Date of publication 28 May 2024, REFERENCE: IEEE ACCESS

Digital Object Identifier 10.1109/ACCESS.2023.1120000

The Experimental Solution of Communication Infrastructure in The Most Deadly Natural Disaster:(230206:0427) of Modern History

IKRAM CELAL KESKIN[1], Student, University of Manisa Celal Bayar

[1]Computer Engineering Dep, Manisa Celal Bayar University, Prof.Dr.Ilhan Varank Campus, Muradiye, MANISA, TR (e-mail: 200316059@ogr.cbu.edu.tr)
[2]Tuzla, Istanbul, TR (e-mail: info@celalkeskin.com.tr)

Corresponding author:Ikram Celal KESKIN (e-mail: info@ celalkeskin.com.tr).

ABSTRACT Turkey was shaken by an earthquake of 7.8 magnitude, which was called as the largest natural disaster of the 21st century at 4:17 pm on February 6, 2023. Earthquake's central bases respectively as Kahramanmaraş Pazarcık and Elbistan districts were recorded. 10 provinces were shot by the earthquake in Turkey. Compared to the area they covered, the total area of the destroyed regions of the cities due to the earthquake was recorded as larger than some of the "countries" in Europe. In other words, if this earthquake had taken place in Europe, some countries of Europe would have been erased from the map. According to the official records, in Turkey, at least 53 thousand 537, and in Syria, at least 8 thousand 476 people lost their lives. Besides a total of more than 122 thousand people were injured. After the "disaster", where such great destruction took place, there were difficulties in some of the services required to survive daily life. One of them was observed in the field of "Digital Communications/Computer Networks". It was seen that private mobile service operators in our country have delayed their services or never have transferred their equipment to the region. It is clearly seen that they did not have any plans or studies on what to do at the time of encountering such a disaster. In this study, the answer to the following question will be searched: "MCBU Computer Engineering Students, who have taken the Computer Network course; if they had created a plan or a design of a network, or if they had created a list of the needed equipment, or if they had developed a demo of the base network construction for communication infrastructure, would they had provided a real solution which helps the people trying to establish communications with life-critical services ?"

INDEX TERMS Network, Communication, Network Infrastructure, Network Services, Network Design, Network Demo

I. INTRODUCTION

THE earthquake having a magnitude of 7.8 on 6 February 2023, which is the biggest disaster of the century in Turkey, took its place in history as the common pain of the whole world. The destroyed area in this earthquake covered the area as large as some of the countries in the world. An earthquake of such a huge size was a real disaster.

In real disaster cases, it is important to keep vital services surviving. Some of these services are; hot/cold food supply, toilet/bath needs, eliminating housing needs, maintenance of basic communication opportunities, educational services, defining the important geo-points for being gathered etc.

The collapse of communication networks during a natural disaster is something we want to avoid at all costs. Systems that are set up amateurishly reveal their flaws and shortcomings during such critical times, leaving us scrambling for makeshift solutions. Our objective is to prevent this scenario from recurring by rebuilding the systems with professionalism and ensuring that contingency plans, like Plan B and Plan C, are always ready to be deployed.

To elaborate, communication networks are crucial during disasters for coordination, emergency responses, and maintaining public order. If these networks fail, it not only hampers rescue operations but also causes widespread panic and disarray. Systems built without foresight and expertise often lack the robustness needed to withstand such emergencies, which is why they fail when they are most needed.

Our approach should start with a thorough assessment of the current infrastructure. Identify the weaknesses and potential points of failure. From there, we need to design a resilient system architecture that can handle various disaster scenarios. This includes ensuring redundancy in critical components, so if one part fails, another can take over without disrupting the entire network.

Moreover, we must incorporate advanced technologies such as automated failover systems, which can quickly switch to backup resources. These systems should be tested regularly under simulated disaster conditions to ensure they work as intended when the real need arises. The use of robust, high-quality materials and equipment is also crucial to ensure durability and reliability.

Furthermore, having clear and well-documented disaster recovery plans is essential. These plans should outline the steps to be taken in case of different types of failures and should be easily accessible to all relevant personnel. Regular training and drills should be conducted to ensure everyone knows their roles and responsibilities during an emergency.

In this report, we will discuss Plan B. Specifically, we will address the necessary steps and materials required to restore communication during the period when the broken cables are being replaced in the event of a disaster. We will cover the following aspects:

Minimum Number of Materials Needed: Identifying the essential materials and equipment required to quickly set up a temporary communication network.

Implementation: Detailed steps on how to deploy these materials effectively.

Simulation Environment Using Cisco Packet Tracer: Creating a simulation of the temporary network setup to validate our implementation plan.

Potential Problems: Identifying possible issues that could arise during the implementation.

Solutions to Potential Problems: Proposing solutions to address these issues and ensure the network remains operational.

By discussing these points, we aim to ensure that, in the event of a disaster, we can swiftly restore communication networks using Plan B, minimizing downtime and maintaining critical communication channels.

II. MATERIALS

The following section outlines the critical materials required for effective disaster recovery operations, specifically focusing on mobile disaster recovery vehicles, drones, and control units.

A. MOBILE DISASTER RECOVERY VEHICLES

The most crucial component we need for materials is mobile internet vehicles. These vehicles must be modified to include a sound-insulated system that converts gasoline to electrical energy. During an earthquake disaster, generating noise can hinder our ability to hear the voices of people trapped under the debris.

Therefore, it is essential that these modified mobile internet vehicles are also capable of providing electricity. Given this dual functionality, it would be more accurate to refer to them as mobile disaster recovery vehicles instead of simply mobile internet vehicles.

Key features and requirements for these vehicles include:

- **Mobile Internet Capability:**The primary function of these vehicles is to establish a temporary communication network. They should be equipped with advanced mobile internet technology to provide reliable connectivity in affected areas.
- **Power Generation:** These vehicles must have built-in generators that convert gasoline to electrical energy. This will ensure they can operate independently without relying on external power sources.
- **Sound Insulation:** The power generation system should be sound-insulated to minimize noise. This is crucial for maintaining a quiet environment to detect any sounds from survivors trapped under the rubble.
- **Versatility:** In addition to providing internet connectivity, these vehicles should be able to power other essential equipment, such as lights, medical devices, and other communication tools.

B. DRONES

Another essential component we need is drones. These drones must also be modified to either have sound-insulated propellers to reduce noise or be of a type that does not use propellers. Additionally, these drones should be equipped with internet coverage extenders. They should have a system that amplifies the WiFi signals of the mobile disaster recovery vehicles.

Key features and requirements for these drones include:

- **Noise Reduction:** The drones must be modified to operate quietly. This can be achieved by using sound-insulated propellers or opting for drones that use alternative propulsion systems that produce less noise. This is crucial for maintaining a quiet environment to aid in rescue operations.
- **Internet Coverage Extension:** The drones should be equipped with technology to extend internet coverage. They must have the capability to amplify and relay WiFi signals from the mobile disaster recovery vehicles, ensuring a broader and more reliable communication network.
- **Mobility and Flexibility:** These drones should be able to operate in various terrains and conditions, providing flexibility in deploying communication networks in hard-to-reach areas.

- **Autonomy and Battery Life:** The drones should have a long battery life and the ability to operate autonomously for extended periods, ensuring continuous support in disaster-stricken areas.

By integrating these modified drones with the mobile disaster recovery vehicles, we can significantly enhance the coverage and reliability of the temporary communication network. This will ensure that we maintain critical communication channels even in the most challenging environments during a disaster recovery operation.

C. CONTROL UNITS

Control units are vital for coordinating the disaster recovery efforts. They ensure that all the mobile disaster recovery vehicles and drones operate in a synchronized manner, providing comprehensive coverage and efficient resource allocation. Control units are divided into three levels: District Control Units, Region Control Units, and a Central Control Unit.

1) District Control Units

District Control Units are responsible for overseeing disaster recovery operations within specific districts. They serve as the first point of contact for deploying resources and managing local recovery efforts.

Key responsibilities include:

- **Local Coordination:** Managing and coordinating the deployment of mobile disaster recovery vehicles and drones within the district.
- **Resource Allocation:** Distributing resources such as power, internet connectivity, and medical supplies based on real-time needs and priorities.
- **Communication Relay:** Ensuring effective communication between field teams and the Region Control Units.

2) Region Control Units

Region Control Units oversee multiple District Control Units, ensuring that disaster recovery efforts are aligned across a broader geographic area. They play a critical role in managing resources and support across districts.

Key responsibilities include:

- **Regional Coordination:** Overseeing and supporting the operations of multiple District Control Units.
- **Resource Management:** Allocating and reallocating resources between districts to optimize the overall recovery effort.
- **Data Aggregation:** Collecting and analyzing data from District Control Units to provide a comprehensive overview of the regional situation.
- **Communication Hub:** Acting as an intermediary between District Control Units and the Central Control Unit to ensure seamless communication.

3) Central Control Unit

The Central Control Unit is the highest level of coordination in the disaster recovery hierarchy. It provides strategic oversight and decision-making support for the entire operation.

Key responsibilities include:

- **Strategic Planning:** Developing and implementing overarching strategies for disaster recovery and resource allocation.
- **Centralized Management:** Coordinating the activities of all Region Control Units to ensure cohesive and efficient operations.
- **Resource Oversight:** Managing national or international resources and deploying them as needed across regions.
- **Policy and Compliance:** Ensuring that all recovery operations comply with national policies and international standards.
- **Advanced Analytics:** Utilizing advanced data analytics to predict needs, allocate resources, and optimize recovery efforts.

By establishing these control units at various levels, we can ensure a well-coordinated and effective disaster recovery operation. This structured approach allows for quick response times, efficient resource utilization, and reliable communication across all levels of the recovery effort.

III. METHODOLOGY

In this section, we detail the implementation of our disaster recovery network infrastructure using Cisco Packet Tracer. Our goal is to establish a robust and resilient communication network that can be rapidly deployed in the event of a natural disaster, ensuring uninterrupted communication for emergency services and affected populations.

Our network design is hierarchical, comprising several levels of control units: Central Control Unit, Region Control Units, and District Control Units. Each unit is responsible for specific geographical areas and functions, ensuring a scalable and manageable network infrastructure.

Our disaster recovery network is designed to ensure robust and resilient communication during natural disasters. The network is organized hierarchically into three levels: Central Control Unit (CCU), Region Control Units (RCUs), and District Control Units (DCUs). This structure allows for scalable and manageable network operations, where each level has specific responsibilities and areas of control.

The units were planned to communicate with mobile disaster recovery vehicles via satellite, but since the satellite is not available in Cisco Packet Tracer, the closest solution to an end system in this scenario could be temporarily laying telephone lines along the road or even parking hundreds of vehicles at road corners. However, this is not the focus of our simulation or the subject we intend to simulate; it is independent of our project.

So how will these people securely access the internet? The answer to this question is very simple for someone staying at a KYK dormitory. We will create an interface system similar to kyk.gsb.gov.tr, where you can log in to the system with your e-Government password and e-Government ID number, and the login record is kept only at the main center. Messages will be encrypted using AES256 encryption before transmission, as security will be needed even at the link layer. Now, everyone can access the internet securely and quickly.

IV. IMPLEMENTATION

In this section, we detail the implementation of our disaster recovery network infrastructure using Cisco Packet Tracer. Our goal is to establish a robust and resilient communication network that can be rapidly deployed in the event of a natural disaster, ensuring uninterrupted communication for emergency services and affected populations.

Our network design is hierarchical, comprising several levels of control units: Central Control Unit (CCU), Region Control Units (RCUs), and District Control Units (DCUs). Each unit is responsible for specific geographical areas and functions, ensuring a scalable and manageable network infrastructure.

The following steps outline the implementation of the network infrastructure:

A. SETUP OF CENTRAL CONTROL UNIT (CCU)

The Central Control Unit (CCU) is configured using a high-end router (e.g., Cisco 2911) connected to a server for central authentication and encryption (AES256). The CCU connects to the Internet Service Provider (ISP) using a serial connection.

```
Router(config)# hostname CCU
Router(config)# interface
GigabitEthernet0/0
Router(config-if)# ip address
192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address
10.0.0.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network
192.168.1.0 0.0.0.255 area 0
Router(config-router)# network
10.0.0.0 0.0.0.3 area 0
Router(config-router)# end
```

B. SETUP OF REGION CONTROL UNITS (RCUS)

Region Control Units (RCUs) are deployed using intermediate routers (e.g., Cisco 1941). Each RCU connects to the CCU using serial or fiber optic connections for redundancy and includes a server for regional authentication and resource management.

```
Router(config)# hostname RCU1
Router(config)# interface
GigabitEthernet0/0
Router(config-if)# ip address
192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address
10.0.0.2 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network
192.168.2.0 0.0.0.255 area 0
Router(config-router)# network
10.0.0.0 0.0.0.3 area 0
Router(config-router)# end
```

C. SETUP OF DISTRICT CONTROL UNITS (DCUS)

District Control Units (DCUs) use routers (e.g., Cisco 1841) and connect to their respective RCUs. Each DCU manages local mobile disaster recovery vehicles and drones, with a backup connection to another RCU to maintain network resilience.

```
Router(config)# hostname DCU1
Router(config)# interface
GigabitEthernet0/0
Router(config-if)# ip address
192.168.?.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address
10.0.1.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network
192.168.?.0 0.0.0.255 area 0
Router(config-router)# network
10.0.1.0 0.0.0.3 area 0
Router(config-router)# end
```

D. MOBILE DISASTER RECOVERY VEHICLES

Mobile disaster recovery vehicles use portable wireless routers (e.g., Cisco 819 ISR) to provide WiFi access and connect back to the nearest DCU. These vehicles are equipped with generators and sound insulation.

```
Router(config)# hostname MobileVehicle1
Router(config)# interface
GigabitEthernet0/0
Router(config-if)# ip address
192.168.20.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address
10.0.2.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network
192.168.20.0 0.0.0.255 area 0
Router(config-router)# network
10.0.2.0 0.0.0.3 area 0
Router(config-router)# end
```

E. DRONES FOR EXTENDED COVERAGE

Drones are simulated using wireless access points (e.g., Cisco Aironet) to extend the WiFi coverage from the mobile disaster recovery vehicles. These access points operate on different channels to avoid interference.

```
AccessPoint(config)# interface Dot11Radio0
AccessPoint(config-if)# ssid
DisasterRecoveryDrone
AccessPoint(config-if)# exit
AccessPoint(config)# interface
GigabitEthernet0
AccessPoint(config-if)# ip address
192.168.25.1 255.255.255.0
AccessPoint(config-if)# no shutdown
AccessPoint(config-if)# exit
AccessPoint(config)# end
```

V. DISCUSSION AND CONCLUSION

A. DISCUSSION

In this section, we consider various potential problems that may arise during the installation and operation of our disaster recovery network infrastructure and provide the most logical solutions to these problems.

Potential Problem: Network Congestion

Network congestion is a significant problem, especially in disaster scenarios where high volumes of data traffic can overwhelm the network. This can cause performance degradation and delays in critical communications. In case of network congestion, a routing algorithm can be written to the empty paths

Potential Problem: Equipment Failures

Equipment failures, including hardware failures and software bugs, can severely impact the functionality of our disaster recovery systems. Ensuring the reliability and robustness of all components is a completely independent factor and will not be covered in this project

Potential Issue: Unexpected Load Distribution

Unexpected load distribution may occur due to uneven demand across the network. This can lead to some nodes being overloaded while others are underutilised, potentially causing performance bottlenecks and inefficient resource utilisation. Optimisation algorithms such as ant colony can be used to make the algorithm run more smoothly

Potential Problem: Noisy Operation of Drones

The noisy operation of drones is a critical issue, especially in rescue missions where quiet environments are required to detect the sounds of victims trapped under debris. To alleviate this problem, noise reduction technologies should be integrated into the drone design. The easiest solution is a propeller-less drone, but by applying sound insulation to the propellers, it can be made much quieter than expected

Potential Issue: Noisy Operation of Petrol-to-Electricity Engine in Mobile Disaster Recovery Vehicles

The noisy operation of petrol-to-electric engines in mobile disaster recovery vehicles can similarly hamper rescue efforts. Soundproofing techniques need to be used to minimise noise levels and provide a conducive environment for identifying survivors.

Potential Issue: Lack of Electricity to Charge Drones and Other Essential Equipment

The availability of electricity to charge drones and other essential equipment is a potential challenge in disaster-affected areas. Ensuring a reliable power supply through the integration of efficient energy generation and storage systems is imperative for continuous operation.

B. CONCLUSION

In conclusion, while this study emphasises the design and deployment of a comprehensive disaster recovery network infrastructure, it is important to address several potential issues to ensure its effectiveness. Network congestion, equipment failures, and unexpected load distribution are key concerns that must be managed through sound planning and resource allocation.

In addition, noise generated by drones and mobile disaster recovery vehicles poses a significant challenge to recovery operations. The implementation of noise reduction technologies and sound insulation techniques will be crucial in overcoming these issues.

The availability of electricity to charge drones and other necessary equipment remains a critical factor for the sustainable functionality of the network. Therefore, it is vital to integrate reliable energy generation and storage solutions.

This study underlines the importance of developing a flexible and adaptable disaster recovery network and how it can be done. Future research should focus on optimising the aspects discussed and exploring innovative solutions to improve the overall effectiveness of disaster response efforts. Further caveats, recommendations and potential improvements should be documented on an ongoing basis and addressed as part of ongoing assessments and updates to network infrastructure.

C. COPYRIGHT ISSUE

VI. REFERENCES

REFERENCES

[1] *"Global CMT Catalog Search"*. Global Centroid Moment Tensor. 6 February 2023. Archived from the original on 7 February 2023. Retrieved 6 February 2023.

[2] https://www.meb.gov.tr/6-subat-depremlerinin-birinci-yilinda-yapilan-egitim-seferberligi/haber/32458/tr

[3] Ocal T., Yıldız A., *"06 ŞUBAT 2023 KAHRAMANMARAŞ DEPREMLERİ ÖNCESİ TOPLANMA ALANLARININ COĞRAFİ ANALİZİ: ANTAKYA VE ÇEVRESİ", Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergis*, vol. 20, no. 52, pp. 132-157, 2023, 10.1109/TED.2016.2628402.

[4] https://www.tmmob.org.tr/sites/default/files/tmmob_deprem_raporu_son_4agustos-part-1.pdf

[5] https://www.trthaber.com/haber/gundem/deprem-bolgesinde-iletisim-aglari-guclendiriliyor-747230.html

[6] https://www.techtarget.com/searchnetworking/tip/IP-addressing-and-subnetting-Calculate-a-subnet-mask-using-the-hosts-formula

[7] https://www.geeksforgeeks.org/small-organization-set-up-in-cisco-packet-tracer/

[8] https://en.wikipedia.org/wiki/Soundproofing

[9] Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H. (2000). *Energy-efficient communication protocol for wireless microsensor networks*. In Proceedings of the 33rd annual Hawaii international conference on system sciences, pp. 10-pp. Available at: https://ieeexplore.ieee.org/document/926982

[10] Huang, C. M., Hsieh, C. H., Yeh, C. Y. (2013). *Disaster management using wireless sensor networks: a measurement study*. IEEE Transactions on Wireless Communications, 12(6), 1989-1999. Available at: https://ieeexplore.ieee.org/document/6525611

[11] Louazani, S., Zrelli, I. (2013). *Wireless Sensor Networks for Disaster Management*. Retrieved from https://www.academia.edu/6393904/Wireless_-Sensor_Networks_for_Disaster_Management

[12] Bhattacharyya, D. K., Kim, T. H. (2014). *An Effective Protocol and Algorithmic Approach for Disaster Management Using Wireless Sensor Networks*. Retrieved from https://www.academia.edu/73754467/An_-Effective_Protocol_and_Algorithmic_Approach_for_Disaster_Management_Using_Wireless_Sensor_Networks

[13] Shinghal, K. (2016). *A Review on Wireless Sensor Network Protocol for Disaster Management*. Retrieved from https://www.academia.edu/54968270/A_Review_on_Wireless_Sensor_Network_Protocol_for_Disaster_Management

[14] Yadav, A., Chauhan, S. (2020). *International Journal of Enterprise Computing and Business Systems: An Effective Protocol and Algorithmic Approach for Disaster Management Using Wireless Sensor Networks*. Retrieved from https://www.academia.edu/73754786/International_-Journal_of_Enterprise_Computing_and_Business_Systems_AN_EFFECTIVE_PROTOCOL_AND_ALGORITHMIC_APPROACH_FOR_-DISASTER_MANAGEMENT_USING_WIRELESS_SENSOR_NETWORKS

CELAL IKRAM KESKIN was born in 2002 in Çiçekdağı, Kırşehir. He completed his high school education (2016-2020) at Mehmet Tekinalp Anatolian High School in Tuzla, Istanbul. In 2020, he won the Department of Computer Engineering at Celal Bayar University. He is currently working part-time at Celal Bayar University Rectorate IT Technical Support.