Towards Efficient and Resilient Wireless Networks for Public Safety Applications

WRITTEN BY
Fan Liang & Qingzhong Liu & Amar Rasheed & Bing Zhou

2022

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Towards Efficient and Resilient Wireless Networks for Public Safety Applications

PI: Fan Liang
Co-PI: Qingzhong Liu, Amar Rasheed, and Bing Zhou
(fxl027, qxl005, axr249, bxz003) @shsu.edu
Computer Science Department
Sam Houston State University

Executive Summary

In this proposal, we propose to establish a theoretical and empirical foundation for designing efficient and resilient wireless networks to support public safety. For this purpose, we propose to develop techniques that enable effective device-to-device (D2D) communication, as well as schemes for optimal and rapid deployment of dynamic wireless networks using mobile base stations (BSs) and unmanned aerial vehicles (UAVs), based on realistic public safety scenarios. This proposal will initiate a scientific foundation for developing efficient and resilient wireless networks to help public safety communities in designing innovative communication techniques to conduct public safety disaster recovery and response. Our proposal will address imminent and urgent issues that, if left unaddressed, will have a profound impact on the development of public safety communication systems and their broadly supported applications, especially in life-threatening public safety situations.

The novelty and unique contributions of this proposal include:

(i) exploring and studying feasible D2D communications tailored to public safety applications.
(ii) developing and validating the techniques that enable quick and cost-effective deployment of dynamic wireless network infrastructure for public safety applications.

Our proposed research tasks and novel techniques can be summarized as follows: (i) Task I. Developing Effective D2D Communication Techniques for Public Safety: We propose to model public safety scenarios based on the collected datasets of real-world cases (i.e., the winter storm disaster in February 2021). We propose to systematically investigate some candidate schemes, in the interest of improving D2D communications, and compare their performance in real-world public safety models. (ii) Task II. Developing Effective Network Deployment Techniques for Public Safety: We propose techniques for performing rapid and cost-effective placement of both mobile BSs and UAVs, and consider factors such as the dynamics of traffic, user density, realistic constraints (e.g., geo-restriction and available information), requirements (e.g., coverage, QoS, and resilience), and public safety scenarios (nature disaster and man-made disaster), etc. We also propose novel schemes to find optimal deployment locations for flying UAVs and mobile BSs, which aim at minimizing deployment time and cost while guaranteeing QoS for public safety users, as well as the resilience of the network.

This project has the following immediate impacts: (i) Technical and Social Impacts: Our research will generate an immediate impact on public safety, emergency response, and emergency rescue. Our theoretical framework and techniques will help to advance the state-of-the-art in the wireless network industry. (ii) Integration of Research, Education, and Outreach: The PI will integrate the proposed research with all aspects of the educational environment, from classroom lectures, seminars, workshops, guest speakers, and lab work on original research, to outreach. The PI will incorporate the outcome of the project into courses on wireless communication and computer networks. The proposed work will provide excellent research and educational opportunities for both graduate and undergraduate students. PI will actively encourage minority students to join this project. The project targets workforce preparation and seeks to make our national wireless critical infrastructure efficient and resilient in supporting public safety. The broader impact of this project also includes instrumental in disseminating results to a broader set of public safety organizations, institutions, and companies in the Texas area.

Key Words: Public Safety; D2D; Dynamic Wireless Networks

Towards Efficient and Resilient Wireless Networks for Public Safety Applications
Project Description

1. Introduction and Overview

In this proposal, we propose to establish a theoretical and empirical foundation for designing efficient and resilient wireless networks to support power public safety applications. For this purpose, we propose to develop techniques that enable rapid and cost-effective deployment of dynamic wireless networks using mobile base stations (BSs) and unmanned aerial vehicles (UAVs), based on realistic public safety scenarios. This proposal will initiate a foundation for developing efficient and resilient wireless networks to help public safety events rescue.

Public safety applications rely on the time-critical delivery of information, both between emergency first responders (EFRs) and with victims and bystanders. Communication is one of the most critical requirements for public safety [1]. As a collaborative effort between law enforcement, fire and rescue, medical services, and often military personnel, the integrity and reliability of public safety communication (PSC) must far exceed commercial standards, as decision-making, organization, and ultimately life-or-death outcomes rest on the efficacy of public safety networks (PSNs) [2]. Although it is important to ensure communication among separate groups when a public safety event occurs, there is no single entity that oversees the entirety of public safety organizations yet. As such, each service may have its own PSN and rely on incompatible and disparate devices and technologies. Furthermore, under emergency conditions, such as terrorist attacks and riots, communications may be degraded or entirely disabled due to the significant increase in demand for communication in the emergency area exceeding the capacity of the local infrastructures (such as BSs) [3, 4, 5]. Moreover, in the case of natural disasters (e.g., earthquakes and hurricanes), the infrastructure (BSs and power supply) in the catastrophe area could be totally destroyed. Since electric power is the driving force of modern society, and the power grid acts key component of the national strategy. Power grid failure aggravates pressure on public communication systems [6]. Specifically, the power grid is fragile, in a disaster, the power grid is the source of a series of secondary disasters since many important rescue systems rely on electric power, especially communication systems. However, recovering the power grid also needs cooperation and communication support. Thus, decision-making, organization, and ultimately life-or-death outcomes rest on the efficacy of communication networks. However, there is no single entity that oversees the entirety of public safety organizations yet [7]. As such, each service may have its own communication network and rely on incompatible and disparate devices and technologies, which increase loss in public safety events.

One recent and well-known power grid safety event, in February 2021, a brutal winter storm battered the state, overwhelming its power grids and forcing millions of Texans to scavenge for the basic elements for survival — food, water and shelter from record cold. Since the power grid failure, total of 246 people was lost during chilly weather, late power recovery and late rescue [8]. While investigating the blackouts, how to reduce the first response time and improve emergency communication support become hot topics. It can be observed from the typical natural disaster, the power grid is fragile and easy to be failed in a natural disaster. Thus, how to provide robust communication support during a natural disaster, especially in power loss is the key to recovery after the disaster. To enable communication for responders in disaster/hostile environments, two complementary solutions are highly required. One is the use of D2D communications to enable direct communication among responders nearby, and the other is to establish a dynamic wireless network infrastructure to meet strict communication requirements for responders. Nonetheless, the power grid failures usually accompany other public safety scenarios, which make the design of both solutions challenging. Notice that, in response to demand from governmental and public safety organizations, the 3rd Generation Partnership Project (3GPP) has continued to provide updated LTE specifications to enable D2D communication and Mission Critical Voice functionality for public safety.

D2D communication can help to recover deficient or damaged communications in public safety events without the assistance of network infrastructure and provides communication services for EFRs. As demand has grown for providing EFRs with rich spatial and temporal data, and increased situational awareness, the public safety community and industry leaders have pushed for a comprehensive platform to solve the inevitable coverage failure inherent to disaster environments. Yet, effectively discovering

proximate devices, ensuring reliable bidirectional D2D links, efficiently using network resources, and supporting strict QoS requirements from EFRs in complicated and hostile public safety scenarios make the design of D2D communications challenging [9]. While several research efforts have been devoted to improving D2D performance (spectrum efficiency, energy efficiency, coverage, interruption, etc.), effective D2D communication tailored to complex public safety events remains unresolved. This calls for the systematic exploration of existing research on D2D communications. On the other hand, integrating mobile BSs and UAVs can improve network coverage to EFRs rapidly, and on-demand [10]. As an area of significant interest, there have been several research investigations in this direction. However, there remain significant deficiencies in the design of techniques to deploy components (e.g., mobile BSs, UAVs) in realistic public safety scenarios [11]. How to quickly and cost-effectively deploy network infrastructure given limited resources, and how to dynamically adapt to the communication needs of EFRs, remain challenging issues.

To address the issues outlined above, our proposal will (i) explore and study the feasible D2D communications tailored to public safety and (ii) develop and validate the techniques that enable quick and cost-effective deployment of dynamic wireless networks for public safety. Our proposed framework is the synergy of D2D techniques, efficient network deployment, and an integrated evaluation platform for public safety research and education.

In the following, the novelty of the proposed research tasks is summarized:

(i) ***Task I: Developing Effective D2D Communication Techniques for Public Safety*** (Section 3.2). In this task, we will model real-world public safety scenarios and develop a framework to explore existing D2D communication techniques. Based on the public safety scenarios, we will implement selected D2D techniques and compare them for public safety use.

(ii) ***Task II: Developing Efficient Network Deployment Techniques for Public Safety*** (Section 3.3). We will develop novel schemes for quick and cost-effective deployment of both mobile BSs and UAVs in realistic public safety scenarios to meet the coverage and QoS requirements of EFRs. The resilience of the deployed networks will be studied as well.

2. Proposed Research Plan

2.1 Overview

As shown in Fig. 1, we consider a generic wireless network model, which leverages D2D communications, and consists of BSs on the ground and UAVs in aerial space to support public safety. Ensuring communication among law enforcement agencies, police officers, first responder teams, and other participants in public safety events is extremely important. Nonetheless, the network infrastructure may be dysfunctional due to either congestion or physical damage. The D2D communication technique can establish connections, provide data transmission, and enable direct communication among EFRs with or without cellular network coverage. Mobile BSs are referred to as "cells on wheels", which can be relocated to support large traffic loads, improve network coverage, reduce the latency of data transmission, etc. UAVs, which carry lightweight BSs, can be deployed in aerial space rapidly to provide

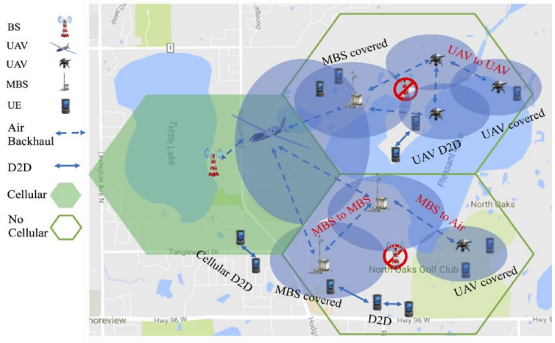

Fig. 1: Network Model

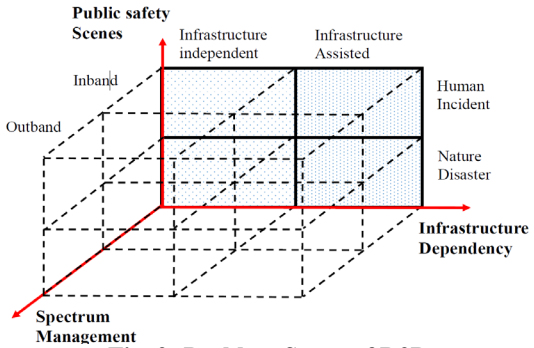

Fig. 2: Problem Space of D2D Communication

high mobility, adaptability, and fast network recovery. The UAVs and ground BSs can communicate with EFRs with rich and complimentary communication links.

In our research, we address the following critical and challenging issues: (I) *How can we identify effective D2D communication techniques for public safety?* (ii) *How can we develop techniques to quickly and cost-effectively deploy dynamic wireless networks to support public safety?* Our proposal is positioned to answer both questions fundamentally.

2.2 Research Task I - Developing Effective D2D Communication Techniques for Public Safety

A. Problem and Our Idea

To meet the communication requirements from EFRs, we consider the design and evaluation effective D2D communication techniques tailored to public safety, enabling EFRs to directly communicate with each other in both the presence and absence of network infrastructure.

While several research efforts on D2D communication have been conducted, most of the research aims to improve the performance (spectrum efficiency, energy efficiency, coverage, interruption, etc.), while the effectiveness of D2D communication is tailored to realistic public safety remains unsolved. To address this issue, it is critical to systematically study existing solutions on D2D communications and conduct a gap analysis to identify feasible techniques that could meet public safety requirements. Fig. 2 illustrates the problem space for D2D communication for public safety use, including infrastructure dependency (infrastructure-independent and infrastructure assisted), spectrum management (in-band and out-band), and public safety scenes (natural disaster and human incident). Notice that infrastructure independence means that devices of EFRs realize communication in a self-organizing way, without the assistance of network infrastructure. Also, in-band D2D uses the cellular licensed spectrum for both D2D and cellular users, while out-band D2D exploits unlicensed spectrum. In this project, we try to leverage Wi-Fi Direct (as an out-band solution) to enable D2D communication, which can not only offload massive data traffic from LTE-based cellular networks but also support public safety and other applications.

B. Proposed Research

We will systematically analyze and compare existing techniques proposed for D2D communication. Candidate techniques will be selected and enhanced to support public safety applications.

Task I-A: Modeling Real-World Public Safety Scenarios: In this subtask, we will study various representative real-world public safety scenarios (natural disasters and human incidents), and design models based on those scenarios. Particularly, we will systematically investigate the public safety conditions surrounding winter storm 2021 in Houston TX and derive models from real-world data. This will enable us to validate the performance of candidate algorithms and schemes in both public safety scenes. We have conducted some preliminary studies and obtained datasets related to these public safety incidents, including timeframe, damage area, personal injuries, communication disabled range, BS information in the incident affected areas, etc.

Task I-B: Investigating Effective D2D Techniques for Public Safety: Based on an extensive review of D2D communication, while there are several schemes proposed to improve D2D communication, the effectiveness of existing schemes for public safety applications is an open issue. To address this issue, we will systematically inspect the existing work on communication in public safety applications. Then, compare their performance in real-world public safety models. We will implement the selected algorithms and schemes in both simulation and emulation environments. We will leverage our extensive research experiments in modeling and simulation using network optimization theory, ns 3/Vienna LTE simulators [12], emulation using Common Open Research Emulator (CORE) [13, 19], and Software Defined Radio (SDR) testbed to evaluate the performances of D2D communication schemes in public safety.

2.3 Research Task II: Developing Effective Network Deployment Techniques for Public Safety

A. Problem, Challenges and Our Ideas

Problem: Recall that when disasters occur, communication infrastructure could be congested or totally damaged, effectively disabling service. This calls for deploying a dynamic wireless network infrastructure to provide coverage and communication for EFRs, in addition to D2D communication

outlined in Task I. Particularly, in this research, we address the issue of how to effectively deploy a dynamic wireless network, which consists of mobile BSs on the ground and UAVs in the aerial, that can support public safety. In our preliminary study [1], we addressed the issues of multi-path data streaming

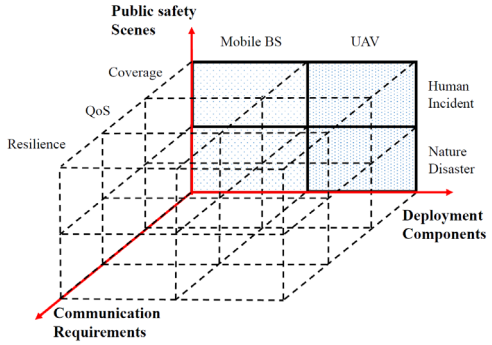

Fig. 3: Problem Space for Dynamic Network Deployment

in mobile Ad-Hoc networks to increase the throughput of the D2D communication. Based on the preliminary research, we will optimize the unmanned aerial vehicles (UAV) deployment to meet the coverage and QoS requirements of EFRs.

Notice that existing commercial networks are not designed with the principles of public safety in mind. Conversely, they are designed for maximizing revenue by allocating the minimum amount of the spectrum necessary per user [14]. Nonetheless, during an emergency, the incident location experiences a spike in traffic from both public users and first responders. The resulting congestion can affect the communication QoS of EFRs. This calls for the design of techniques that can optimally and rapidly deploy mobile wireless networks via mobile BSs and UAVs, meeting dynamic traffic needs for public safety. The dynamically deployed mobile wireless network can provide coverage for EFRs, support high traffic load, reduce end-to-end delay, avoid congestion, and improve the efficiency of network resource use in incident areas.

Challenges and Our Ideas: How to deploy wireless networks rapidly and cost-effectively in a public safety situation remains a challenging issue. The deployed mobile wireless networks need to serve a large number of EFRs with diverse QoS requirements. With limited resources (bandwidths, power, etc.), limited coverage range, and geographically and temporarily dynamic traffic, optimally deploying mobile BSs and UAVs in public safety scenarios to meet design requirements (maximizing network throughput, ensuring strict and diverse QoS requirements, improving system resilience to cyber-attacks, etc.) is critical. One challenge is to find the optimal deployment scheme for the given public safety scenario, which includes selecting the optimal number of UAVs and their deployment locations (x, y, h), in order to cooperate with mobile BSs on the ground and provide the required coverage for a given number of EFRs in the disaster area. To improve the resilience of the deployed network, more than one UAV shall be deployed within the communication distance of EFRs, which may need to deliver massive amounts of traffic and urgent information with very high reliability and strict QoS requirements. Also, when public safety settings change rapidly in the disaster area and EFRs become mobile, traffic intensity will change rapidly, posing additional challenges to the adaptability of the network.

To address the challenges, we shall develop techniques for quickly and cost-effectively deploying both mobile BSs and UAVs, and consider the dynamics of traffic, user density distribution, realistic constraints (geo-restriction, information availability, etc.), deployment costs, coverage and QoS for users, and the specifics of the public safety models. Fig. 3 shows the problem space of the dynamic deployment of wireless networks, including deployment components (mobile BSs and UAVs), communication requirements (coverage, QoS, and resilience), and public safety scenarios (nature disasters and human incidents). Based on the outlined problem space, we shall first design schemes for optimal deployment of mobile BSs and UAVs, and then develop novel schemes to find optimal locations for flying UAVs and moving BSs, which aim at minimizing deployment time and cost while guaranteeing QoS for EFRs.

B. Proposed Research

Our preliminary results establish the foundation for further study of the optimal deployment of mobile BSs and UAVs in dynamically deployed wireless networks, as well as their resilience to cyber-threats.

Task II-A: Optimally Deploying Mobile BS: In this subtask, we will study how to efficiently place mobile BSs to provide coverage for EFRs and minimize the travel time of mobile BSs. We will consider real-time guidance schemes, which can dynamically determine and adjust optimal routes from the current location to the destination during travel, while additionally considering the driver's preference [15]. To ensure that EFRs are covered by mobile BS, we need at least one BS inside each region. One goal in the deployment is to balance the signal-to-noise ratio (SNR) of any point over the entire region. Then, the optimal position of a mobile BS is the "center" of the disk covering the region, which ensures that the SNR of any point inside the region is balanced. Nonetheless, one mobile BS can be located at the intersection of multiple disks to cover users. Thus, we will define the areas formed by the disks and their intersections. Then, one optimization problem is how to select the minimum number of areas to deploy BSs to guarantee coverage. This problem can be formalized as the minimum set coverage problem, which aims to find the minimum number of subsets to cover the whole area. We will develop cost-effective algorithms to solve this problem, in which we can greedily select the subset that can cover the maximum number of uncovered EFRs.

When a large-scale incident occurs in an area, the traffic intensity will most likely rise above a threshold value, indicating that the original placement of mobile BS cannot handle the newly imposed user and traffic requirements. Thus, we will need to move BSs to new locations that can satisfy the new user's demands. After selecting the area to place a BS, in order to determine the exact position for the next move, we will apply mechanisms (e.g., Hungarian method [16], etc.) for solving the assignment problem to minimize the total movement of all mobile BSs. Nonetheless, we will consider practical constraints. For example, when we apply mobile BS deployment schemes to generate candidate locations for an incident area, some candidate locations may be in non-deployment areas or restricted sites. For these ineligible candidate locations, we will use a real-world map of the incident area to determine the next appropriate candidate location for deployment. This may influence the coverage and interfere with other BSs. Thus, determining the most appropriate candidate locations becomes another important issue for mobile BS deployment in restricted areas. We will also consider the case in which user density information is not available. To deal with this, one possible solution is to let mobile BSs perform a random walk with obstacle avoidance [17]. On reaching the points that maximize local communication area coverage, they stop navigation and become references for others to spread further.

Task II-B: Optimally Deploying UAV: The connectivity problem between UAVs and EFRs can be formalized as a minimal spanning tree (MST) problem. If we define global connectivity as the probability that a message can be successfully transmitted to all EFRs in the network under unlimited energy, but with limited power conditions, the MST is the optimal solution for connectivity. Then, the probability that a command is transmitted to all EFRs can be computed as the product of successful transmission probabilities of the links on the MST. To find a local optimum, starting from any initialization point, we will find a way to change the UAV's location so that a better MST can be obtained. With the preliminary results mentioned earlier, we shall adjust and adapt our algorithm into realistic, comprehensive, and applicable scenarios (i.e., traffic intensity adapted, QoS, and priority-aware dynamic UAV positioning).

The following three scenarios will be considered: (i) *Scenario 1*: Given the location, traffic, and required traffic priorities of EFRs, we shall find the minimum number of UAVs needed, and their locations. Additionally, when the traffic intensity fluctuates dramatically, we shall find the mobility pattern to relocate UAVs with minimal overall travel distance (i.e., shortest distance). (ii) *Scenario 2*: Given a limited number of UAVs, we shall maximize the coverage and satisfaction rates of EFRs, in which the traffic per EFRs and priority shall be considered. As a result, the UAVs shall dynamically adapt to the dynamic nature of traffic intensity, provide baseline coverage, guarantees the QoS of EFRs, satisfy the priority traffic requirements, and further improve the resilience of the dynamic network (i.e., provide backup UAVs for traffic with different priorities). (iii) *Scenario 3*: With the best satisfaction provided from the limited number of UAVs, some EFRs may not be adequately satisfied due to limited resources. Considering limited resources of UAVs, other problems to be addressed lie in resource sharing and scheduling to fulfill the requirements from responders (coverage, QoS awareness).

The joint deployment of mobile BSs and UAVs will be studied to enhance the performance of deployed networks to adapt to public safety scenarios. The mobile BS, which provides efficiency, reliability, and durability from the rich power supply and high network capacity, is limited in topographical accessibility, as well as reaction time. In contrast, the UAV has the advantages of quick response, high accessibility, and adaptability. By leveraging the advantages of both mobile BSs and UAVs, joint deployment will be studied in the following three cases. First, with the initial deployment of mobile BSs, the network can be further improved by enlisting the support of UAVs when the mobile BSs are not capable of meeting QoS requirements of EFRs. For example, the mobile BSs may be blocked by rioters in some extreme cases, and the UAV can be deployed to recover the network in such an area. Second, with the UAVs initially deployed, which quickly respond to an emergency, the network efficiency, reliability, and durability can be enhanced by leveraging additional mobile BSs. For example, when an emergency (e.g., power grid failure) suddenly occurs, the UAV can be deployed quickly as the first to arrive, and then mobile BSs can participate in further improving network coverage. Last, the mobile BSs and UAVs can be deployed equally and coexist to establish the network in the case of public safety incidents (e.g., Baltimore riot).

Task II-C: Developing Techniques to Improve Network Resilience: We will develop a theoretical framework to systematically explore the space of cyber-threats in the deployed wireless network, investigate their impacts on EFRs and system performance, and develop effective techniques to mitigate attacks. By leveraging our prior work and the PI's research in cybersecurity, we will develop a generic modeling framework to explore threats from the plane of attacks (i.e., user/data plane and control plane), security services (i.e., data integrity and data availability, etc.), and attack venues (i.e., UE, mobile BS, UAV). To secure the deployed network, we will develop an integrated defense system against diversified cyber-threats, which span generic countermeasures from the following perspectives: attack prevention, detection, and response. We will also leverage our designed distributed systems [8] to improve the efficiency of threat detection and analysis.

3. Project Execution

The following will be the task detail and important milestones of this project.

Task I: Developing Effective D2D Communication Techniques for Public Safety

(i) *Task I-A – Modeling Real-World Public Safety Scenarios*: In this subtask, we will study some representative real-world public safety scenarios (natural disasters and human incidents), and design the models based on those public safety cases. Particularly, we will systematically investigate public safety scenarios of winter storm disaster in Houston 2021 and develop models from them. Then, we will validate the performance of candidate algorithms and schemes applied to both public safety scenes. We have done some preliminary work to obtain datasets related to these public safety incidents, including timeframe, damage area, personal injuries, communication disabled range, BS information of the disaster scenes, etc.

(ii) *Task I-B – Investigating Effective D2D Techniques for Public Safety:* There are several schemes proposed to improve D2D communication, however, the effectiveness of existing schemes in public safety scenarios remains unsolved. To address this issue, we will systematically model and analyze some selected schemes based on our survey and prior works, implement them, and compare their performance in real-world public safety models. We will implement the selected algorithms and schemes in both simulation and emulation environments, and then implement them in our real-world testbed as well. We will leverage our extensive research experiments in modeling and simulation using optimization theory, using CORE [1, 5] and SDR testbed to evaluate the performance of D2D communication schemes in the public safety models. After the implementation of the modeled scenarios in Task I-A and candidate algorithms in Task I-B, we follow the procedure that applies modeling/simulation, emulation, and testbed to create prototypes of D2D communication applications in public safety scenarios.

Evaluation Metrics for Task I: We will define the metrics to evaluate Task I from the following perspectives: (a) We will inspect the public safety models that evaluate the parameter datasets for rationality and authenticity. Also, we will review the public safety model to insure that is not missing any important factors that are abstracted from real public safety scenario datasets. (b) Discovery is a key

enabler for D2D communications and ProSe. We will evaluate time cost and efficiency by using selected discovery algorithms to discover UEs in the coverage area during public safety situations. (c) We will evaluate the efficiency of network resource allocation schemes. (d) Relay is usually used for extending the coverage of the communication in public safety scenes. We will evaluate the effectiveness of relays, include relay node selection, multi-hop routing, and relay assignment.

Task II: Developing Effective Network Deployment Techniques for Public Safety

(i) *Task II-A – Optimally Deploying Mobile BS:* In this subtask, we will study how to efficiently place mobile BSs to provide the necessary coverage for EFRs and optimize the travel time of mobile BSs. We will leverage our prior work on real-time en-route guidance scheme, which can dynamically calculate and adjust the optimal route from its current location to the destination during travel with consideration for the driver's preferences [1]. We will study deployment problems in various scenarios, geographically and temporally dynamic traffic patterns, whether the user population density is available or not available, and other realistic constraints. At the conclusion of this research subtask, we will obtain our optimal scheme for deploying mobile BSs for public safety.

(ii) *Task II-B – Optimally Deploying UAV:* The connectivity problem between UAVs and EFRs can be formalized as a minimum spanning tree problem. We will develop three scenarios based on MST. We will integrate LTE techniques with UAVs designed for individual public safety models. Then, we will adjust and adapt our algorithm into realistic, comprehensive, and applicable scenarios (i.e., traffic intensity adaptation, QoS and priority-aware dynamic UAV positioning). Finally, we will obtain the optimal scheme that integrates both mobile BSs and UAVs to improve performance in real public safety scenes.

(iii) *Task II-C: Developing Techniques to Improve Network Resilience:* We will develop a theoretical framework to systematically explore the space of cyber-threats in the deployed wireless network and investigate their impacts on EFRs and system performance. To secure the deployed network, we will develop an integrated defense system against diversified cyber threats from the perspectives of attack prevention, detection, and response. Our existing cloud-based systems will be integrated to improve the efficiency of threat detection and analysis.

To validate the effectiveness and feasibility of our proposed deployment schemes, we design modeling/simulation, emulation, and testbed implementation with realistic public safety scenarios. Our designed evaluation considers large-scale city-level simulation, medium-scale town-level emulation, and small-scale physical testbed implementation.

Evaluation Metrics for Task II: We consider comprehensive metrics to evaluate the performance of the deployment schemes, including overhead and performance gain in the public safety scenes. Observations in a public safety scene can be quantified by the network coverage ratio, user density, and demand QoS. The overhead of the proposed schemes can be evaluated by the time taken in completing deployment, deployment cost, and computational and control overhead. The network performance gain can be measured by network capacity, delay, path loss rate, jitter, etc.

The **timeline** of the project is given in Table 1. In the first two months, we will focus on Task I. There are two milestones in this stage. The first milestone is 04/28/2022, and the output is public safety scenario models. The second milestone is 05/21/2022, the output being the selected candidate algorithms. In the following 3 months, we will devote most of our efforts to Task II, achieving three milestones as well. The first milestone is 06/24/2022. The output is a selected scheme for optimizing the deployment of BSs. The second milestone is 07/29/2022. The output is a selected scheme for optimizing the deployment of the UAVs. The third milestone is 08/15/2022, and the output is a theoretical framework to systematically explore the space of cyber-threats in the deployed wireless networks and investigate their impacts on EFRs and system performance.

The deliverables of this project include theoretical, technical, and algorithmic design and proof, as well as real testbed implementation and demonstration. We are confident in our ability to carry out this new research project. As discussed below, we have extensive research and developmental experience in the areas of multi-disciplinary research with recognized experts in wireless networks (D2D communication, public safety, performance modeling, simulation, and emulation), as well as experts in system, security and resilience research, which are closely related to the work proposed herein.

Task Name	Duration	Start	Finish
Task I: Developing Effective D2D Communication Techniques for Public Safety	**45 days**	**3/21**	**5/21**
Task I-A: Modeling Real-World Public Safety Scenarios	28 days	3/21	4/27
Milestore 1	0 days	4/28	4/28
Task I-B: Investigating Effective D2D Techniques for Pulibc Safety	36 days	4/1	5/20
Milestore 2	0 days	5/21	5/21
Task II: Developing Effective Network Deployment Techniques for Public Safety	**75 days**	**5/2**	**8/15**
Task II-A: Optimally Deploying Mobile BS	38 days	5/2	6/22
Milestore 3	0 days	6/24	6/24
Task II-B: Optimally Deploying UAB	42 days	6/1	7/28
Milestore 4	0 days	7/29	7/29
Task II-C: Developing Techniques to Improve Network Resilience	32 days	7/1	8/14
Milestore 5	0 days	8/15	8/15

Table 1: Project Schedule

Biographical Sketch

Dr. Fan Liang

FAN LIANG is currently an assistant professor in computer science at Sam Houston State University (SHSU). He received his bachelor's degree in computer science from Northwestern Polytech University, Xi'an, China, in 2005, master's degree in computer engineering from the University of Massachusetts Dartmouth in 2015, and doctoral degree in computer science at Towson University in 2021. Before joining Towson University, he had 9 years of industry working experience in the network security area. His research interests include effective and secure Deep Learning-Driven data analytics in IoT Systems and effective and secure Edge Computing in IoT Systems. In addition, his research is also related to IoT search engines and data trading. Based on his research interests, he has published 19 publications, which include book chapters, solid journal papers, and conference papers in the last 4 years. In addition, he worked with Dr. Wei Yu to successfully win NSF and NIST funding during the Ph.D.

Dr. Qingzhong Liu

Dr. Qingzhong Liu is currently an associate professor in computer science at Sam Houston State University (SHSU), and he has been approved to promote for a full professor by SHSU. His research interests are primarily focused on cybersecurity, digital forensics, bioinformatics, multimedia computing and forensics, artificial intelligence, and computing application. His study has been funded by US Army, NIJ, NSF, and NIH. He was honored with several awards, including the Fraud Impact Award at Great Houston in 2015, SHSU College of Science and Engineering Technology Research Excellence Award in 2016, SHSU Excellence in Scholarly and Creative Activity Award in 2017. In 2021, He was selected by Stanford University as one of the world's top 2% scientists in artificial intelligence and image processing.

Dr. Amar Rasheed

Dr. Amar Rasheed is an Assistant Professor in the Department of Computer Science at Sam Houston State University. He has more than 15 years of research and teaching experience. He has held multiple research and teaching positions before joining Sam Houston State University in Spring 2020. He worked as an assistant professor and was the director of the IoT and Embedded Systems Security Lab at Armstrong State University, where he conducted and managed multiple undergraduate and graduate research projects in the areas of Authentications, Industrial Control Systems, and Data Privacy protocols for IoT systems. His research works were published in high-quality IEEE Transaction papers and conference proceedings. Dr. Rasheed also held a position as a postdoctoral fellowship in the Information Science and Technology Division at Applied Research Lab at Pennsylvania State University. Dr. Rasheed developed multiple key distribution algorithms for stationary and mobile unmanned vehicle systems, his works were funded by the Air Force Lab

Dr. Rasheed's research interests include embedded system security based on ARM Cortex-M* platforms, hardware design and multi-sensor fusion algorithms for IoT and sensor networks security, hardware-based key distribution scheme, data privacy protocols, light-weight authentication schemes for power-efficient systems, secure data transfer protocol for industrial control systems, hardware security and malware analysis for IoT systems, light-weight intrusion detection systems for IoT, designing and integrating UWB/LoRa wireless capabilities into IoT systems.

Dr. Bing Zhou

Dr. Zhou has been actively teaching and training students in computer science and cybersecurity for more than 10 years, advising and mentoring over 60 students at all levels. She published several research papers with students. Several of her former master's students have joined Ph.D. programs. She was recognized with the Faculty and Student Team Awards from the Center for Enhancing Undergraduate Research Experiences and Creative Activities (EURECA) of SHSU in 2016 and 2018. Zhou is also an impactful scholar in the professional community, four of her journal articles are recognized as the top 1% highly cited papers by the Web of Science. Her research interests include Cybersecurity, Database Forensics, Soft Computing, and Data Mining. She has served on the TPC for several highly ranked conferences including AAAI and IJCAI. She has also served as an external reviewer of ABET accredited programs for peer institutions.

Budget

- A total of $149,617.90 will be allocated to the project, including $44,798.90 for equipment and $104,819.00 for personnel.
- Equipment: to implement and evaluate the proposed tasks, we need to purchase equipment. Including 5G communication equipment, Unmanned aerial vehicles, Laptops, etc. The details are listed in Table 2.
- Personnel: Required personnel includes PI, Co-PI, undergraduate and graduate students. The PI and Co-PI will develop the methodologies, algorithms, hardware and implement the proposed tasks. Students will take responsibility for environment settings, hardware configurations, programing, and evaluations. For undergraduate students, the hourly rate is $18.75, and they work 20 hours pre-week. For graduate students, the monthly salary is $2,400.00.
- The budget details are shown below:

Equipment Type	Equipment Detial	Quantity		Price		Amount
5G Router	Nighthawk M5 5G WiFi 6 Mobile Router Unlocked	10		$699.99		$6,999.90
Terminal	Raspberry Pi 4 Model B 2019 Quad Core 64 Bit WiFi Bluetooth	20		$180.00		$3,600.00
Communication module	SIM8202X-M2 SIMCom Original 5G Module	20		$290.00		$5,800.00
UAV	DJI Mavic 3	10		$2,199.00		$21,990.00
5G Data Plan	5G unlimited data plan from Verizon	10		$130.00		$1,300.00
Laptop	Precision 7560 Data Science Workstation	1		$5,109.00		$5,109.00
Total Amount for Equipment						$44,798.90
Personnel	**Number of Personnel**	**Duration (Months)**		**Salary Per Month**		**Amount**
PI	1	1		$9,224.00		$9,224.00
Co-PI	3	0.5		$10,930.00		$16,395.00
Undergraduate Students	8	3		$1,500.00		$36,000.00
Graduate Students	6	3		$2,400.00		$43,200.00
Total Amount for Personnel						$104,819.00
Total Amount						$149,617.90

Table 2 Project Budget

Reference:

[1] Hildmann, Hanno, and Ernö Kovacs. "Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety." *Drones* 3, no. 3 (2019): 59.

[2] Deepak, G. C., Alexandros Ladas, Yusuf Abdulrahman Sambo, Haris Pervaiz, Christos Politis, and Muhammad Ali Imran. "An overview of post-disaster emergency communication systems in the future networks." *IEEE Wireless Communications* 26, no. 6 (2019): 132-139.

[3] Chen, Chao, Carlos Pomalaza-Ráez, Mike Colone, Robert Martin, and Jim Isaacs. "Modeling of a public safety communication system for emergency response." In *2009 IEEE International Conference on Communications*, pp. 1-5. IEEE, 2009.

[4] Du, Chunquan, and Shunbing Zhu. "Research on urban public safety emergency management early warning system based on technologies for the internet of things." *Procedia Engineering* 45 (2012): 748-754.

[5] Alsamhi, Saeed H., Faris A. Almalki, Ou Ma, Mohammad Samar Ansari, and Marios C. Angelides. "Performance optimization of tethered balloon technology for public safety and emergency communications." *Telecommunication Systems* 75, no. 2 (2020): 235-244.

[6] Fang, Xi, Satyajayant Misra, Guoliang Xue, and Dejun Yang. "Smart grid—The new and improved power grid: A survey." *IEEE communications surveys & tutorials* 14, no. 4 (2011): 944-980.

[7] Fredericksen, Patricia J., and Daniel Levin. "Accountability and the use of volunteer officers in public safety organizations." *Public performance & management review* 27, no. 4 (2004): 118-143.

[8] February 13–17, 2021 North American winter storm – Wikipedia: https://en.wikipedia.org/wiki/February_13%E2%80%9317,_2021_North_American_winter_storm

[9] Haus, Michael, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. "Security and privacy in device-to-device (D2D) communication: A review." *IEEE Communications Surveys & Tutorials* 19, no. 2 (2017): 1054-1079.

[10] Huang, Wenhuan, Zhaohui Yang, Cunhua Pan, Lu Pei, Ming Chen, Mohammad Shikh-Bahaei, Maged Elkashlan, and Arumugam Nallanathan. "Joint power, altitude, location and bandwidth optimization for UAV with underlaid D2D communications." *IEEE Wireless Communications Letters* 8, no. 2 (2018): 524-527.

[11] Zeng, Yong, Rui Zhang, and Teng Joon Lim. "Wireless communications with unmanned aerial vehicles: Opportunities and challenges." *IEEE Communications Magazine* 54, no. 5 (2016): 36-42.

[12] Abreu, Thiago, Bruno Baynat, Marouen Gachaoui, Tania Jiménez, and Narcisse Nya. "Comparative study of LTE simulations with the ns-3 and the Vienna simulators." In *SimuTools*, pp. 55-63. 2015.

[13] Tan, Song, Wen-Zhan Song, Qifen Dong, and Lang Tong. "Score: Smart-grid common open research emulator." In *2012 IEEE third international conference on smart grid communications (SmartGridComm)*, pp. 282-287. IEEE, 2012.

[14] Cao, Jin, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. "A survey on security aspects for LTE and LTE-A networks." IEEE communications surveys & tutorials 16, no. 1 (2013): 283-302.

[15] F. Liang, J. Nguyen, W. Gao, W. G. Hatcher and W. Yu, "Towards UAV Assisted Multi-Path Data Streaming in Mobile Ad-Hoc Networks," *2018 International Conference on Computing, Networking and Communications (ICNC)*, 2018, pp. 599-603, doi: 10.1109/ICCNC.2018.8390303.

[16] Kuhn, Harold W. "The Hungarian method for the assignment problem." *Naval research logistics quarterly* 2, no. 1-2 (1955): 83-97.

[17] Kegeleirs, Miquel, David Garzón Ramos, and Mauro Birattari. "Random walk exploration for swarm mapping." In *Annual conference towards autonomous robotic systems*, pp. 211-222. Springer, Cham, 2019.

[18] Bhuyan, Monowar H., Hirak Jyoti Kashyap, Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Detecting distributed denial of service attacks: methods, tools and future directions." *The Computer Journal* 57, no. 4 (2014): 537-556.

[19] Gao, Weichao, Hengshuo Liang, James Nguyen, Fan Liang, Wei Yu, Chao Lu, and Mont Orpilla. "Emulation-based performance evaluation of the delay tolerant networking (DTN) in dynamic network topologies." In *International Conference on Software Engineering Research, Management and Applications*, pp. 23-41. Springer, Cham, 2019.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Liang, F. , Liu, Q. , Rasheed, A. , Zhou, B. (2022). Towards Efficient and Resilient Wireless Networks for Public Safety Applications (Report No. 2022 - 1003). The Sam Houston State University Institute for Homeland Security.

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY