advice was given to callers in the North Tower who were located below and above the impact area. However, the policy created in the aftermath of the 1993 bombing was clearly inappropriate in the context of 9/11. The FDNY chiefs immediately altered the policy and ordered an evacuation as

soon as they arrived in the lobby of the North Tower. One group of occupants on the 83rd floor repeatedly asked 911 operators if the fire was above or below them. The callers were transferred several times and were eventually advised to stay where they were. These callers are unlikely to have survived. Several operators independently decided to tell callers to evacuate if they could. In the South Tower, many occupants continued to call for advice after the second plane hit. The investigation concluded that the 911 system "remained plagued by the operators' lack of awareness". This lack of information may have caused civilians above the impact not to attempt to descend" when the South Tower's stairwell A may still have been passable [1,4].

The communication between building occupants was a problem too. For instance, if one group finds that an exit is blocked during a scenario then they may pass this information to other groups in the same area of the simulated building. The multiple communications channels that were used during September 11th illustrate the naivety of the process. In particular, no previous scenarios seem to consider the impact of widespread cellular telecommunications on evacuation behavior. Fire and impact damage prevented many occupants from hearing the North Tower's deputy fire safety director when he advised tenants to descend at least two floors below the smoke or fire and to wait there. Similarly, many occupants could not use the emergency number '911'. However, the 911 operators and emergency number '911' operators and FDNY dispatchers could not tell callers whether they were above or below the fire [1,4].

2. Safety and Early Response Techniques

Responders rely on a variety of infrastructures for public safety networks to provide mission-critical applications. As an example, land mobile radio (LMR), based on analog voice communications over locally dedicated radio frequencies and transmission facilities had been the mainstay of public safety agencies [2]. Another novel solution is integrating WLAN and Terrestrial Trunked Radio (TETRA) networks. This integration allows a range of brand new capabilities enabled by the WALN, such as broadband data services, true concurrent voice and data services, simultaneous reception of many group calls, reduced call setup and voice transmission delays, improved vice quality, and so forth. IP multicast and Voice-over-IP (VoIP) technologies are great aid to achieving this kind of system [3]. Push-to-talk (PTT) technologies recently have been the domain of traditional land mobile radio (LMR) networks. In the past few years, PTT resurged as a service offered by commercial providers, driven first by private subscribers and, increasingly, by organizations such as law enforcement agencies that traditionally really on LMR's. Many emerging technologies such as voice over IP, CDMA used in 2.5/3G systems helped the resurgence of PTT service [5]. There are many other technologies and techniques used and being developed for safety and early response. It is expensive to build a public safety network exclusively for mission-critical applications. Instead, it is common to build one public safety network shared by both mission-critical and non-mission-critical applications. Such system will be equipped with QoS mechanisms in place to provide preferential treatment to mission-critical applications in an even of an incident. Policy-based resource allocation methods can be effective tools in such a system [6].

3. Using Available Infrastructure for Safety and Early Response

After the math of 9/11, every institution comes to the conclusion that every infrastructure building needs to be equipped with early and safety response system. This conclusion was supported by many tragic events that have happened even after terror attack of 9/11. The idea of having a fixed and working early response system in every building has emerged. The WTC buildings were equipped with great early response technologies but apparently the catastrophe was huge and what has been implemented did not cope with such huge of an action. Big count of the casualties we lost in 9/11 could have been saved if we had a constant feedback to what is going on from within. The lack of information about the exact damage

assessment after the attacks led to the delay of the right action to be taken, rather in some cases, doing the wrong action, such as advising people to stay where they were while they could have escaped the scene using passable stairways at that time. During such huge events, a right decision / action in the right moment could have saved thousands of lives instantly.

Putting all the history of 9/11, Virginia-Tech University and many other worldwide tragic and terror incidents together, made us think how we can do such a feedback from within to the outside world if an emergency to happen to one of the buildings in the University of Bridgeport, in particular, Engineering & Technology Building where we work most of the time.

3.1 Assessment

We started to study how we can implement such a system in the engineering and technology building under the following conditions:

1. Simple and cheap implementation since acquiring a huge budget for such a project was not feasible
2. Fixed system and dedicated to the building; works 24/7.
3. Can work in most if not all the emergencies.
4. In case of an emergency, it can send information from inside to outside.
5. Emergency responders can communicate directions and instructions for the people inside the building in case of any emergency. Needless to say, the instructions could be different to people in different parts of the building according to the situation at that particular location.
6. This system could work even if there is no power due to the emergency.

If the condition #1 was not there, we might be able to have a fast and easy solution since cost factor is a big limitation to any project. We started by collecting information about what we have in the building. We basically have the following:

1. Great Ethernet network infrastructure where basically every laboratory / office / class-room has many data-drops (CAT-6). We have a Gig -feed to the network-room (Tech-114), so the speed of the network was not an issue.
2. The network topology was a collection of multiple starts spanning three floors, where the main star located in Tech-114 as in Figurer-1. So basically every drop eventually connected to the network-room.
3. The building has wireless access through many 802.11g Cisco Access Points (AP) spread over the three floors. The wireless access basically covers all the areas including the hallways.
4. Cameras spread over the building especially in the laboratories. Few are installed in class-rooms and hallways. These cameras are connected to a central network-room (Tech-151). The cameras are fixed (not movable) and do motion-detection recording to a central recording device. The recording device had network capability where you can have access to the recording through its http built-in server. The machines assigned a static IP address. It comes with software application where you can access the recording over Internet. We checked the quality of such application and it was reasonable. One exception, you cannot record the voice from all the cameras at one time.
5. There are no speakers in the building where emergency responders can send (voice) information from outside to stranded occupants in case of an emergency (that was scary while remembering the tragic event of 9/11).
6. Cell/Mobile phone reception is good except of the lower level (basement). We tried the signals of the major cell phone companies in the area.

7. Emergency exit signs and lights are installed all over the building according to the state code; we know it is tested regularly.
8. The building does not have an emergency electric generator, so in a case of power outage, no instant / temporary electric-power could be provided to the crucial parts of the building such as the network-room; except the emergency lights and exit signs which have rechargeable-batteries. The network equipment (routers, switches, hubs, access points) do not have Uninterrupted Power Supply (UPS). That means in case of a power failure due to an emergency (such as a fire), no access to the network infrastructure is possible.

3.2 Planning

We started by connecting the dots together and putting together few plans. The moment we finish one plan, we analyze its weaknesses and then plug a patch into it and come up with a better plan.

3.2.1 Plan I: Make it simple

Since we have a network of cameras connected to a single recording machine which is Internet accessible, install the application on a PC located outside the building to get a live picture of what is happening during the emergency. If there is a power outage then the data network and camera network will not work. There is no intercom system to communicate the information to the people inside the building. To fix and improve this plan, we developed plan II.

3.2.2 Plan II: Combine cameras network with data infrastructure network

We have to have a kind of UPS for the recording machine and the power-feed to the cameras. We also need to have UPS in all the network devices from the camera recording machine down to the main network room. That means every hub or switch down to the main switch in the network room to the router and maybe the fiber power should be protected against power failure. Install zoned intercom devices in all critical and easy-to-hear areas. This intercom system must be supported by rechargeable-battery to be able to function in case of power-failure, Figurer-2. What will happen if a fire as an example (or normal failure) eats up one of the network devices that connect the recording machine? Of course no communication will happen at all. So, this scenario works in some incidents like Virginia-Tech but might not work in the incident of 9/11 where a huge fire could have destructed the network by the fire flames. What else we can do in plan III to mitigate such weaknesses?

3.2.3 Plan III: Introduced Wireless

The idea of using a wired network could not work in case of a huge disastrous incident such as a spreading fire. This risk could be reduced by segmenting the network but again, it cannot provide a complete fault-tolerance. It seems that relying on wired network does not work. We need to move to wireless communications world. So, we need to use a network or a fleet of wireless cameras. These wireless cameras could be connected via dedicated Access Points (AP) and / or dedicated channels to the infrastructure network. With this design we see a safe path among the cameras and the AP's. Multiple cameras and AP's on one area works as a good fault-tolerance. However, AP's in infrastructure mode are connected by wires. This brings us to a smaller version of the problem of Plan II. Let's eliminate all wires!

3.2.4 Plan IV: Completely Wireless

Complete Ad-Hoc network where cameras and AP's communicate via Ad Hoc Network. We presume that the cameras and AP's have power-outage fault tolerance like if they have rechargeable-batteries, they are connected to UPS, or maybe their power circuits are connected to a central power-generator which kicks off in complete or partial power-failure. Since the cameras are not connected to a central networked recorder, each and every camera should have its simple / basic web (http) server, where it could be accessed from another IP machine, inside or outside the network.

4. Current Supporting Technology:

We have put together four plans. While disregarding the cost factor, we tried to find out if the current available technology can support any of the plans by acquiring the required parts and equipment. We had absolutely no obstacles to implement the first three plans. We basically can acquire all the parts that we are missing (we had a good infrastructure in the building already). We were able to implement the first three plans. Unfortunately, Plan IV was very hard to fully implement as per the design described above.

In addition, 802.11 wireless LANs were designed with LAN-style data transmission in mind. Only recently have multimedia applications been introduced onto the LAN, and wireless soon followed. The natural progression was to see multimedia applications move onto the wireless infrastructure, making mobile voice and video possible. 802.11 base standard defines a set of Quality of Service (QoS) extensions to the 802.11 MAC layer that are designed to provide higher-quality and more consistent voice and video transmission [7].

5. Cost Analysis

It is very hard to have direct comparison and analysis for the cost of the four proposed plans. There are many parameters to factor for which makes it a completely not linear proposition. Parameters could include but not limited to:

1. Technology used and equipment cost
2. Supported infrastructure, this includes, power-protection infrastructure, network infrastructure, camera network infrastructure, to name few.
3. coverage area or how many cameras per specific sized-area
4. Fault tolerance equipment
5. Quality of the video / audio

We have acquired prices for the four plans. One constraint we have is to have one camera per one closed area (class-room, laboratory, office, are examples of a closed area). The camera is static (not rotating or movable). We come with the following cost comparison in Figure-3 (approximation). We notice that as we upgrade the plan the cost will rise. However, the fault-tolerance and response efficiency will improve.

6. Future Work

There are few other wireless LAN infrastructure that we need to implement and see how efficient for building early and safety response systems such as wireless LAN bridges, wireless Workgroup bridges, wireless LAN switches, enterprise wireless gateways and WLAN Mesh routers. Mesh routers introduce WLAN technology at the core of the network with the hope of giving certain types of networks a much needed component; reliability. These network types are specific, such as across cities, within historic buildings where cabling isn't allowed and for constructed networks such as disaster relief sites. Reliability is achieved through high availability, and high availability is achieved through instant failover WLAN mesh router use proprietary routing protocols to route data traffic between the mesh routers [6]. There is

also a large room to check for suitable network equipment and cameras to be used in case of certain emergencies. As an example, using a fire rated Access Points, cameras and wires to build safety networks. To make sure the communicated information is understood by everyone, multi-lingual system could be adopted. Handicapped occupants during emergency incidents might need different needs and / or methods of communication. So far we spoke about audio format of instructions to be sent, how about a sort of projection show / video in certain areas of the incident.

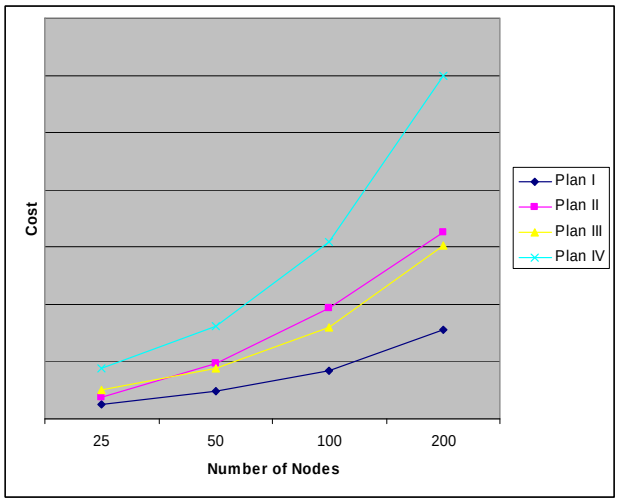

Figure 3: Plan Cost Comparison (Estimation)

6. Conclusion:

In this paper we have developed a practical approach to figure out how to build an early and safety response system that could fully work under sever emergencies such 9/11 catastrophic incident. We started with the understanding of the need of adapting the current available technologies; wireless technologies in particular. We have checked for different approaches that could get us the best fault-tolerance. We needed to have a direct feedback from within the incident to the external world with an efficient and working channel of communication from the external emergency responder (presuming that they cannot be inside the incident area) to the people who need help inside the incident area. The quality of video and audio streaming over wireless channel is not great yet under most of the current technologies. There is still a reasonable sized room for improvement.

References

[1] C.W. Johnson, "Applying the Lessons of the Attack on the World Trade Center, 11th September 2001, to the Design and Use of Interactive Evacuation Simulations", CHI 2005.

[2] T.L. Doumi," Spectrum Considerations for Public Safety in the United States", IEEE Communications Magazine, January 2006

[3] A.K. Salkintzis, "Evolving Public Safety Communication Systems by Integrating WLAN and TETRA Networks", IEEE Communications Magazine, January 2006

[4] US National Commission on Terrorist Attacks Upon the United States, 9/11 Commission Report, Washington DC, 2004. Available on: http://www.9-11commission.gov.

[5] L.A. DaSilva, G.E. Morgan, C.W. Bostian, D. G. Sweeney, S. F. Midkiff, J. H. Reed, C. Tompson, W.G. Newhall, B. Woerner, "The Resurgence of Push-to-Talk Technologies", IEEE Communications Magazine, January 2006

[6] J.Q. Bao, L. Guo, W.C. Lee, "Policy-Based Resource Allocation in a Wireless Public Safety Network for Incident Scene Management", MobiCom '06 Proceedings of the 12th annual international conference on Mobile computing and networking

[7] Certified Wireless Network Administrator, Official Study Guide, Third Edition.

Biographies

Dr. Khaled Elleihty received the B.Sc. degree in computer science and automatic control from Alexandria University in 1983, the MS Degree in computer networks from the same university in 1986, and the MS and Ph.D. degrees in computer science from The Center for Advanced Computer Studies at the University of Louisiana at Lafayette in 1988 and 1990, respectively. From 1983 to 1986, he was with the Computer Science Department, Alexandria University, Egypt, as a lecturer. From September 1990 to May 1995 he worked as an assistant professor at the Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. From May 1995 to December 2000, he has worked as an Associate Professor in the same department. In January 2000, Dr. Elleithy has joined the Department of Computer Science and Engineering in University of Bridgeport as an associate professor. In May 2003 Dr. Elleithy was promoted to full professor. In March 2006, Professor Elleithy was appointed Associate Dean for Graduate Programs in the School of Engineering at the University of Bridgeport. Dr. Elleithy published more than seventy research papers in international journals and conferences. He has research interests are in the areas of computer networks, network security, mobile communications, and formal approaches for design and verification.

Abdelshakour Abuzneid has received his BS degree in Computer Engineering and Control from Yarmouk University and MS degree in Computer Engineering from the University of Bridgeport in May 1997. Currently Abdelshakour is pursuing his PhD in Computer Science & Engineering from the University of Bridgeport. His research interest is in Data / computer / wireless / mobile communications. He has published few journal and conference papers. Abdelshakour has worked as a reviewer to many conferences. Abelshakour has 12 years of experience in the field of networks and systems. His MCSE, MCP, CWNA and SCSA certified.

Mohannad Abuzneid has received his BS degree in Computer Engineering and Control from Yarmouk University and will receive his MS degree in Computer Engineering from the University of Bridgeport in May 2008.