IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received July 16, 2019, accepted July 20, 2019, date of publication July 29, 2019, date of current version August 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2931539

Design and Deployment of UAV-Aided Post-Disaster Emergency Network

KIRTAN GOPAL PANDA[1], SHRAYAN DAS[1], DEBARATI SEN[1], (Senior Member, IEEE), AND WASIM ARIF[2], (Member, IEEE)
[1]Indian Institute of Technology Kharagpur, Kharagpur 721302, India
[2]National Institute of Technology Silchar, Silchar 788010, India

Corresponding author: Kirtan Gopal Panda (kirtangopal.panda@gmail.com)

This work was supported by the Ministry of Electronics and Information Technology, Government of India, through the program "Development of National Disaster Spectrum (NDS) and Disaster Communication Backbone Architecture (DiCoBA) with Prototype Development" under Grant 21(1)2015-CC & BT Dated 30-09-2015.

ABSTRACT Designing a reliable, resilient, and quickly deployable emergency communication network is a key challenge for post-disaster management. In this paper, a UAV-assisted emergency Wi-Fi network is proposed to expedite the rescue operations by guiding the survivors to the nearest rescue camp location. Here, the Raspberry PI (RPI) development board, mounted on UAV is considered to form a Wi-Fi chain network over the disaster region. During network set-up, the proposed solutions for the design challenges like UAV synchronization, avoid communication disruption and surveillance data management are the key contributions of this paper. The designed UAV network is capable of doing on-site surveillance and transmitting the data to the relief center for better rescue planning. One major challenge is to alert a survivor about the emergency network, which is addressed by designing a captive portal. Furthermore, to extend the Wi-Fi network, an Android-based application is developed by which each smartphone acts as a relay for its neighbor. Three types of field experiment are carried out to evaluate the performance of the designed prototype. It is found from the field results; the Wi-Fi access point mode and user datagram protocol are more suitable for network design as compared to Ad-Hoc mode and transmission control protocol, respectively. It is also observed from the experiment that the maximum hop distance for the prototype is 280 meters and 290 meters for a Wi-Fi configuration following IEEE 802.11n and IEEE 802.11ac protocol, respectively.

INDEX TERMS Unmanned aerial vehicle (UAV), post-disaster management, emergency network, network chain.

I. INTRODUCTION

Over the past few years, the world has seen many disasters such as the Tohoku earthquake and tsunami in Japan (2011), the Haiyan typhoon in the Philippines (2013), the Gorkha earthquake in Nepal (2015), and the Fani cyclone in India (2019). A disaster can be natural or man-made, which causes massive destruction of infrastructures and loss of human lives. The first few hours following a disaster may be considered as the golden relief time to save the lives of several victims by providing emergency aid. Statistically, nearly half of the total casualties occur just within 2-3 hours after a disaster [1]. During disaster, the existing infrastructure and the conventional communication systems collapse, and the affected areas are disconnected without any means of exchange of information. Therefore, it becomes difficult for First-Responders (FRs) to locate the survivors during Search And Rescue (SAR) operation and also for survivors to communicate for emergency aid. To alleviate post-disaster consequences and save lives, communication between survivor and rescue crew is crucial to take place. Therefore, it is indispensable to design a reliable, resilient, and a quickly deployable emergency communication network for the post-disaster situation.

In a post-disaster scenario, mainly three different strategies are documented for setting up an emergency communication network [2]. The strategies are based on 1) satellite communication, 2) Locally Deployed Resource Unit (LDRU), and

The associate editor coordinating the review of this manuscript and approving it for publication was Gurkan Tuna.

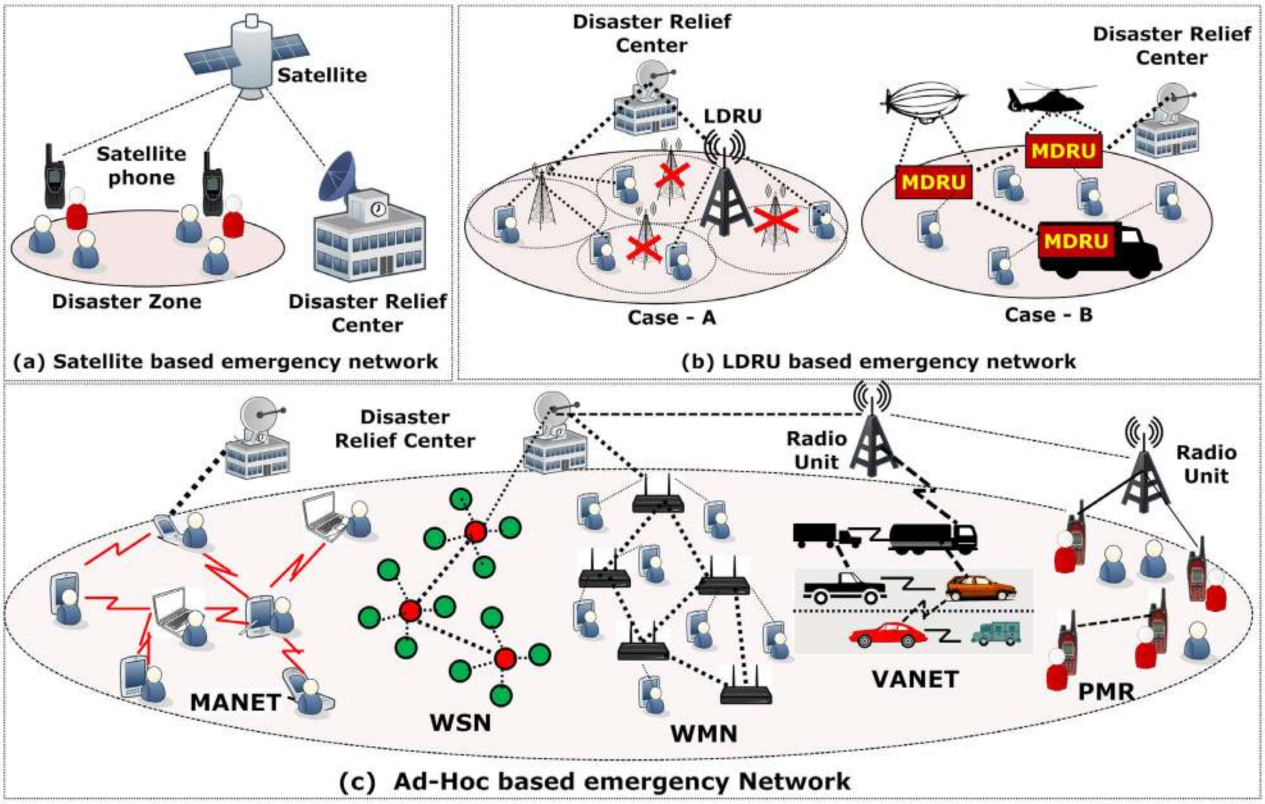


FIGURE 1. Different types of emergency network based on different strategies. (a) Satellite based emergency network, (b) LDRU based emergency network (Case A - few cellular base stations are damaged, Case B - all base stations are damaged), (c) Ad-Hoc based emergency network (formation of MANET, WSN, WMN, VANET and PMR over the disaster region).

3) Ad-Hoc connection. In Fig. 1, different types of emergency network based on the above three strategies are shown. The most common and traditionally used emergency communication system is satellite-based communication. But, the high cost of satellite phones compared to smartphones and the requirement of basic operational knowledge, limits its service only to a few survivors and FRs. Use of satellite communication can be fully utilized if the smartphone manufacturer incorporates an emergency mode with a compatible transmission scheme or by using commercially available products like bivystick [3]. Both the solutions have an adverse effect on the cost and battery life of the smartphone. In 2014, Vodafone unveiled Vodafone Instant Network mini [4], which can host a mobile network of 100 meters coverage via satellite in the disaster region. As the device needs to be carried and installed manually, it is not preferable for all post-disaster scenarios.

Emergency communication set-up using LDRU may differ depending upon the intensity of the disaster. In some cases, only a few cellular Base Stations (BSs) are damaged (Case A) whereas in other cases, almost all the BSs are lost (Case B). In Case A, to start emergency communication, remaining BSs need to change the earlier transmission scheme to serve a large coverage area [5]. The remaining area is served by LDRU. For Case B, specially designed Movable and Deployable Resource Units (MDRUs) are used [6]. Each MDRU container carries the components such as the wired/wireless transceiver, switches/routers, servers, power source unit, and air conditioner for providing a communication service [7]. It is transported to the disaster zones through helicopters, trucks, airships, etc. Although MDRUs have quite advanced features such as remote operation and maintenance, modularized and virtualized MDRU functions, but it requires a few days for restoration. The golden time for rescue may be missed if we solely rely on MDRU based communication.

With the above considerations, wireless Ad-Hoc network has been considered as an appealing technology for emergency communication [8]. Due to no pre-existing infrastructure requirement for Ad-Hoc network set-up, this technology has garnered major attention as a solution for designing a post-disaster communication system. The basic idea behind the Ad-Hoc network is to set-up a temporary multihop communication link between two or several nodes where each node acts a router and host at the same time. With evolution, new Ad-Hoc paradigms are developed for different disaster scenarios such as a Mobile Ad-Hoc Network (MANET), Vehicular Ad-Hoc Network (VANET), Delay Tolerant Network (DTN), Wireless Sensor Network (WSN), Professional/Private Mobile Radio (PMR) and Wireless Mesh Network (WMN) [8].

Over a disaster region, MANETs can be formed by using two main wireless technologies, namely, Wi-Fi and Bluetooth. Every smartphone and laptop acts as a node for the MANET and the node mobility is considered to be low. To implement MANET, Network Auto-configuration Software (NAS) and all the proactive and reactive routing protocols must be installed in each smartphone and laptop in advance [9]. VANET and DTN are two special cases of MANET. In VANET, the node mobility is considered to be high (vehicular speed). VANET is useful in a disaster scenario such as massive traffic accidents, terrorism manifest, and landslides, etc. In [10], RescueME system is developed over VANET to store user location securely and routinely using existing infrastructure and use it during disaster rescue. DTN is useful when the density of nodes over the region is low. In that case, MANET will be malfunctioning in route discovery and route establishment. DTN can be applied for low and high mobility case. MANETs have many challenges such as prediction of accurate mobility model [8], design of multihop energy efficient routing protocol fit for different node topology, network security issue such as nasty neighbor relaying packets [11].

WSN consists of spatially distributed dedicated sensors for monitoring and recording the environmental conditions. Related to disaster, WSN can be used as early-warning systems [12], [13], detection and monitoring system [14], [15] but their use in post-disaster scenarios remains largely uninvestigated. In a post-disaster situation, it is challenging to deploy new sensors or replace the damaged sensors manually [8]. PMR systems such as TErrestrial Trunked RAdio (TETRA) and TERTRAPOL are used for public protection and disaster relief operation [16]. PMR supports both Ad-Hoc mode and the infrastructure mode of operation. It has a lack of interoperability with other open civilian wireless systems. Over a disaster region, PMR offers teleservice and data service with a low data rate.

As the world becomes more data-centric rather than voice-centric, design of Long Term Evolution (LTE) based public safety communications has also garnered attention. There exist land mobile radio systems like FirstNet, which uses LTE technology to provide emergency broadband service [17], [18]. The performance of the Unmanned Aerial Base Stations (UABSs) for public safety communication is investigated in [19]. For the post-disaster management, in [20] Unmanned Aerial Vehicle (UAV) assisted LTE network is designed by using femtocells. Following a disaster, establishing an LTE network for emergency communication is an expensive process due to the high cost of the BSs.

Use of WMN for a disaster like situations is quite popular as compared to other Ad-Hoc paradigms discussed above. Based on WMN, different commercial products are already available in market such as GoTenna [21], GoHeart [22]. It allows for sending text message and location during a disaster. The major disadvantage of these products is its high price. In a post-disaster situation, the primary goal of WMN is to form a backbone and access network by using Wi-Fi or WiMAX technology. WiMAX is considered in [23], [24] to implement broadband service and effective business continuity service during and after a disaster. Although regarding coverage, WiMAX outperforms Wi-Fi by miles, but the requirement of a particular receiver at the subscriber end limits its use for a disaster situation. With the rapid growth of smartphone users, Wi-Fi now becomes ubiquitous. There is a high probability that every survivor has a smartphone with Wi-Fi connectivity. Therefore, Wi-Fi may be considered as a primary choice for designing a cost-effective and fast deployable emergency network.

In [25], the Wi-Fi Access Points (APs) are used to set-up a local area network in a post-disaster situation. Similarly, in BRCK, a device developed by Ushahidi, the Kenyan-based company, uses Wi-Fi to exchange information during crisis and disaster events [4]. The manual deployment of APs over a region is a time-taking process and not preferable in all disaster scenarios. Use of flying objects for emergency network set-up may be a smart choice. In [26], helium-filled balloons are used to design a Wi-Fi-based mesh network named SKYMESH. Usually, emergency communication systems are powered by batteries. For the long term of operation, the tethered balloon is considered in [27]. A new type of emergency network is designed in [1], where BSs are carried by helicopters, airships and hot balloons over disaster zones. Use of helicopters and hot balloons requires a considerable budget, with an added challenge of continuous tracking of the carrier balloons.

Nowadays, the advent of the UAV gives a new dimension for emergency network design [28], [29]. A UAV, also known as drone, is a flying aircraft without a human pilot aboard. Thus, for the successful operation of UAV-assisted emergency network, mobility model is essential for navigating UAVs fleet. According to [30], mobility models are grouped into five classes: Pure Randomized Mobility Models (PRMM), Time-Dependent Mobility Models (TDMM), Path-Planned Mobility Models (PPMM), Group Mobility Models (GMM), and Topology-Control-based Mobility Models (TCMM). Among all, GMM and TCMM follow inter UAV connectivity awareness, which is essential to set-up an emergency network. Compared to GMM, in TCMM, random movement of UAVs is replaced by control mobility through sensible data exchange among UAVs. The decision of the next waypoint in this model depends on constraints like coverage area [31], connectivity [32] and residual energy [33]. In [34], all three constraints are jointly considered to decide the next movement. A more refined and appropriate fuzzy logic based approach is applied in [35] for computing the internal parameters required for the decision-making process in [34].

Design a UAV-assisted emergency Wi-Fi network will take less network restoration time and also cost-effective due to the use of Wi-Fi. There are a few experimental studies have been documented so far on UAV based network. In [36], a drone-based wireless network is created by using wireless-AC 7260 network adapter interfaced with the Intel Galileo board. The network coverage investigated for both Ad-Hoc and

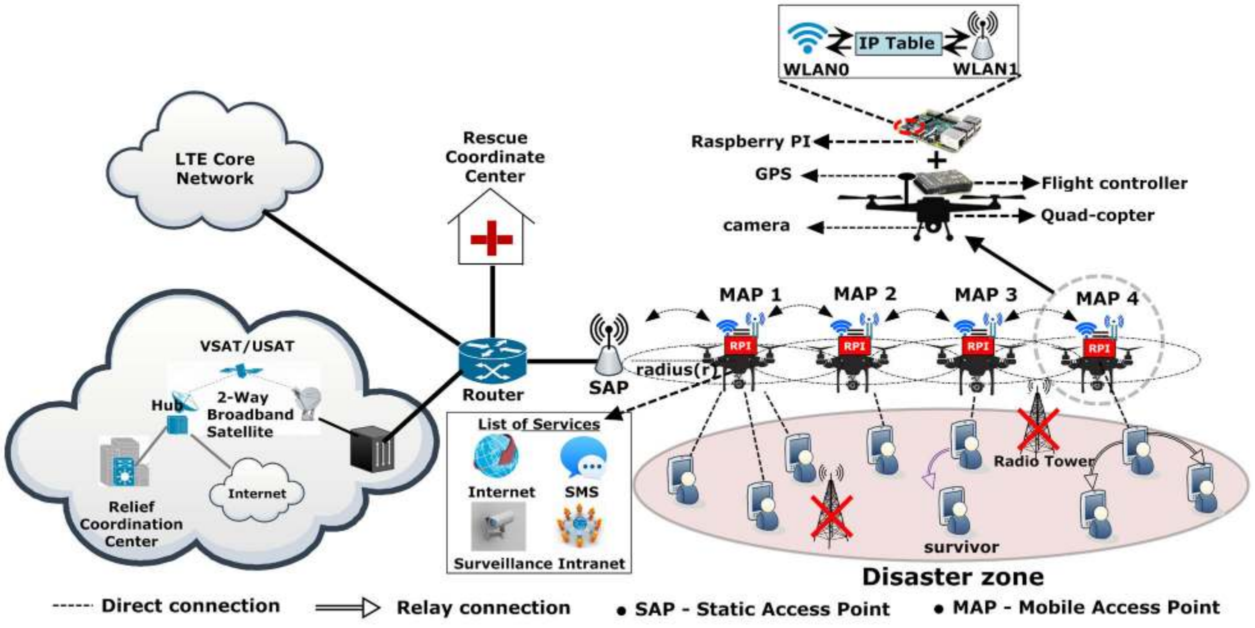


FIGURE 2. WiND network model for post-disaster management.

infrastructure mode of operation is found to be 48 meters. A drone-based WMN is developed for video surveillance over a disaster region by using expensive open-mesh OM2P and MR1750 APs in [37]. For an efficient mesh network design, Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.) advanced protocol is used. Similarly, in [38], an autonomous Micro Air Vehicles (MAVs) are designed and mounted with two wireless interfaces: Ralink 3572 Wi-Fi adapter for data transmission and XBee Pro 802.15.4 for control information transmission to set-up a MANET. Although drone-based Wi-Fi network design is already addressed in the above literature, design a cost-effective, resilient and multi-objective emergency network, that capable of on-site surveillance, accelerating SAR, helping survivors by providing essential first aid tips and rescue camp locations are yet to be addressed.

The objective of this paper is to design a cost-effective, user-friendly, and fast-deployable emergency communication network by integrating the RPI board with UAV. The proposed emergency network has the following goals:

- Design a mobility model for UAV synchronization and form a chain network over the disaster region to provide an emergency Wi-Fi service to the survivors.
- This exigency network must support on-site surveillance over the disaster region and transmit the data to the rescue center for better rescue planning.
- To make it robust, each movable Wi-Fi nodes must be configured to manage connection disruption in the chain network.
- Design an alert system to inform the survivors about the usage of the emergency network, essential first aid tips, and guide them to the nearest rescue camp.
- Due to small Wi-Fi coverage, it is compelled to extend the emergency network with the help of existing available resources (smartphones) in that disaster region.

The rest of the paper is organized as follows. Section II describes the system architecture of UAV assisted emergency Wi-Fi network and its strategy. The list of problems faced during prototype design and their solutions will be focused in section III. Section IV highlights all the results obtained from the field experimental set-ups. Finally, the conclusion about the paper is drawn in section V.

II. SYSTEM ARCHITECTURE

Emergency response immediately after a disaster plays a vital role in post-disaster risk reduction. There is no doubt that the Flying Ad-Hoc Network (FANET) has the potential to set-up a quick emergency network as compared to other options discussed earlier. Design UAV-based Wi-Fi network will be a cost-effective solution due to the high chance of smartphone availability. Compared to custom-made relief equipment, there are no prerequisites for the Wi-Fi network, and it is easy to configure. Thus Wi-Fi is the primary technology considered here for designing an emergency network known as Wi-Fi Network on Drone (WiND).

A. DESIGN OF WiND

Fig. 2 illustrates the network model of WiND, specially designed for the post-disaster scenario. This emergency network is formed by a swarm of drones communicating with each other over Wi-Fi and create a network chain between the Rescue Coordinate Center (RCC) and the survivors. It supports internet, intranet, Short Message Service (SMS), and on-site surveillance. It assists the survivors by providing necessary information such as nearest rescue camp locations, basic first aid tips and collects valuable information like the number of survivors, their condition, and landmark information. It helps the relief team to locate the victims and also the survivors by alerting them from future danger.

In WiND, each UAV has a payload capacity of 1 kg equipped with a Global Positioning System (GPS) transceiver and a flight controller board. According to Fig. 2, every Mobile Access Point (MAP) in WiND has to provide Wi-Fi service to the survivors and simultaneously connect to an AP of its predecessor to form network chain. Therefore, each drone must have two wireless interfaces. One interface provides a hotspot service over the region, and another will be used as a Wi-Fi client, for establishing a communication link with its immediate predecessor for inter-drone communication.

To enable the aforementioned feature, Raspberry PI (RPI) 3 Model B+ development board (mounted on each drone) is considered. Although there are many alternatives of RPI with better hardware configurations are available in the market such as ASUS Tinker Board, LattePanda 4G/64GB, ODROID-XU4, and Qualcomm Dragon board, RPI is found to be least costly among all. Other features of RPI that convince to select this board are its built-in 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac Wireless LAN, IOT Wi-Fi feature for the simultaneous station and AP mode of operation, a camera interface for surveillance, USB interface for data transfer, open-source operating system, run on power banks and lightweight [39], [40]. The RPI development board also supports an external Wi-Fi dongle and mini-PCI Wi-Fi card to improve Wi-Fi performance. But, it is not preferred as it increases the power consumption as well as the cost. Thus, over a single interface, two wireless interfaces, WLAN0 and WLAN1, are created in RPI. There are dedicated routers available in the market with OpenWRT and DD-WRT firmware, which simplify the mesh network design and management. But, for an emergency network with multi-objectives like network chain formation, surveillance, and control UAV navigation, single RPI board is enough.

Out of the two interfaces, WLAN1 is configured as an AP, which requires a static IP, IP pool for the clients, Service Set IDentifier (SSID) name, and a fixed channel number. Among the different IP classes, Class A is preferable due to its large IP address range. WLAN0 follows the default Wi-Fi client configuration. An IP table is defined between WLAN1 and WLAN0 to forward IP packets. Although the security of UAV network from lethal cyber-attacks [41] is important, for ease of access by the survivors over the disaster region, the designed AP follows open authentication. Besides setting up a chain network, RPI helps in surveillance, data management, and does all the real-time processing. It acts as a brain of each MAP and passes information such as location coordinates and altitude to Pixhawk (flight controller board) over serial communication port.

In the case of WiND, instead of feeding information to all drones, one drone named as master is the point of contact for mission planning. Whenever a disaster occurs, according to the rescue plan a list of longitudes, latitudes, and altitudes first need to be shared to the RPI mounted on the master drone over a designed Graphical User Interface (GUI). The distance between the two consecutive coordinates is the maximum hop distance, which equals to the radius (r) of Wi-Fi coverage. The master drone responsibility is to share all necessary initial information with other drones in the following manner: master's predecessor act as a master for its immediate predecessor. Initially, during network set-up, only the master drone has all the coordinates. It will share all coordinates except the last one to its immediate predecessor drone. Similarly, the immediate predecessor passes the coordinates except for the last one to its predecessor. For UAVs navigation, a modified version Pursue Mobility Model (PMM) [30], a sub-class of GMM with collision avoidance and network connectivity constraint is considered. All the drones maintain a fixed altitude during chain formation, and after that, they may change their height according to the requirement of the user throughput.

Post-disaster inspection has a significant impact on rescue planning. The WiND is also capable of doing surveillance over the region with the help of a camera module embedded in RPI. The surveillance can be done in two ways depending on the decision of SAR advisory group. One way is to perform only surveillance, collect necessary information, come back to the base station, and deliver the information to RCC. In this case, master UAV requires four coordinates as input, which are the endpoints of maximum length and breadth of the disaster-hit region. Once the coordinates are shared, RPI of the master UAV assigns a list of coordinates, which includes initial location, all intermediate hops and the final location to the other UAVs. The breadth of the region will decide the gap between two UAVs during surveillance. UAV swarms will form a line to cover the maximum area for surveillance and fly over the region. Each RPI will do a continuous video recording.

Another method for surveillance starts only after setting up a network chain. Once each UAV reaches to its last coordinate of the list, it starts doing surveillance. Over the network chain, the newly generated surveillance file needs to be sent to RCC server through multi-hop communication. In WiND to avoid network congestion, the surveillance is restricted to capture images only. Every RPI captures snapshots at a regular time interval and saves it in a specific folder inside the memory. The newly generated surveillance files are transferred to the server only after a certain time interval. It is preferable to keep the time interval for capturing an image and transmitting it to the server to be almost of the same duration, so that the excess transmission load due to large transmission interval or low spectral efficiency due to small transmission interval is avoided. In section III and IV, surveillance method will be discussed more in details.

III. DESIGN CHALLENGES AND SOLUTIONS

This section is mainly focused on the critical design challenges faced during WiND design and the proposed solutions. During chain formation over the disaster region, synchronization among UAVs is imperative. Each MAP continuously monitors its predecessor and takes necessary action before connection disruption. As UAVs with high mobility carry the APs, there is a high chance of miss-communication and the network chain will break. Therefore, each MAP should be intelligent enough to handle this situation. Even though an emergency network is created over the region, there is a difficulty to alert the survivors about the network and communicate with them without prerequisite training. Therefore, the designed interface must be easy to use and interactive. The WiND is based on Wi-Fi network of small coverage. It is required to extend the coverage with the help of existing resources in the disaster region is a challenging situation. During surveillance and data transmission, each RPI must be programmed to handle essential data management, unnecessary data re-transmission, and avoid network congestion.

A. SYNCHRONIZATION DURING NETWORK CHAIN FORMATION

Once a disaster happens, the first job is to share a list of coordinates (waypoints) to master UAV over a GUI platform. The master UAV will share the coordinates to its predecessor, wait for a certain delay and then start flying to its first target location. Under PMM, the predecessor UAV continuously following the trajectory of its master UAV. During hopping from one coordinate to the next, there must be synchronization between the master and its predecessor to avoid the collision and any communication disruption due to the high inter-UAV gap.

List of coordinates provided by the commander of RCC to master UAV are GPS based navigation, which follows the geodetic coordinate system [42]. During network chain formation, every UAV must maintain a fixed gap with its master to avoid collision. Therefore, the North-East-Down (NED) coordinate system is used between the master and its immediate predecessor (slave). NED comes under the cartesian coordinate system. Under NED the slave, instead of moving to a particular point, follows the master with a velocity component in its North, East and Down axis, where the magnitude is directly proportional to the amount of separation between its present location and its target location. This leads to a smooth as well as an efficient movement of the slaves and less chance for Wi-Fi connection disruption.

During network chain set-up, the vehicle mode follows by the master is 'AUTO' mode, whereas the slave follows 'GUIDED' mode. RPI of the master initially reads the waypoints and assigns to Pixhack over the Mavlink protocol [43] one after another. In between, the RPI also fetches NED (north - N_m, east - E_m, down - D_m) coordinates from the Pixhack, update it on a text file named 'LOC' and share it with the slave over a regular interval (δ_1). The value of δ_1 should be decided wisely. If it is high, then it may happen master will move out of the network coverage, if very low then unnecessary it increases the network load. RPI of slave reads this text file over a regular interval (δ_2) and finds its relative distance with respect to north (R_N), east (R_E), and down (R_D) between new target location and its own NED coordinates (N_s, E_s, D_s). To avoid errors in sensors precision while measuring NED coordinates, there must be an error threshold (N_{th}, E_{th}, D_{th}) to accept up to a specific error value. Algorithm 1 represents the steps followed by the slave in every δ_2 period. In step 4, step 5, and step 6 the RPI of slave assigns a velocity component for north (V_N), east (V_E), and down (V_D) respectively concerning the relative distance and ideal UAV speed (S). If the difference is more, then velocity will be more in that particular direction. Due to any reason, if the Wi-Fi connection breaks, then the slave will hold its position until there is an update in LOC.

Algorithm 1 Algorithm for Slave Navigation Under GUIDED Mode

```
   Result: Reached target location
   Input  : LOC
   Output: $V_N$ =0, $V_E$ =0, $V_D$ =0
1  initialization: $V_N$ =0, $V_E$ =0, $V_D$ =0, $R_N = N_m$ - $N_s$,
     $R_E = E_m$ - $E_s$, $R_D = D_m$ - $D_s$ ;
2  while $R_N \neq 0$ or $R_E \neq 0$ or $R_D \neq 0$ do
3      if $R_N \geq N_{th}$ and $R_E \geq E_{th}$ and $R_D \geq D_{th}$ then
4          $V_N = R_N$*S;
5          $V_E = R_E$*S;
6          $V_D = R_D$*S;
7      else
8          $V_N = 0$;
9          $V_E = 0$;
10         $V_D = 0$;
11     end
12 end
```

B. INTELLIGENT MAP DESIGN FOR AUTO RE-CONNECTION WITH WI-FI ACCESS POINT

Use of the NED coordinate system during chain formation helps each MAP to maintain the received signal strength of its immediate predecessor AP above a threshold value. If unfortunately the connection breaks, then the master will stop and hold its position for a fixed amount of time. In between, Wi-Fi of master starts scanning the available Beacon frames and checks the SSID of its immediate predecessor MAP AP. If SSID is found then hold the position, else change its altitude to avoid any collision and moves slowly backward direction till finding slave's SSID. Even after chain formation, there may be a chance of connection break due to any malfunctioning of RPI. It may happen that the MAP is completely damaged. Therefore, each MAP must be intelligent enough to handle this situation and re-establish the connection.

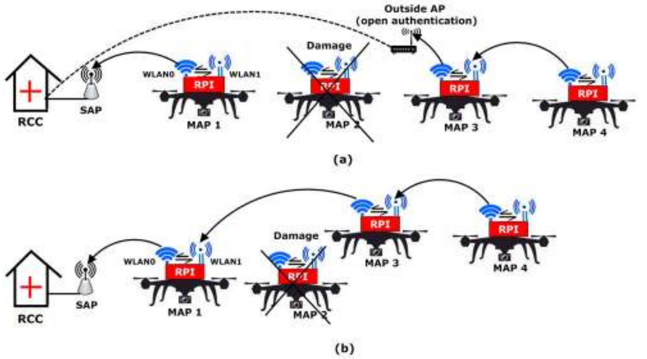


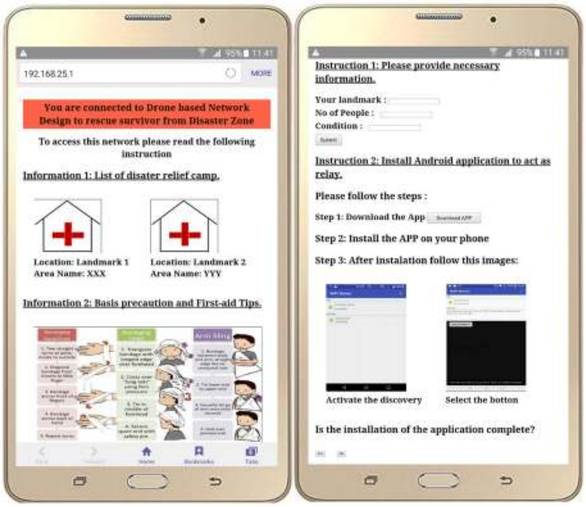
FIGURE 3. Possible situations during auto re-connection of WLAN0.
(a) Connection re-established with RCC through outside AP,
(b) Connection re-established after the damage of MAP2 (previously registered AP).

Algorithm 2 Algorithm for Auto Re-Connection of WLAN0

```
   Result: Network chain re-established
   Input  : L,N,S,P
   Output: P=1
1  initialization: i=1;
2  while $P==0$ and $i \leq N$ do
3      if $p==0$ and $L(i)==S$ then
4          wait $\delta_t$;
5          ping X;
6      else
7          if $P==0$ then
8              $W^*_{sup}$ = L(i);
9              $W_{sup} \leftarrow W^*_{sup}$;
10             wait $\delta_t$;
11             ping X;
12             i=i+1;
13         end
14     end
15 end
```

In RPI, for Wi-Fi (WLAN0), there exists a configuration file named wpa_supplicant, where the lists of all accepted networks and security policies, including pre-shared keys, are stored. Once the connection breaks, WLAN0 will able to re-connect to the previously allowed network. For a dynamic scenario in WiND, it is not suitable to simply rely on default configuration file as it may happen previously registered APs can be damaged, or a new AP is available through which a better connection is possible. In Fig. 3, the possible situations during auto-reconnection of WLAN0 are shown. Over the disaster region, apart from the WiND's APs, there may exist external APs with open authentication.

Algorithm 2 is designed for auto re-connection of WLAN0 after scanning the Beacon. Let 'L' is the list prepared after scanning the Beacon frames, in which previous network SSID 'S' is in the first place if available and others will be arranged in descending order according to the Receive Signal Strength Indicator (RSSI). N is the total number of SSIDs available on the list. WLAN0 picks SSID from the list one by one and tries to connect. It requires δ_t time to set-up a connection. Once WLAN0 connects to the SSID, it will ping the IP address of the RCC server 'X' to check whether the selected SSID is right or wrong. Let P is the outcomes from ping operation, W_{sup} is the old Wi-Fi configuration file, and W^*_{sup} is the update configuration file. In step 9, the W_{sup} is replaced by W^*_{sup} if S is not available in L. If through the selected SSID the RCC server is unable to ping (P=0) then from step 8 to step 12 will be executed again. Each RPI has the information of IP address of each hotspots of WiND and the IP of RCC server.


192.168.25.1

You are connected to Drone based Network Design to rescue survivor from Disaster Zone

To access this network please read the following instruction

Information 1: List of disater relief camp.

Location: Landmark 1
Area Name: XXX

Location: Landmark 2
Area Name: YYY

Information 2: Basis precaution and First-aid Tips.

Instruction 1: Please provide necessary information.

Your landmark :
No of People :
Condition :

Instruction 2: Install Android application to act as relay.

Please follow the steps :

Step 1: Download the App

Step 2: Install the APP on your phone

Step 3: After instalation follow this images:

Activate the discovery

Select the botton

Is the installation of the application complete?

FIGURE 4. Screenshot of the designed captive portal to guide survivors in post-disaster situation.

C. WiND AS A HELPING HAND FOR DISASTER RELIEF

After the disaster, convey necessary information to the survivors is a challenging task. Even after setting up an emergency network over the disaster region, the survivors are unaware of the way to use the emergency network. Therefore, once a survivor connects to the Wi-Fi network, it is required to guide the user either through notification or by a welcome screen. It is also required to convey some basic instruction regarding the usage of the network. In the WiND, with the help of a captive portal, the Wi-Fi users are notified and guided about the usage of the emergency network. In each RPI mounted on the drone, a web server is created, and through the captive portal, a web page is hosted. The captive portal will continually greet the user until the required action is completed.

A screenshot of the designed captive portal is shown in Fig. 4. Through the portal, necessary information is conveyed to the survivors like the nearest rescue camp locations, basic first-aid tips, instruction to download Android application and how to use it to convert the smartphone to act as relay. Through the web page (captive portal), information such as the number of survivors, their landmark and health condition are also collected and saved in a text file in RPI. There is a provision in the web page to allow the survivor to access a specific website to get more necessary information. The web page is hosted locally from each RPI rather than a central location to avoid unnecessary network load. If the commander of RCC wants to update some information of the web page at on-site, then over the multi-hop communication, through a suitable command old web page file will be replaced by a newly designed web page.

D. EXTEND WiND COVERAGE USING EXISTING RESOURCES

A Wi-Fi network usually has small network coverage. For large scale disaster, the most challenging situation for WiND is to provide full network coverage over the disaster-hit region. One possible solution is to deploy large scale of UAVs over the entire area. But it is not preferable due to the high capital requirement, and it degrades network performance parameters such as decreased throughput, increased network delay. The network will be more complex and will have low resilience. Thus an alternate solution is required. In the case of WiND, each smartphone connects with the Wi-Fi network acts as a relay for its neighbor located out of the coverage area with the help of a NAS [44].

NAS is designed by using Wi-Fi direct concept to provide both hotspot and Wi-Fi service. Wi-Fi direct uses a Software AP (Soft AP) which makes it possible for a smartphone device to act as both AP and Wi-Fi client simultaneously. There exist a peer to peer (p2p) connection with another device over AP and at the same time the device continues to maintain the uplink connection over Wi-Fi. In [45], Wi-Fi direct is used to disseminate alerts over the Wi-Fi network in a disaster region. Similarly, in [46] to set-up a Device to Device (D2D) communication over a disaster region, an application is designed based on Wi-Fi direct. For configuring a smartphone to act as a relay, an Android-based application is developed based on Wi-Fi direct. After enabling the application, Wi-Fi direct peer to peer manager gets enable. It registers a broadcast receiver for Wi-Fi direct, listens to Wi-Fi direct events, and displays available peers. In Fig. 4, the screenshots of the designed application is shown. The application is hosted from the local web server created in RPI and a download button with all instructions related to its usage are mentioned in the captive portal. The reasons to host the application from each RPI, instead of a central server is to avoid any unnecessary network load on the network chain.

E. SURVEILLANCE BY WiND

During surveillance, there is a requirement of proper data management to store surveillance data, retrieve it during transmission, and avoid overwriting of data. In the WiND, for different types of surveillance data (video, image, text), a specific folder is created in each RPI. Once a surveillance file is generated, with the default name, the current date, and an index number is appended. The date will help in identifying the day of surveillance, and the index number will avoid overwriting of files and also keep track of the number of data generated. Here the index number is picked from a saved text file filled with numbers serially. Use of external text file instead of using inbuilt counter of RPI helps to avoid any chance of overwriting due to reset of the counter for malfunctioning of RPI or any other reason.

Algorithm 3 Algorithm to Append Date and Index Number to the Default Name of Newly Generated Surveillance File

```
   Result: Successfully index and date are appended
   Input  : C,D,T, N
   Output: $Y^+$
 1 initialization: i=0, m=0,T=0
 2 while i==0 do
 3     if i== $\delta_C$ then
 4         generate Y
 5         i= C(1)
 6         $Y^+ \leftarrow Y + i + D$
 7         delete C(1)
 8         C(N)=i
 9         m= size(T)
10         T(m+1)=i
11         i=0;
12     else
13         i=i+1
14     end
15 end
```

Algorithm 4 Algorithm for Transmitting Surveillance Data to RCC Server

```
   Result: File transmission successful
 1 initialization i=T(1), j=0;
 2 while $i \neq 0$ do
 3     if P==1 and j== $\delta_T$ then
 4         $Y^+ = Y + i + D$;
 5         transmit $Y^+$ to X;
 6         received ACK;
 7         delete T(1);
 8         j=0;
 9     else
10         j=j+1;
11     end
12 end
```

Algorithm 3 is proposed for data management while collecting surveillance data at a regular interval of δ_C. In each RPI, there is a camera index text file named 'C', filled with numbers from 1 to N, where 'N' depends on the time interval for taking snapshots, and the total duration of surveillance. 'D' stands for the date, 'T' is the transmit index text file, which will be empty initially, and 'Y' is the default name of the generated data. In step 5, one index value will be picked

TABLE 1. List of hardware and software tools used for WiND design.

Components Name	Use	price (in INR)	Type
Pixhawk PX4 2.4.8	Flight controller	5,500	Hardware Tools
Z450 Flame Wheel	Frame	850	
DYS 30A ESC	Speed controller	2,600	
X2212 KV980 II	Motor	4,800	
UBLOX NEO7M	GPS module	1,500	
1045(10X4.5) Props	Propeller	260	
B-25C-2500-4S1P	Battery	2,700	
RPI 3 model B+	Development board	2,500	
Module V2 - 8	Camera module	1,900	
Raspbian Stretch	Operating system	-	Software Tools
pure-ftpd	FTP server creation	-	
Wput	FTP file transfer	-	
Apache server	Host web page	-	
nodogsplash	Captive portal creation	-	

from C, and Y will be appended with D and index (i) in step 6. The same index value will be stored at the bottom of C in step 8 for reuse and also saved in T (step 10) to identify the files that need to be transmitted. Generating a file during surveillance and transferring that file to its destination are two independent events. Algorithm 4 represents the steps followed by RPI while transmitting data to the RCC server at a regular interval of δ_T. RPI first check the connection status with RCC server by pinging to X. Data transmission in step 5 will happen only if T is not empty. In step 7, the respective index will be deleted from T once an acknowledgment (ACK) is received.

IV. RESULTS AND DISCUSSION

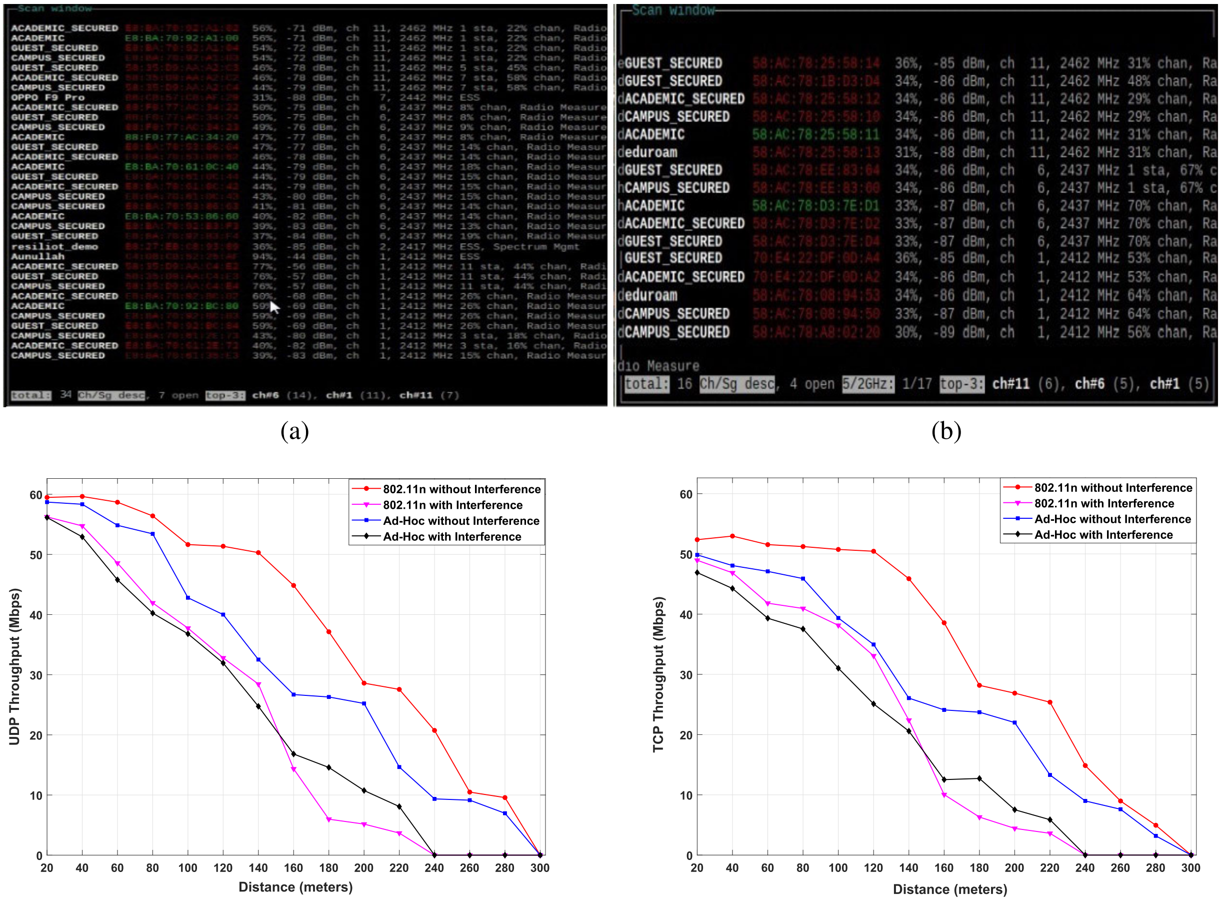
The performance of WiND is assessed with the help of a prototype model consisting of two quad-copters and three RPIs. All the hardware and software tools used for developing the prototype of WiND are listed in TABLE 1. The initial phase of WiND design starts from selecting a proper wireless technology with the best configuration to form a network chain. Therefore, several field experiments are carried out using RPIs. After the successful integration of MAP and chain network formation, through field experiments, the feasibility and reliability of WiND are verified. Three experimental set-ups prepared for addressing different issues are:

- **Experimental set-up 1-** Prepared for assessing the network performance between two nodes of WiND, especially to know the maximum hop distance.
- **Experimental set-up 2-** Prepared for surveillance testing of the designed prototype of WiND.
- **Experimental set-up 3-** Prepared for validating master-slave synchronization in WiND.

In WiND, information about internode hop distance is essential for mission planning. Experimental set-up 1 is prepared to do a comparative study on different wireless technology and configurations supported by RPI and find the maximum hop distance for them. Each RPI supports dual-band (2.4GHz and 5 GHz) and both infrastructure mode (Wi-Fi AP) and Ad-Hoc mode of operation. It also supports internet protocol like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) for data transmission. The overall performance of the chain network is generally depended on each node's network performance. Thus, two RPIs (one act as a server and other as a client) are considered to assess the network performance of WiND. Once the network chain is formed, each MAP of WiND will be in location hold mode, and the mobility will be approximately zero. Due to this reason, the field experiments for finding maximum hop distance are carried out under static condition of RPIs. At the campus playground, with the help of Iperf3, from the client to server, 10 MB of data is transferred in every 20 meters gap. Here, 10 MB of data size is considered for the experiment as the WiND will allow to transfer the less volume of data like surveillance snapshots, text file, and web page over the chain network. In the disaster region, it may happen some APs remain undamaged and causes interference to WiND. Therefore, evaluation of network performance under interference is needed for 2.4 GHz band as it is widely used as compared to the 5 GHz band.

With the above consideration, under experimental set-up 1, two case studies are done as: **Case I -** Performance of Wi-Fi AP and Ad-Hoc under 2.4 GHz band with and without interference for TCP and UDP connection, **Case II-** Performance of Wi-Fi AP and Ad-Hoc under 5 GHz band with different channel BW for TCP and UDP connection. All the field experiments in both cases are performed on built in Proant PCB antenna of RPI. For Case I, one RPI (server) is configured to IEEE 802.11n Wi-Fi AP or Ad-Hoc supporting 20 MHz channel BW, and another RPI is configured to access it. Here, 40 MHz channel BW for IEEE 802.11n is not considered as there is less chance of finding eight free contiguous channels. AP set in 40 MHz channel BW will trigger to 20 MHz once it finds any of the channels under 40 MHz is busy. In Case II, the server is configured to IEEE 802.11ac with channel BW of 20 MHz, 40 MHz, 80 MHz and Ad-Hoc with channel BW of 20 MHz only due to hardware limitation. Under 2.4 GHz band, it is essential to choose a channel for low interference as it is frequently used. As three non-overlapping channels 1, 6, and 11 are usually used, so channel 3 is preferred for both Ad-Hoc and Wi-Fi AP mode of operations. Similarly, in case II, channel 44 is used.

Fig. 5 represents the inter-node network performance for Case I. During the experiment, the outcome of Beacon scan for interference and no-interference scenarios are shown in Fig. 5 (a) and Fig. 5 (b) respectively. Scan result shows the number of existing APs, their type, channel number, and signal strength. It is found that for interference scenario, eight APs in channel 1 with high signal strength (> -70 dBm) are interfering with the server. For no-interference scenario, although there are numbers of APs are found after Wi-Fi Beacon scan, but no one is interfering as their signal strength is found to be lower than -85 dBm. Fig. 5 (c) and Fig. 5 (d) represent the throughput performance for UDP and TCP connections.



```
Scan window
ACADEMIC_SECURED E8:BA:70:92:A1:02  56%, -71 dBm, ch  11, 2462 MHz 1 sta, 22% chan, Radio
ACADEMIC         E8:BA:70:92:A1:00  56%, -71 dBm, ch  11, 2462 MHz 1 sta, 22% chan, Radio
GUEST_SECURED    E8:BA:70:92:A1:04  54%, -72 dBm, ch  11, 2462 MHz 1 sta, 22% chan, Radio
CAMPUS_SECURED   E8:BA:70:92:A1:03  54%, -72 dBm, ch  11, 2462 MHz 1 sta, 22% chan, Radio
GUEST_SECURED    58:35:D9:AA:A2:C3  46%, -78 dBm, ch  11, 2462 MHz 5 sta, 45% chan, Radio
ACADEMIC_SECURED 58:35:D9:AA:A2:C2  46%, -78 dBm, ch  11, 2462 MHz 7 sta, 58% chan, Radio
CAMPUS_SECURED   58:35:D9:AA:A2:C4  44%, -79 dBm, ch  11, 2462 MHz 7 sta, 58% chan, Radio
OPPO F9 Pro      86:C8:57:C8:AF:29  31%, -88 dBm, ch   7, 2442 MHz ESS
ACADEMIC_SECURED 88:F0:77:AC:34:22  50%, -75 dBm, ch   6, 2437 MHz 8% chan, Radio Measure
GUEST_SECURED    88:F0:77:AC:34:24  50%, -75 dBm, ch   6, 2437 MHz 8% chan, Radio Measure
CAMPUS_SECURED   88:F0:77:AC:34:23  49%, -76 dBm, ch   6, 2437 MHz 9% chan, Radio Measure
ACADEMIC         88:F0:77:AC:34:20  47%, -77 dBm, ch   6, 2437 MHz 8% chan, Radio Measure
GUEST_SECURED    E8:BA:70:53:86:64  47%, -77 dBm, ch   6, 2437 MHz 14% chan, Radio Measur
ACADEMIC_SECURED E8:BA:70:53:86:62  46%, -78 dBm, ch   6, 2437 MHz 14% chan, Radio Measur
ACADEMIC         E8:BA:70:61:0C:40  44%, -79 dBm, ch   6, 2437 MHz 18% chan, Radio Measur
GUEST_SECURED    E8:BA:70:61:0C:44  44%, -79 dBm, ch   6, 2437 MHz 15% chan, Radio Measur
ACADEMIC_SECURED E8:BA:70:61:0C:42  44%, -79 dBm, ch   6, 2437 MHz 15% chan, Radio Measur
CAMPUS_SECURED   E8:BA:70:61:0C:43  43%, -80 dBm, ch   6, 2437 MHz 15% chan, Radio Measur
CAMPUS_SECURED   E8:BA:70:53:86:63  41%, -81 dBm, ch   6, 2437 MHz 14% chan, Radio Measur
ACADEMIC         E8:BA:70:53:86:60  40%, -82 dBm, ch   6, 2437 MHz 14% chan, Radio Measur
CAMPUS_SECURED   E8:BA:70:92:B3:F3  39%, -83 dBm, ch   6, 2437 MHz 13% chan, Radio Measur
GUEST_SECURED    E8:BA:70:92:B3:F4  37%, -84 dBm, ch   6, 2437 MHz 19% chan, Radio Measur
resiliot_demo    88:27:E8:C8:93:89  36%, -85 dBm, ch   2, 2417 MHz ESS, Spectrum Mgmt
Aunullah         C4:0B:CB:52:25:4F  94%, -44 dBm, ch   1, 2412 MHz ESS
ACADEMIC_SECURED 58:35:D9:AA:C4:E2  77%, -56 dBm, ch   1, 2412 MHz 11 sta, 44% chan, Radi
GUEST_SECURED    58:35:D9:AA:C4:E3  76%, -57 dBm, ch   1, 2412 MHz 11 sta, 44% chan, Radi
CAMPUS_SECURED   58:35:D9:AA:C4:E4  76%, -57 dBm, ch   1, 2412 MHz 11 sta, 44% chan, Radi
ACADEMIC_SECURED E8:BA:70:92:BC:82  60%, -68 dBm, ch   1, 2412 MHz 26% chan, Radio Measur
ACADEMIC         E8:BA:70:92:BC:80  59%, -69 dBm, ch   1, 2412 MHz 26% chan, Radio Measur
CAMPUS_SECURED   E8:BA:70:92:BC:83  59%, -69 dBm, ch   1, 2412 MHz 26% chan, Radio Measur
GUEST_SECURED    E8:BA:70:92:BC:84  59%, -69 dBm, ch   1, 2412 MHz 26% chan, Radio Measur
CAMPUS_SECURED   E8:BA:70:61:2E:73  43%, -80 dBm, ch   1, 2412 MHz 3 sta, 18% chan, Radio
ACADEMIC_SECURED E8:BA:70:61:2E:72  40%, -82 dBm, ch   1, 2412 MHz 3 sta, 16% chan, Radio
CAMPUS_SECURED   E8:BA:70:61:35:E3  39%, -83 dBm, ch   1, 2412 MHz 15% chan, Radio Measur

total: 34 Ch/Sg desc, 7 open top-3: ch#6 (14), ch#1 (11), ch#11 (7)
```

(a)

```
Scan window

eGUEST_SECURED    58:AC:78:25:58:14 36%, -85 dBm, ch  11, 2462 MHz 31% chan, Ra
dGUEST_SECURED    58:AC:78:1B:D3:D4 34%, -86 dBm, ch  11, 2462 MHz 48% chan, Ra
dACADEMIC_SECURED 58:AC:78:25:58:12 34%, -86 dBm, ch  11, 2462 MHz 29% chan, Ra
dCAMPUS_SECURED   58:AC:78:25:58:10 34%, -86 dBm, ch  11, 2462 MHz 29% chan, Ra
dACADEMIC         58:AC:78:25:58:11 34%, -86 dBm, ch  11, 2462 MHz 31% chan, Ra
deduroam          58:AC:78:25:58:13 31%, -88 dBm, ch  11, 2462 MHz 31% chan, Ra
dGUEST_SECURED    58:AC:78:EE:83:64 34%, -86 dBm, ch   6, 2437 MHz 1 sta, 67% c
hCAMPUS_SECURED   58:AC:78:EE:83:60 34%, -86 dBm, ch   6, 2437 MHz 1 sta, 67% c
hACADEMIC         58:AC:78:D3:7E:D1 33%, -87 dBm, ch   6, 2437 MHz 70% chan, Ra
dACADEMIC_SECURED 58:AC:78:D3:7E:D2 33%, -87 dBm, ch   6, 2437 MHz 70% chan, Ra
dGUEST_SECURED    58:AC:78:D3:7E:D4 33%, -87 dBm, ch   6, 2437 MHz 70% chan, Ra
|GUEST_SECURED    70:E4:22:DF:0D:A4 36%, -85 dBm, ch   1, 2412 MHz 53% chan, Ra
dACADEMIC_SECURED 70:E4:22:DF:0D:A2 34%, -86 dBm, ch   1, 2412 MHz 53% chan, Ra
deduroam          58:AC:78:08:94:53 34%, -86 dBm, ch   1, 2412 MHz 64% chan, Ra
dCAMPUS_SECURED   58:AC:78:08:94:50 33%, -87 dBm, ch   1, 2412 MHz 64% chan, Ra
dCAMPUS_SECURED   58:AC:78:A8:02:20 30%, -89 dBm, ch   1, 2412 MHz 56% chan, Ra

dio Measure
total: 16 Ch/Sg desc, 4 open 5/2GHz: 1/17 top-3: ch#11 (6), ch#6 (5), ch#1 (5)
```

(b)

(c)

(d)

FIGURE 5. Network performance of WiND for 2.4 GHz band under Wi-Fi AP and Ad-Hoc mode of operations with and without interference. (a) Beacon scan result for interference scenario, (b) Beacon scan result for no-interference scenario, (c) Throughput achieved for UDP connection between two RPIs, (d) Throughput achieved for TCP connection between two RPIs.

It is obtained from the results, irrespective of scenarios UDP performs better than TCP due to nonexistent ACK, which permits a continuous packet stream. But for higher distance (> 250 meters for no-interference and > 180 meters for interference) UDP packet loss is increasing. Therefore, it is recommended to choose TCP connection for successful transmission under low RSSI. While comparing Wi-Fi AP with Ad-Hoc, Wi-Fi AP achieves higher throughput compared to Ad-Hoc for the same channel BW except for interference scenario. It is observed under interference, the network performance in terms of throughput and coverage degrades. The maximum hop distance limits to 220 meters for interference, whereas for no-interference it is found to be 280 meters. Although with interference, Ad-Hoc performs better for higher distance (> 150 meters), but Wi-Fi AP will be preferred due to the ease of operation. A survivor can easily connect to a Wi-Fi network with no prerequisite requirement.

Fig. 6 represents the inter-node network performance for Case II. Similar to Case I, in Case II for 20 MHz channel BW, Wi-Fi AP mode performs better than Ad-Hoc. While comparing throughput performance for different channel BW of IEEE 802.11ac, it is found that for 80 MHz the throughput is quite high as compared to 20 MHz and very close to 40 MHz. Although it is expected a high throughput difference between 80 MHz and 40 MHz as similar to the result obtained for 40 MHz and 20 MHz, but the maximum throughput limitation of Proant PCB antenna of RPI limits the performance for 80 MHz channel BW. By comparing Case I and Case II, it is observed the coverage range for IEEE 802.11ac is 10 meters higher than IEEE 802.11n. It happens due to transmit beamforming supported by RPI, explicit for IEEE 802.11ac [47]. The maximum hop distance between two nodes for Case II is found to be 290 meters.

Apart from the network parameters measurement, the current consumption for different configuration is also measured. It is found that RPI, as a client with no transmission, draws a current of 480 mA. During transmission under Wi-Fi AP and Ad-Hoc mode, RPI draws a current of 780 mA and 600 mA respectively. For different channel BW and frequency band, there is no change in current consumption. For WiND, the extra power consumption of Wi-Fi AP mode

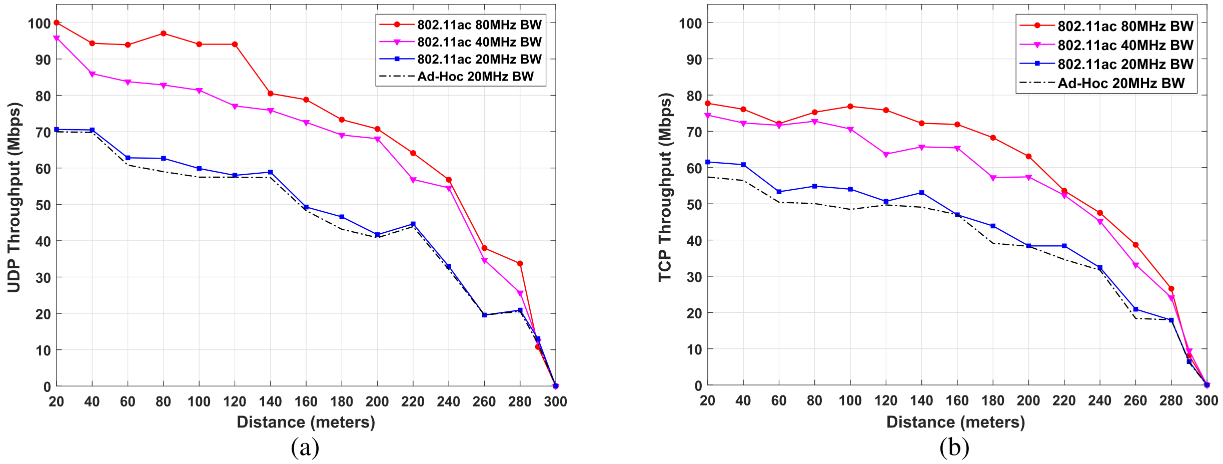


FIGURE 6. **Network performance of WiND for 5 GHz band under Wi-Fi AP and Ad-Hoc mode of operations. (a) Throughput achieved for UDP connection between two RPIs for different channel BW and mode of operation, (b) Throughput achieved for TCP connection between two RPIs for different channel BW and mode of operation.**

is not an issue as RPI can be powered by a power bank of high mAh value.

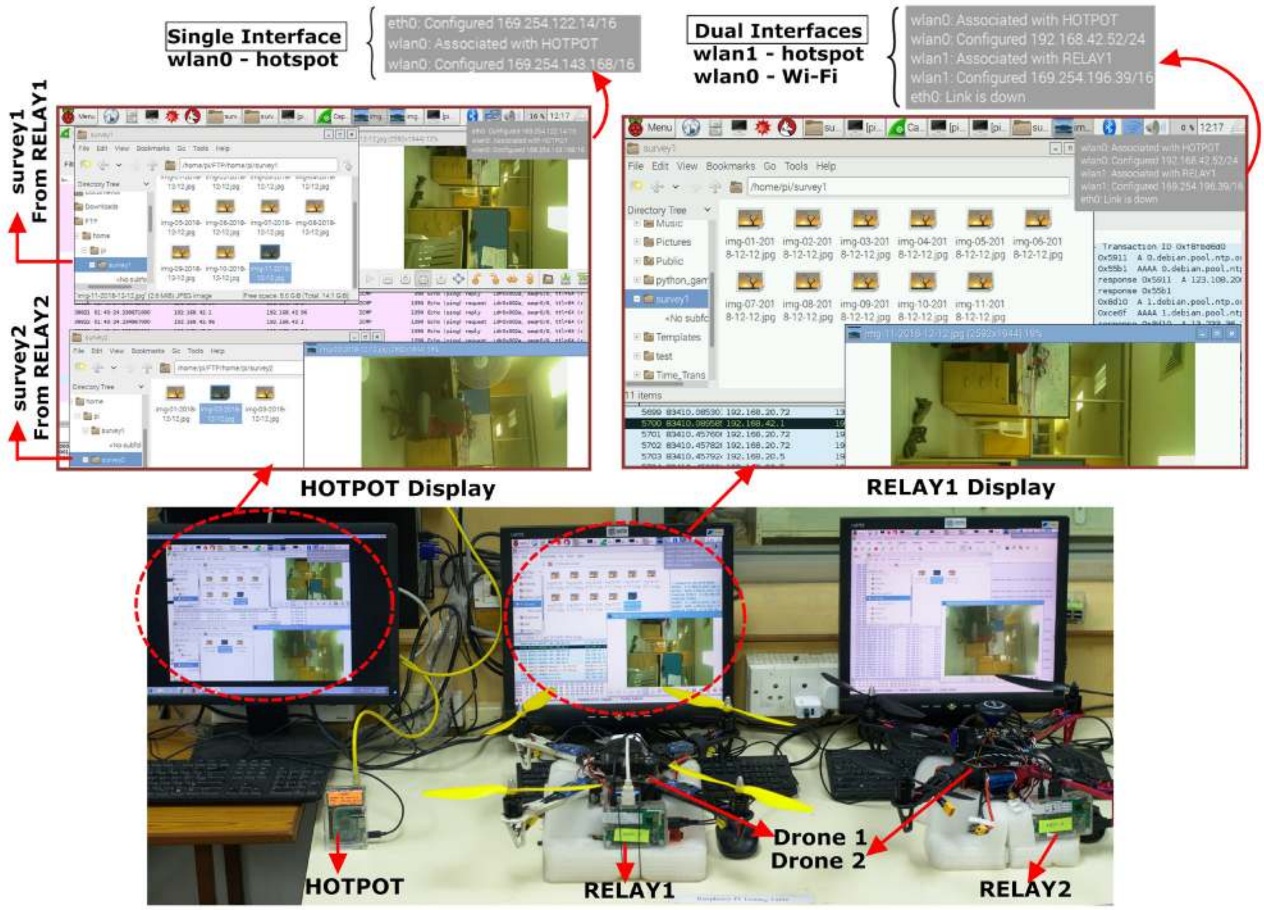
In the case of WiND, for the communication between MAP and survivor, only 2.4 GHz band is preferable as most of the smartphone supports up to IEEE 802.11n. Whereas, for the chain network, only for high throughput requirement, the 5GHz band is recommended. Between Wi-Fi AP and Ad-Hoc, Wi-Fi AP mode is preferable for WiND design irrespective of the frequency band. It is due to its high throughput performance and ease of operation. For IEEE 802.11ac, 40 MHz channel BW is recommended as the achieved throughput is close to 80 MHz, and it will reduce the effect of interference due to less channel BW. For WiND design, both UDP and TCP connection are justified. Based on RSSI (highly related to distance), the decision will be taken to select either UDP or TCP connection. Similarly, after scanning the Beacon, based on the number of existing APs in 2.4 GHz band, UAV height from the ground will be decided.

Experimental set-up 2 depicted in Fig. 7 is prepared for surveillance testing of WiND. It contains three nodes, namely, HOTPOT, RELAY1, and RELAY2. The RELAY1 and RELAY2 are connected to the display unit through High Definition Multimedia Interface (HDMI) port. The HOTPOT is connected with the help of Virtual Network Computing (VNC) via Local Access Network (LAN) port to the display unit. Here HOTPOT is working as RCC server for storing all the on-site information. It has a single wireless interface WLAN0, and it works as a hotspot with SSID name HOTPOT. In RELAY1, there are two wireless interfaces: WLAN0 is used as Wi-Fi client and WLAN1 is used as a hotspot with SSID name RELAY1. A similar configuration is mimicked for RELAY2. Finally, a network chain is formed RELAY2 to HOTPOT – by connecting WLAN0 of RELAY2 → WLAN1 of RELAY1 and WLAN0 of RELAY1 → WLAN0 of HOTPOT.

For surveillance, one survey folder is created in each RPI to store the surveillance images. For example, in RELAY1 survey1, and in RELAY2 survey2 folders are created initially. The reason to create a folder with the same name with the respective index number is to identify easily at RCC server after transmitting. The snapshots are stored inside the survey folder with a common name 'img.jpg'. Then an index number and date are appended with the earlier title. Once the ping for HOTPOT is successful, the newly generated snapshots are transferred to the file server of RCC at a regular interval from RELAY1 and RELAY2. Network auto-connection capability is also tested with the same test bed. The required time δ_t to set-up a connection is different based on the situations. If the WLAN0 wants to re-connect the previous SSID, then around 26 milliseconds is required. While connecting to a new SSID after the failure of the previous SSID, around 5.84 seconds is required.

Experimental set-up 3 is performed to validate the algorithm designed for the master-slave synchronization during network chain formation. Fig. 8 represents the results obtained from the field experiment for master-slave synchronization. Initially, the master RPI is assigned geodetic coordinates according to the mission planning. For the ease of operation, a GUI platform is developed as shown in Fig. 8 (a) to feed the coordinates. The GUI has the following arguments:

- **Vehicle Address -** The port address of the RPI to which the telemetry port of the Pixhawk flight controller is connected.
- **Baudrate -** Transfer speed (bits/sec) with which the communication will be established.
- **WayPoints -** The number of geological location points to which the UAV has to maneuver.
- **Latitude -** Latitude of the geological location in degrees.
- **Longitude -** Longitude of the geological location in degrees.
- **Altitude -** Height from the ground in meters.



```
eth0: Configured 169.254.122.14/16
wlan0: Associated with HOTPOT
wlan0: Configured 169.254.143.168/16
```

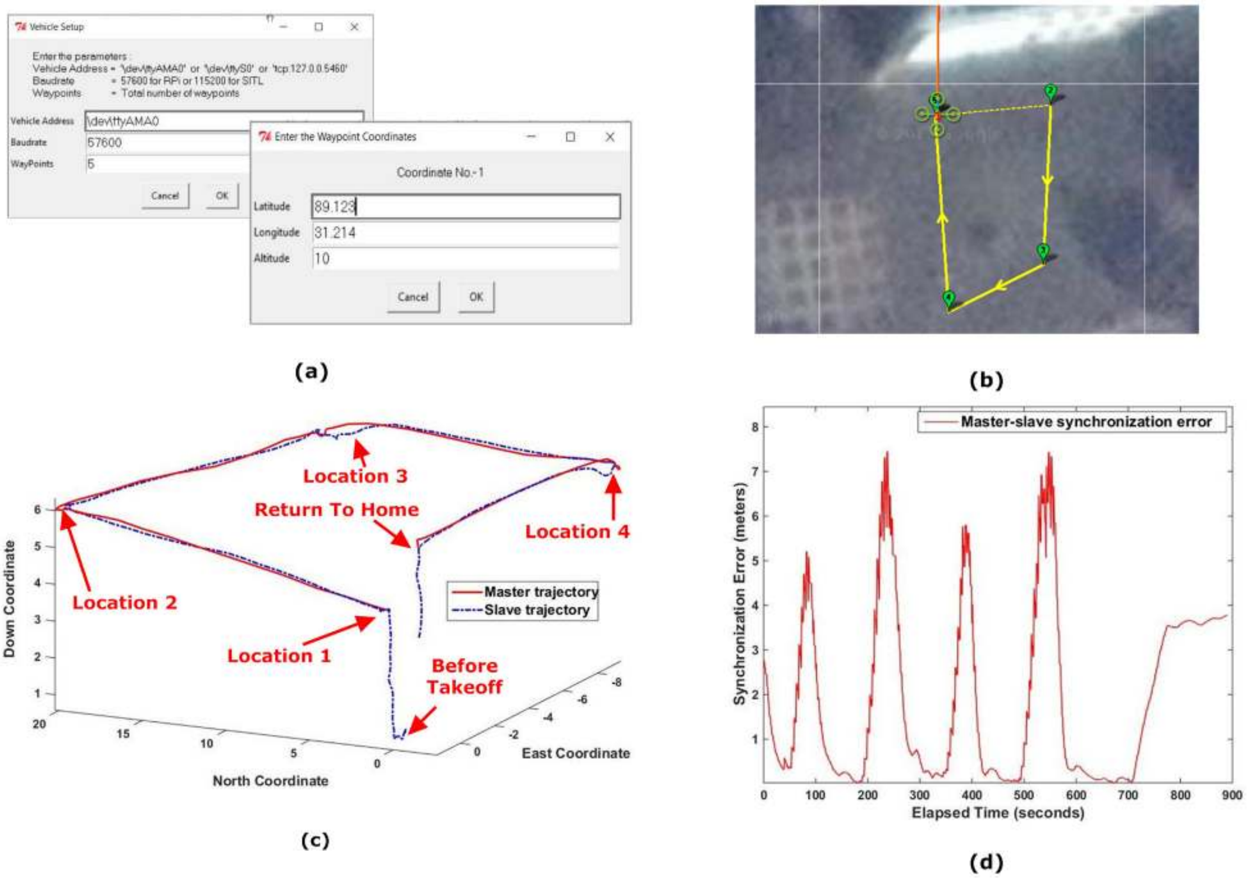
```
wlan0: Associated with HOTPOT
wlan0: Configured 192.168.42.52/24
wlan1: Associated with RELAY1
wlan1: Configured 169.254.196.39/16
eth0: Link is down
```

FIGURE 7. Experimental set-up of WiND for surveillance testing. In the figure, the two wireless interfaces, wlan0 and wlan1 are addressed as WLAN0 and WLAN1 respectively throughout the paper.

The RPI of the master will act as a brain of the quad-copter and control the Pixhack. Once the arguments are passed, a Python script will run on the RPI of the master and establish a communication link with the Pixhack to configure its mission according to the input coordinates. In Fig. 8 (b), the mission planned by master UAV is shown. RPI gives the command to Pixhack to takeoff and executes the flight mission. Throughout the mission, the RPI also keeps monitoring the UAV position and its separation from the target location. To maintain synchronization with RPI of the slave, in every 1 second interval, the master shares its NED coordinates over a text file with the slave RPI.

The RPI of slave accesses the shared text file in every 1.5 seconds intervals and then calculates its relative distance concerning the new target location mentioned in the text file. In the experiment, the ideal speed of the slave is set at 0.5 meters per second. All the NED coordinates shared by master and slave's own NED coordinates are saved in slave to know the actual trajectory of both during field testing. Fig. 8 (c), shows the trajectory of master and slave during field testing. While master UAV takes-off, the slave will discard all NED coordinates unless the master reaches a distance higher than the threshold value. Thus at the initial point of time, only the slave path is found in the trajectory plot. Simliarly, when master is arrived at return to home location, it stops sharing its location. By comparing the slave and master trajectory, it is found that the slave has a smooth path and good synchronization with the master.

To support the above statement, synchronization error in terms of Euclidean distance between NED coordinates are plotted in Fig. 8 (d). It is found that the maximum error between a slave and master is approximately 7 meters. Once the error increases, proportionally the drone relative speed increases, and a sharp fall in the error graph is noticed. At five location the error is tending to zero as master holds its position at each location for a few seconds. Slave is able to maintain zero synchronization error during that time. There is a constant error observed at the end, as the master stops sharing its location after reaching the return to the home location. From the field study, it is observed that setting the same ideal speed value at both master and slave is a better choice. Setting a lower ideal speed value in both master and slave will give a smooth movement between master and slave due to which there is a less chance of connection disruption.



Vehicle Setup

Enter the parameters :
Vehicle Address = '\dev\ttyAMA0' or '\dev\ttyS0' or 'tcp:127.0.0.5460'
Baudrate = 57600 for RPi or 115200 for SITL
Waypoints = Total number of waypoints

Vehicle Address: \dev\ttyAMA0
Baudrate: 57600
WayPoints: 5

Enter the Waypoint Coordinates

Coordinate No.-1

Latitude: 89.123
Longitude: 31.214
Altitude: 10

FIGURE 8. Results obtained from field experimental set-up 3, designed to validate the master-slave synchronization algorithm. (a) Snapshots of the designed Graphical User Interface (GUI) to feed coordinates easily to master during mission planning, (b) Trajectory of the master during mission planning according to given geodetic coordinates, (c) Trajectory plot of master and slave, while slave follows master and master follows a given mission, (d) Synchronization error plot between slave and master.

V. CONCLUSION

In this paper, the application of UAV in the view of post-disaster management is explored. We have designed a prototype of UAV-assisted emergency Wi-Fi based network to accelerate SAR operation and do on-site surveillance over the disaster region. To this end, we have used the RPI3 B+ development board, mounted on UAV to form an emergency Wi-Fi network over the disaster region. Adding to this, an Android application is designed to extend the Wi-Fi network coverage. A captive portal is intended to guide the survivors to find the relief camp locations and alert with precautionary measures. We have also proposed the algorithm for Wi-Fi auto re-connection, smooth network chain formation, and data management during surveillance. The performance of the designed prototype is assessed by doing three different types of field experiments. The first one is carried out to find a suitable wireless technology supported by RPI and its range; the second is carried out to do surveillance testing, and the last test is carried out to validate the algorithm proposed for the slave to follow the master. The experimental results reveal that although UDP throughput performance is better than TCP, but both UDP and TCP are recommended for WiND operation. For smaller distance, UDP is better due to high throughput performance, whereas the connection-oriented protocol TCP is better for larger distance. The performance of Wi-Fi AP is found to be better than the Ad-Hoc mode of operation irrespective of the frequency band. The maximum hop distance is found to be 280 and 290 meters for IEEE 802.11n and 802.11ac respectively. Under interference, the hop distance limits to 220 meters in case of IEEE 802.11n. Both hop distance and data rate can be improved by upgrading the hardware limitation of RPI such as the use of 5 dBi antenna instead of inbuilt Proant PCB antenna and using MIMO configuration, etc.

REFERENCES

[1] Z. Shao, Y. Liu, Y. Wu, and L. Shen, "A rapid and reliable disaster emergency mobile communication system via aerial ad hoc BS networks," in *Proc. IEEE 7th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, Sep. 2011, pp. 1–4.

[2] P. D. Pradeep and B. A. Kumar, "A survey of emergency communication network architectures," *Int. J. Service, Sci. Technol.*, vol. 8, no. 4, pp. 61–68, 2015.

[3] *Bivystic*. Accessed: Jul. 30, 2019. [Online]. Available: https://www.bivystick.com/

[4] R. Premkumar. *Wireless Networks for Disaster Relief*. Accessed: Jul. 30, 2018. [Online]. Available: http://www.cse.wustl.edu/~jain/cse574-14/ftp/disaster.pdf

[5] V. Y. Kishorbhai and N. N. Vasantbhai, "AON: A survey on emergency communication systems during a catastrophic disaster," *Procedia Comput. Sci.*, vol. 115, pp. 838–845, Aug. 2017.

[6] T. Sakano, S. Kotabe, T. Komukai, T. Kumagai, Y. Shimizu, A. Takahara, T. Ngo, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "Bringing movable and deployable networks to disaster areas: Development and field test of MDRU," *IEEE Netw.*, vol. 30, no. 1, pp. 86–91, Jan./Feb. 2016.

[7] ITU-T Focus Group. (May 2014). *Requirements on the Improvement of Network Resilience and Recovery With Movable and Deployable ICT Resource Units*. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-6-NRR-requirement.pdf

[8] D. G. Reina, M. Askalani, S. L. Toral, F. Barrero, E. Asimakopoulou, and N. Bessis, "A survey on multihop Ad-Hoc networks for disaster response scenarios," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 10, p. 647037, 2015.

[9] Q. Minh, K. Nguyen, and S. Yamada, "On-site configuration of wireless multihop access networks," IPSJ SIG, Japan, Tech. Rep., Sep. 2013.

[10] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "RescueMe: Location-based secure and dependable VANETs for disaster rescue," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 659–669, Mar. 2011.

[11] E. Onwuka, A. Folaponmile, and M. Ahmed, "MANET: A reliable network in disaster areas," *Jorind*, vol. 9, no. 2, pp. 105–113, 2011.

[12] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff, "Wireless sensor networks for flash-flood alerting," in *Proc. IEEE 5th Int. Caracas Conf. Devices, Circuits Syst.*, vol. 1, Nov. 2004, pp. 142–146.

[13] M. Bahrepour, N. Meratnia, M. Poel, Z. Taghikhaki, and P. J. Havinga, "Distributed event detection in wireless sensor networks for disaster management," in *Proc. IEEE 2nd Int. Conf. Intell. Netw. Collaborative Syst. (INCOS)*, Nov. 2010, pp. 507–512.

[14] A. R. Ulucinar, I. Korpeoglu, and A. E. Cetin, "A Wi-Fi cluster based wireless sensor network application and deployment for wildfire detection," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 10, 2014, Art. no. 651957.

[15] W. Wang and L. Guo, "The application of wireless sensor network technology in earthquake disaster," in *Proc. IEEE Int. Conf. Ind. Control Electron. Eng. (ICICEE)*, Aug. 2012, pp. 52–55.

[16] H. Aïache, V. Conan, G. Guibé, J. Leguay, C. Le Martret, J. M. Barcelo, L. Cerda, J. Garcia, R. Knopp, N. Nikaein, and X. Gonzalez, "WIDENS: Advanced wireless ad-hoc networks for public safety," in *Proc. IST Mobile Wireless Commun. Summit*, Dresden, Germany, 2005.

[17] A. Kumbhar and I. Güvenç, "A comparative study of land mobile radio and LTE-based public safety communications," in *Proc. IEEE SoutheastCon*, Apr. 2015, pp. 1–8.

[18] A. Paulson and T. Schwengler, "A review of public safety communications, from LMR to voice over LTE (VoLT E)," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 3513–3517.

[19] A. Merwaday and I. Güvenç, "UAV assisted heterogeneous networks for public safety communications," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Mar. 2015, pp. 329–334.

[20] M. Deruyck, J. Wyckmans, W. Joseph, and L. Martens, "Designing UAV-aided emergency networks for large-scale disaster scenarios," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 79, 2018.

[21] *Gotenna*. Accessed: Jul. 30, 2019. [Online]. Available: https://gotenna.com/

[22] *Goheart*. Accessed: Jul. 30, 2019. [Online]. Available: https://www.kickstarter.com/projects/crazyboytech/goheart-the-ultimate-outdoor-networking-device

[23] X. Bai, "Broadband wireless access in disaster emergency response," M.S. thesis, Roy. Inst. Technol., Stockholm, Sweden, 2016.

[24] E. Sithirasenan and N. Almahdouri, "Using WiMAX for effective business continuity during and after disaster," in *Proc. ACM 6th Int. Conf. Wireless Commun. Mobile Comput.*, 2010, pp. 494–498.

[25] G. T. C. Gunaratna, P. V. N. M. Jayarathna, S. S. P. Sandamini, and D. S. De Silva, "Implementing wireless Adhoc networks for disaster relief communication," in *Proc. IEEE 8th Int. Conf. Ubi-Media Comput. (UMEDIA)*, Aug. 2015, pp. 66–71.

[26] H. Suzuki, Y. Kaneko, K. Mase, S. Yamazaki, and H. Makino, "An ad hoc network in the sky, SKYMESH, for large-scale disaster recovery," in *Proc. IEEE 64th Veh. Technol. Conf.*, Sep. 2006, pp. 1–5.

[27] T.-H. Lee and T. Choi, "Self-powered wireless communication platform for disaster relief," in *Proc. Symp. IEEE 13th Asia–Pacific Netw. Oper. Manage.*, Sep. 2011, pp. 1–3.

[28] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, 4th Quart., 2016.

[29] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the sky: Leveraging UAVs for disaster management," *IEEE Pervasive Comput.*, vol. 16, no. 1, pp. 24–32, Jan. 2017.

[30] A. Bujari, C. T. Calafate, J.-C. Cano, P. Manzoni, C. E. Palazzi, and D. Ronzani, "Flying ad-hoc network application scenarios and mobility models," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 10, pp. 1550–1558, 2017.

[31] E. Yanmaz, R. Kuschnig, M. Quaritsch, C. Bettstetter, and B. Rinner, "On path planning strategies for networked unmanned aerial vehicles," in *Proc. IEEE Workshops Comput. Commun. (INFOCOM WKSHPS)*, Apr. 2011, pp. 212–216.

[32] Z. Han, A. L. Swindlehurst, and K. J. R. Liu, "Optimization of MANET connectivity via smart deployment/movement of unmanned air vehicles," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3533–3546, Sep. 2009.

[33] D. Zorbas, T. Razafindralambo, D. P. P. Luigi, and F. Guerriero, "Energy efficient mobile target tracking using flying drones," *Procedia Comput. Sci.*, vol. 19, pp. 80–87, Jun. 2013.

[34] M.-A. Messous, S.-M. Senouci, and H. Sedjelmaci, "Network connectivity and area coverage for UAV fleet mobility model with energy constraint," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[35] M.-A. Messous, H. Sedjelmaci, and S.-M. Senouci, "Implementing an emerging mobility model for a fleet of UAVs based on a fuzzy logic inference system," *Pervasive Mobile Comput.*, vol. 42, pp. 393–410, Dec. 2017.

[36] A. Guillen-Perez, R. Sanchez-Iborra, M.-D. Cano, J. C. Sanchez-Aarnoutse, and J. Garcia-Haro, "WiFi networks on drones," in *Proc. Kaleidoscope*, 2016, pp. 1–8.

[37] G. S. L. K. Chand, M. Lee, and S. Y. Shin, "Drone based wireless mesh network for disaster/military environment," *J. Comput. Commun.*, vol. 6, no. 4, p. 44, 2018.

[38] A. Jimenez-Pacheco, D. Bouhired, Y. Gasser, J.-C. Zufferey, D. Floreano, and B. Rimoldi, "Implementation of a wireless mesh network of ultra light MAVs with dynamic routing," in *Proc. IEEE Globecom Workshops*, Dec. 2012, pp. 1591–1596.

[39] *Raspberry Pi3 Model B+, the Latest Revision of Our Third-Generation Single-Board Computer*. Accessed: Jul. 30, 2019. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

[40] *Raspberry Pi3 Model B+ Station + AP Configuration*. Accessed: Jul. 30, 2019. [Online]. Available: https://imti.co/iot-wifi/

[41] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal Cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.

[42] G. Cai, B. M. Chen, and T. H. Lee, *Unmanned Rotorcraft Systems*. London, U.K.: Springer-Verlag, 2011.

[43] *Communicating With Raspberry PI via MAVLink and MAVLink Installation Description*. Accessed: Aug. 16, 2018. [Online]. Available: http://ardupilot.org/dev/docs/raspberry-pi-via-mavlink.html

[44] Q. T. Minh, Y. Shibata, C. Borcea, and S. Yamada, "On-site configuration of disaster recovery access networks made easy," *Ad Hoc Netw.*, vol. 40, pp. 46–60, Apr. 2016.

[45] A. A. Shahin and M. Younis, "Alert dissemination protocol using service discovery in Wi-Fi direct," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7018–7023.

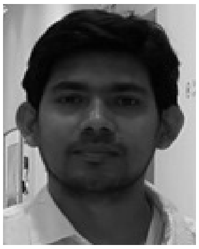
[46] M. El Alami, N. Benamar, M. Younis, and A. A. Shahin, "A framework for hotspot support using Wi-Fi direct based device-to-device links," in *Proc. IEEE 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 552–557.

[47] *CYW43455—Single-Chip 5G WiFi IEEE 802.11n/ac MAC/ Baseband/ Radio With Integrated Bluetooth 5.0*. Accessed: Jul. 30, 2019. [Online]. Available: https://www.cypress.com/file/358916/download

KIRTAN GOPAL PANDA received the B.Tech. degree in electronics and communication engineering from the NM Institute of Engineering and Technology, Bhubaneswar, India, in 2010, and the M.Tech. in communication and signal processing engineering from the National Institute of Technology, Silchar, India, in 2016. He is currently pursuing the Ph.D. degree with the G.S. Sanyal School of Telecommunications, IIT Kharagpur, India, under the Supervision of Prof. D. Sen. He was a Junior Project Assistant in the project entitled as Development of National Disaster Spectrum (NDS) and Disaster Communication Backbone Architecture (DiCoBA) with Prototype Development, from 2016 to 2018. His research interests include wireless communication systems, resource allocation in cloud RAN, and emergency network design.

SHRAYAN DAS received the bachelor's degree in electronics and telecommunication engineering from Bengal Engineering and Science University, Shibpur, India. He is currently pursuing the M.S. (by Research) degree with the G. S. Sanyal School of Telecommunications, IIT Kharagpur, India. He is also a Junior Project Assistant with the G. S. Sanyal School of Telecommunications, Indian Institute of Technology, Kharagpur, India. Prior to this, he was an Associate Systems Engineer with IBM India Pvt., Ltd. His research interests include wireless communication systems, routing algorithms, datacenter networks, drone-based mobile Ad-hoc network for disaster communication, and convex optimization.

DEBARATI SEN received the Ph.D. degree in telecommunication engineering from the Indian Institute of Technology Kharagpur, India, where she is currently an Associate Professor. She was a Postdoctoral Research Fellow with the Chalmers University of Technology, Sweden, and a Senior Chief Engineer with Samsung Research and Development Institute India, Bangalore (SRI-B), India. She is an Editorial Board Member of two international journals. Her research interests include wireless and optical communication systems, mostly on MB-OFDM, synchronization, equalization, UWB, BAN, green communications, 60 GHz communications, and baseband algorithm design for coherent optical communications. She was a recipient of the Best Paper Award at Samsung Tech., Conference 2010, and the IEI Young Engineers Award 2010.



WASIM ARIF received the B.E. degree in electronics and communication engineering from Burdwan University, India, the M.E. degree in telecommunication engineering from Jadavpur University, India, and the Ph.D. degree from NIT Silchar, India. He is currently an Assistant Professor with the National Institute of Technology Silchar, India. His research interests include wireless communication technology, mostly on cognitive radio technology, compressed sensing, and next generation wireless technology for medical applications.