IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 29, 2018, accepted October 25, 2018, date of publication November 5, 2018, date of current version December 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2879760

Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions

WEI YU[1], HANSONG XU[1], JAMES NGUYEN[2], ERIK BLASCH[3], (Senior Member, IEEE), AMIRSHAHRAM HEMATIAN[1], AND WEICHAO GAO[1]

[1]Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA
[2]U.S. Army Communications-Electronics Research, Development, and Engineering Center, Aberdeen Proving Ground, MD 21005, USA
[3]U.S. Air Force Research Laboratory, 13441 Rome, Italy

Corresponding authors: Wei Yu (wyu@towson.edu) and Hansong Xu (hxu2@students.towson.edu)

ABSTRACT To prevent economic losses, maintain social order, and protect the well-being of the populace during public safety and crisis recovery scenarios, such as man-made and natural disasters, the efficient and effective delivery of time-critical information to first responders and victims plays a key role. Nonetheless, too often, the communication infrastructures that enable time-critical information delivery become dysfunctional, due to traffic overloads or physical damage. Thus, the user-side solution [e.g., device-to-device (D2D) communications] and the network-side solution [e.g., dynamic wireless networks (DWNs)] are essential communication techniques that can enhance or restore communication for responders and victims in the harsh environment associated with public safety scenes. While D2D has been widely studied and investigated in legacy/commercial communication networks, as well as DWN, little work has been done toward adapting D2D and DWN from a public safety perspective. In this survey, we first design a layered structure, consisting of the public safety service layer, time-critical information delivery layer, and physical object layer, from which to consider the public safety system and its key components. We then extensively review research efforts on both D2D and DWN as complimentary user-side and network-side communication techniques toward effective public safety communications. Particularly, we investigate the approaches and standardization progress of D2D and DWN for public safety communications. Finally, we provide insights into challenges and potential solutions regarding D2D, DWN, security and resilience, and performance evaluation of public safety communication, as well as the integration of state-of-the-art communication and computing technologies to further improve time-critical information delivery in various public safety scenarios.

INDEX TERMS Device-to-device communications, dynamic wireless networks, public safety communications, Internet of Things, cloud/edge computing, 5G.

I. INTRODUCTION

A. MOTIVATION

Two recent and well-known public safety scenarios, the Baltimore Riots in 2015 and Hurricane Harvey in 2017, are typical examples of public safety emergencies. Specifically, during the riots in Baltimore, Maryland, occurring from the middle of April to early May in 2015, over 1000 police officers and 2500 national guardsmen were deployed into the city, and a state of emergency was declared. As cellular towers were overloaded, significant problems plagued police communications during that time. As a result, approximately 113 police officers were injured, more than 16 law enforcement vehicles were destroyed, and city order was non-existent [2], [77], [120], [149].

More recently, in 2017, hurricane Harvey made landfall in eastern Texas in mid-August, leading to massive flooding over a period of four days. The result was thousands of homes being inundated, at least 71 deaths, and an estimated \$70 billion in economic losses [1], [146]. The first communication status report from the FCC (Federal Communications Commission) indicated that, of the 55 affected counties of Texas and Louisiana, 3 counties experienced more than 50 % of their cell sites being down, the hardest hit experiencing 94.7 % cell site outage [53].

The massive consequences of communication instability and damage demonstrated in the above scenarios extend to all public safety events (e.g., terrorist attacks, riots, and natural disasters such as earthquakes and hurricanes), and pose extreme threats of economic loss, societal disorder, and loss of life. To minimize the consequences of public safety emergencies, reliable communication responses must be conducted rapidly through the process of situation awareness and crisis coordination, including emergency monitoring, reporting, and relief. Those responses are highly reliant on the interoperation and collaboration of multiple response agencies (law enforcement, fire and rescue, military personnel, medical response, and others). Nonetheless, too often in public safety scenarios, the delay, inaccuracy, and failure of time-critical information delivery to and among the multiple responders hinders the ability for rapid response. Specifically, significant traffic increases in the affected area of a public safety event may degrade or disable communication through the local network infrastructure. In addition, under natural disasters, network infrastructure and power supply in the catastrophe area could be physically damaged or destroyed.

From the perspective of time-critical information delivery, the communication infrastructure is vulnerable to overloading and physical damage by both manmade and natural disasters. In either case, if the communication quality of service (QoS) for public safety responders and victims cannot be satisfied, recovery activities could be greatly hindered. The key orthogonal components of a wireless network are the wireless infrastructure and the mobile devices, representing the two primary components (i.e., network infrastructure and user device). On one hand, the wireless network infrastructure on the network side consists of Base Stations (BSs), control and management subsystems, data centers, etc. On the other hand, mobile edge devices such as smartphones interact with each other through the support of the wireless communication infrastructure or discover other nearby devices and establish direct communication. The techniques applied to the wireless network infrastructure to improve network performance are considered network-side solutions, such as optimal base station deployment schemes and algorithms, protocols to support control and management, etc. In addition, techniques directly applied to mobile devices, such as direct communication (D2D, etc.) comprise user-side solutions.

Toward enabling and improving wireless communication technology for public safety communications, both D2D communication on the user side and DWN deployment on the network side can be integrated as orthogonal and complimentary solutions. As a user-side solution, D2D enables communication among public safety responders, independent of the existing network infrastructure, as the public safety responders may operate outside of coverage areas or in areas with limited or degraded network capacity. Complimentary to this solution, dynamic wireless network deployment, as a network-side solution, can dynamically establish a wireless network infrastructure to increase network capacity and temporarily provide network coverage for public safety responders, adapting to ongoing public safety events. Nonetheless, complicated public safety scenarios make the design of both solutions challenging.

B. RELATED WORK

Various surveys have reviewed research efforts on leveraging communication technologies to ensure critical information delivery from different aspects. Particularly, Räty [125] reviewed the key components in the surveillance system, its development, and challenges to the performance constraints. The key components, which act as a collaborative effort to enable the capability of information collection and situation awareness, consist of video/audio-based surveillance, wireless network data transmission, and energy efficient remote sensing. The challenges to advancing the surveillance system include the implementation of the distributed real-time system, inter-/intra-cooperation of the multiple surveillance techniques, intelligence of the software autonomy, and their energy efficiency and scalability. Baldini *et al.* [20] comprehensively and broadly reviewed public safety hierarchy organizations, possible public safety scenarios, standards and regulations, and communication technologies, among others. In particular, the communication technologies (e.g., the dedicated radio system APCO 20 in the USA), commercial radio system (e.g., GSM and LTE), and others (e.g., WiFi/WiMax) were described and compared.

LTE, as one of the most extensive and successful commercial wireless communication networks worldwide, naturally supports and addresses specific communication requirements for public safety applications. For example, Liebhart *et al.* [87] investigated LTE for public safety, including features, services, techniques, etc. In particular, LTE supports various priority services that can be potentially important for public safety, including warning message broadcasting, multimedia service, and lawful interception. The proximity service and group communication service on top of LTE are also critical for public safety. Also, recently, Kumbhar *et al.* [79] reviewed spectrum allocation for public safety and standard activities, LMRS-based narrowband and LTE-based broadband for public safety, as well as the integration of emerging technologies, such as mmWave, massive MIMO (Multiple-Input and Multiple-Output), unmanned aerial vehicles (UAVs), etc. Finally, Zeng *et al.* [169] reviewed the network architecture, channel characteristics, and design aspects of UAV-aided wireless communication networks to serve various applications (agriculture, aeronautics, etc.). Two communication techniques (UAV-aided mobile relaying and D2D) were pointed out to improve the network performance.

D2D communication is a technique that enables the direct communication of User Equipment (UE) when the parties are within range for direct communication. In cellular networks, D2D can enable direct communication without traversing the central network infrastructure. In this way, the direct communication between devices can provide reduced delay and higher throughput. Such gains intro-

TABLE 1. Comparison with related works.

Related work	Public Safety						Communication						
	Surveillance System	Organization Hierarchy	Spectrum	Application	Security &Privacy	Evaluation Platform	Sensor Network	Dedicated Communication Systems	SDR	LTE	Portable Network	D2D	MANET /VANET
[125]	✓						✓						
[20]		✓						✓					
[79]			✓						✓	✓			
[169]											✓		
[21]												✓	
[96]										✓		✓	
[55]				✓						✓		✓	
[11]													✓
[63]					✓								✓
This Survey				✓	✓	✓				✓	✓	✓	✓

duced by the improved spectral efficiency result from the reduced communication distance. In the D2D-enabled cellular network, the cellular infrastructure manages/assists D2D communication, including in device discovery, link establishment, and others, via its wide coverage [21], [57], [96]. D2D is important for supporting communication in various public safety scenarios, as it can provide communication services in a peer-to-peer fashion, with the aid of network infrastructure in in-coverage cases, or without the aid of network infrastructure in out-of-coverage cases [55]. Also, in the mobile/vehicular ad hoc network(MANET/VANET), various devices can form a dynamic wireless network that enables information sharing between devices without the intervention of the network infrastructure [11]. In MANET/VANET, the information sharing relies on multi-hop packet forwarding, which does incur the challenges of network performance and security issues [63]. Overall, MANET/VANET supports public safety scenarios when a network infrastructure is not available.

We appraise and compare the contributions of various surveys in Table 1, including surveys in communication, public safety, and other related areas. The checkmarks indicate the main focus of a specific survey paper. Notice that the table identifies the key components, and the sparsity of the literature indicates a need for a more comprehensive survey. For example, survey [125] focused on the assessment of surveillance systems and wireless sensor networks. In comparison, our survey studied the untouched areas of combined communication and public safety. Additionally, distinct from existing efforts, this survey introduces a layered structure to outline public safety and its key components, reviews the primary user-side solution (i.e., D2D communication) and network-side solution (i.e., DWN deployment) necessary to overcome the challenges of public safety emergencies, and which can work cooperatively in supporting the time-critical information delivery in various public safety scenarios. In general, this paper (i) explores and studies the feasible D2D communications tailored to public safety; (ii) investigates and evaluates the rapid, cost-effective, and resilient deployment of DWN for public safety; and (iii) outlines open issues and potential solutions for D2D communication, DWN deployment, security and resilience, modeling, simulation and performance evaluation; as well as the integration of emerging techniques, such as IoT, cloud/edge computing and 5G.

C. CONTRIBUTIONS AND OUTLINE OF THE PAPER

Our contributions can be summarized as follows.

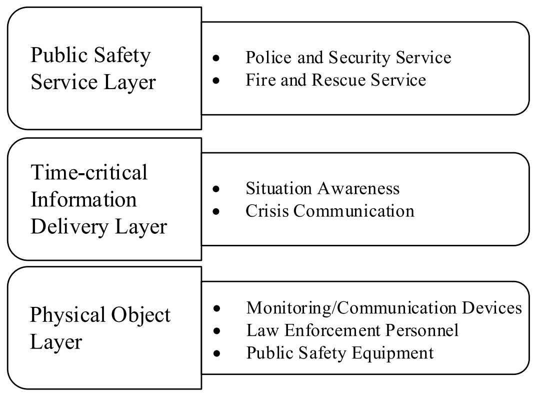

FIGURE 1. Layered structure on public safety.

First, we design a taxonomy that consists of three layers (i.e., public safety service layer, time-critical information delivery layer, and physical object layer) to provide a generic layer structure for public safety systems, as shown in Fig. 1. Considering, then, the time-critical information delivery layer, we present a pyramid structure, as shown in Fig. 2, where time-critical information, communication application, and communication techniques indicate the top, middle, and bottom layers, respectively. Notice that the critical and supportive communication techniques, which comprise the bottom layer of the pyramid structure, are the key objectives of this paper.

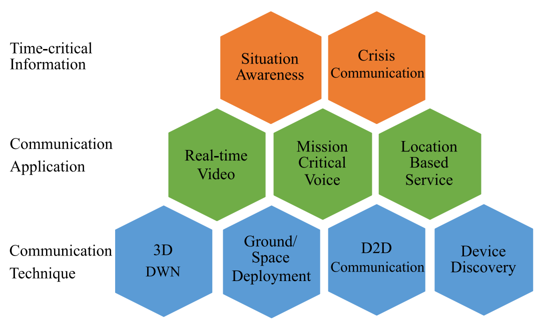

FIGURE 2. Pyramid structure on time-critical information delivery.

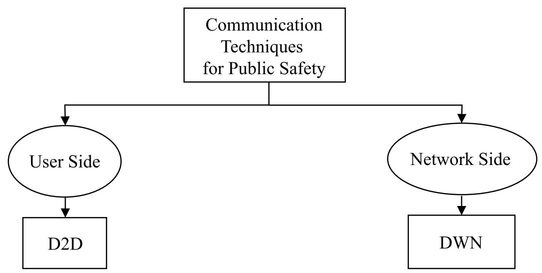

FIGURE 3. User-side and network-side communication techniques on public safety.

Second, we consider two critical and complementary communication techniques to address user connectivity and network establishment for public safety communications. As shown in Fig. 3, public safety communication techniques can be considered from both user-side and network-side perspectives. We systematically review the research efforts regarding D2D as one representative user-side communication technique, outlined in Fig. 4 subdivided into in-coverage and out-of-coverage mechanisms that can cope with public safety events and natural disasters. We also investigate research efforts in the network-side communication technique of DWN deployment via the aid of ground mobile BS, UAV-based mobile BS, and a hybrid network, as shown in Fig. 6.

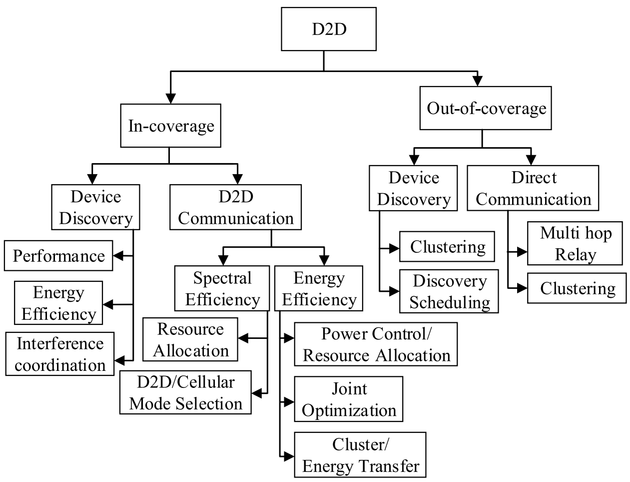

FIGURE 4. User-side communication technique: D2D.

Third, we illustrate challenges and future research directions in public safety networks. To be specific, the challenges on the user-side and network-side consist of D2D, DWN deployment, security and resilience, and performance evaluation. In addition, future directions address the outlined challenges, including the D2D design, DWN use, threat assessment, and the integration of modeling, simulation, emulation, and testbed. We also outline needs and challenges in integrating state-of-the-art communication and computing technologies, including Internet-of-Things (IoT), cloud computing, and 5G, to improve interconnectivity, computing, and network for public safety.

The remainder of this survey paper is organized as follows: In Section II, we define the layered structure of the public safety, and describe the key elements, as well as the user-side and network-side communication techniques in the communication layer. In Section III, we conduct a systematic survey of D2D communication as a user-side solution for public safety communications. In Section IV, we investigate the network-side solution of dynamically deploying network infrastructure for public safety. In Section V, we outline a number of challenges in D2D, DWN, emergent technologies, and highlight potential solutions. Finally, In Section VI, we provide final remarks.

II. PUBLIC SAFETY OVERVIEW

In this section, we overview the critical components in public safety, including physical objects, time-critical information delivery and public safety services via a layered structure in Fig. 1. Notice that our survey focuses on communication techniques, which are critical to support time-critical information delivery.

A. OVERVIEW

Fig. 1 shows a layered structure, presenting the public safety system's key components. The Physical Object Layer (POL) represents the physical public safety objects or hardware, including monitoring sensors, surveillance cameras, rescue equipment, mobile phones, and walkie-talkies, to name a few, which are critical to supporting situation awareness and crisis communication, as well as rescue processes. Above that, the Time-critical Information Delivery Layer (TIDL) affords data distribution for situation awareness and crisis communication, for both first responder teams and victims. Notice that various communication networks, including cellular networks for mobile phone communication, wireless sensor networks for sensor communication, vehicular networks for vehicular communication, and so on, play key roles in supporting the data transmission and information sharing between both first responder teams and victims. With support from physical objects and information delivery, in the Public Safety Services Layer (PSSL), a number of services exist that are designed to analyze, understand, and respond to public safety events and can be carried out effectively and efficiently toward the prevention and reduction of losses, including fire and rescue services, police and security services, etc.

Notice that the three-layer structure is generic and designed to present the key components in the public safety system comprehensively, and to segregate these components into reasonably separate domains. The public safety services layer provides the major services to coordinate public safety events, direct necessary resources, and prevent losses in various public safety scenarios. The TIDL provides the information delivery during crisis communication. The POL describes physical objects that support the information sharing and response activities.

B. PUBLIC SAFETY SERVICES LAYER

In PSSL, we investigate the critical public safety services that supports public safety response to address possible threats to the well-being of the general public and to better understand the public safety scenarios. The investigation of PSSL focuses on what public safety services are provided during the three phases of public safety response (i.e., the disaster prevention, emergency management, and disaster relief). To begin with, we first categorize public safety scenarios into two cases: (i) predictable and (ii) unpredictable, for both public safety events and natural disasters. As a few examples, public safety events such as the Olympic games and, large-scale gatherings, and concerts are considered predictable, whereas terrorist attacks, man-made structure failures, and human-induced disasters are considered unpredictable. Also, some natural disasters (e.g., hurricanes and floods) are reasonably predictable, and occur under a limited duration. Meanwhile, earthquakes and wildfires are examples of typically unforeseen natural disasters.

TABLE 2. Public safety response demands.

Response Efforts		Disaster Prevention	Emergency Management	Disaster Relief
Public Safety Events	Predictable	High	High	Low
	Unpredictable	Low	High	Medium
Natural disasters	Predictable	High	Low	High
	Unpredictable	Low	Low	High

Public safety services generally approach to the two categories of public safety scenarios differently. As shown in Table 2, in predictable public safety scenarios, the various emergency services departments (police, fire, rescue, etc.) put significant effort into disaster prevention. For instance, police departments schedule more police officers to enforce the safety of gathered people and provide security for large events. Fire and rescue departments are also on hand, and prepared for possible incidents. Thus, efforts with high preparedness in the prevention phase shall be in place quickly and effectively in the emergency management phase. This means efforts in the disaster relief will generally not be as high.

In unpredictable public safety events, law enforcement departments may not be fully prepared, due to time limitations and abruptness of the events. Thus, most of the emergency response efforts shall come in the emergency management phase and disaster relief phase to manage response and mitigate losses. On the other hand, in the predictable natural disasters, law enforcement and first responders shall be well prepared to coordinate efforts and minimize the risk of possible loss. Due to the scale and strength of natural disasters, a significant number of efforts need to be conducted in the aftermath of disasters. For unpredictable natural disasters, the disaster relief phase demands significant efforts to be in place rapidly.

C. TIME-CRITICAL INFORMATION DELIVERY LAYER

The pyramid structure in Fig. 2 presents the methodology that enables time-critical information delivery in public safety response. The pyramid structure consists of information delivery services (i.e., situation awareness and crisis communication) in the TIDL. In the communication application layer, we consider a number of key services (location-based service, mission critical voice, and real-time video), which have rich content and various objects to support the information delivery services. The communication techniques layer, which consists of the network-side DWN (ground/space deployment and 3D DWN) and user-side D2D (device discovery and D2D communication), is capable of establishing effective and resilient connections among victims and responders in public safety scenarios.

In the TIDL, the services of situation awareness and crisis communication that coordinate and manage the efforts denoted above for the public safety services from law enforcement and emergency response departments consist of three phases: (i) *information collection*, (ii) *information analysis*, and (iii) *information exchange*. For information collection, the various detecting sensors, alert subsystems, surveillance subsystems, and personnel play key roles in collecting the information before, during and after the public safety scenarios. For example, in disaster prevention, the information center collects the disaster information from all possible sources and initiates the necessary responses. In emergency management, the information center continues monitoring the situation dynamics and releases updated responses. At the disaster relief phase, the rescue responses disseminate in a timely manner. The information exchange among the different law enforcement efforts improves the efficiency and effectiveness of public safety services. Especially, in the event of natural disasters, traditional communication infrastructures may be dysfunctional or damaged, and local information exchange can be critical to the disaster relief.

In the communication application layer (CAL), the key applications (i.e., location-based service, mission critical voice, and real-time video) are necessary in information collection, analysis, and exchange for critical communication services. In the following, we describe those applications in detail.

1) MISSION CRITICAL VOICE

Mission critical voice provides time-critical voice transmission to support situation awareness and crisis communication in public safety services. Mainly, the voice service consists of direct talk, Push-To-Talk (PTT), group call, emergency voice alert, etc. Direct talk provides direct communication in a unit-to-unit manner out-of-coverage of the network. PTT is the instantaneous multicast or broadcast of the critical information in one or multiple talk groups. Leveraging the PTT function in the LTE network has the potential benefit of better QoS from the broadband cellular networks. Group call indicates one-to-many communication inside a communication group. With mission critical voice delivery, the efficiency of the situation awareness and crisis communication leads to quicker and more effective response.

2) LOCATION-BASED SERVICE (LBS)

LBS indicates the 3D geo-localization, mapping, navigation, interoperability, and others, and enables the first responder teams to carry out efforts effectively. Particularly, 3D geo-localization indicates the location of targets by address, with additional information (the floor, height, etc.) that can accurately describe the target's geolocation [49], [141]. Especially, in an indoor environment, the 3D geo-localization appears more accurate in terms of allocating targets with different altitudes in complex environments. Mapping in public safety indicates the interoperable ''base map'' that allows the cross-agency collaboration, indoor and outdoor location, data input, etc. Navigation indicates route planning, organization, and real-time location data delivery for the responder teams. In addition, the LBS interoperability enables data collection, data transmission and device display.

3) REAL-TIME VIDEO

Video contains authentic and meaningful information in a high-density form, and can be extremely helpful towards determining situation awareness and directing crisis communication in public safety scenarios, containing significant volumes of visual and audio content. Real-time video delivery requires large bandwidth of the communication network, as well as large network resources for serving large-scale emergencies. Real-time video services improve, the accuracy, effectiveness, and efficiency of the response activities.

In the communication techniques layer, we consider D2D and DWN as representative user-end and network-end solutions. The detailed study and comparison of techniques in D2D and DWN are provided in Sections III and Section IV, respectively. Fig. 3 illustrates a representation of the structure of communication techniques for public safety.

D. PHYSICAL OBJECT LAYER

The physical object layer (POL) indicates the group of physical objects that participate in and support response activities and communications, including monitoring/communication devices, public safety equipment and emergency response personnel. The monitoring/communication devices are the specific sensors, cameras, User Equipment (UEs), and Base Stations (BSs), supporting situation awareness and crisis communication. The monitoring/communication devices play critical roles in improving the effectiveness and efficiency of disaster prevention, emergency management, and disaster relief.

POL supports forecasting such a hurricane, where numerous deployed air pressure sensors and wind speed sensors monitor the atmospheric and weather conditions for the collection and determination of hurricane conditions. In addition, to gain awareness of a public safety related scene, such as the Baltimore riot, a number of cameras on the street can observe the behaviors of crowds, what individuals may be carrying, and their direction of movement, and others. Thus, the UEs and BSs form a communication system that can deliver critical information to people and law enforcement personnel to prevent losses. The public safety equipment consists of police vehicles/watercraft for rescue, fire extinguishers, and many other products. The equipment needs to be deployed and operated by the law enforcement and rescue personnel (police, fire and rescue, and others) to serve in the responses of disaster prevention, emergency management and disaster relief. To improve the situation awareness of public safety scenes, IoT devices render useful information [89], [132].

III. COMMUNICATION TECHNIQUES AND EXISTING PROGRESS: D2D COMMUNICATION FOR PUBLIC SAFETY

In this section, we review the D2D communication techniques at the user side for public safety. We discuss approaches for in-coverage and out-of-coverage D2D to deal with the aftermath of various public safety scenarios. We also review the existing progress in D2D communication development.

A. OVERVIEW

Recall the two recent public safety scenarios: 2015 Baltimore Riots and 2017 Hurricane Harvey, which incurred the typical consequences for the communication in public safety scenarios (i.e., in-coverage and out-of-coverage). These public safety events caused the cellular network to be overloaded or infrastructure damaged, which lead to hindered communication. In such situations, the victims are not able to communicate outside of the affected area, and the situation and degree of emergency cannot be observed by the outside rescue teams. To connect affected areas and the outside world, the user-side solution established links to nearby users regardless of the overloaded or damaged network infrastructure. As a user-side solution, D2D communication recovers deficient or damaged communications in disaster situations without the assistance of network infrastructure, and provide communication services for public safety responders.

We now present a taxonomy to investigate and study the existing research efforts on D2D, as shown in Fig. 4. The taxonomy investigates two subareas: (i) *D2D in-coverage*, and (ii) *D2D out-of-coverage*, to cope with the public safety events and natural disasters individually. Then, in each subarea, we review device discovery and D2D communication as the two key elements. Device discovery indicates the discovering of nearby devices to establish direct communication links. Under the coverage of the cellular network, three factors include measuring device discovery schemes, these being performance (e.g., discovery probability), energy efficiency, and interference coordination (spectrum resource management). Existing research efforts on device discovery for D2D communication consider factors such as spectral efficiency and energy efficiency [140]. Related to spectrum efficiency, the resource allocation schemes and mode selection are important efforts. Similarly, the power allocation, resource allocation, joint optimization of both, and cluster/energy transfer are important research efforts towards energy efficiency. For out-of-coverage device discovery, research efforts mainly consist of clustering and discovery scheduling.

B. D2D IN-COVERAGE

In the following, we review the techniques relevant to D2D in-coverage.

1) DEVICE DISCOVERY

Device discovery is a key enabler to initialize D2D communication, which requires the accurate and efficient detection of the proximate devices. Specifically, in emergency areas, the device discovery performance measures (i.e., discovery probability, time efficiency, and resource efficiency) are challenging due to the complex communication environment, and limited energy and spectrum resources. Generally, device discovery schemes can be categorized as either network-centric or device-centric, which result in different usage of the discovery resource block (DRB) in the D2D in-coverage case. In the network-centric discovery scheme, the network assigns the DRB to each UE in a centralized way. In contrast, in the device-centric schemes, the UE selects DRB from the resource pool in a distributed way.

In the following, we conduct an investigation of research works on network-centric device discovery schemes from the following three key categories: (i) *performance*, (ii) *energy efficient*, and (iii) *interference coordination*. It is worth mentioning that the categorization relies on the tradeoffs between the investigated resource (i.e., energy and spectrum) and the discovery performance.

a: PERFORMANCE

Network-centric device discovery achieves the best possible discovery performance due to its global coverage and better network knowledge [54], [145]. The higher level of knowledge about network information in the Evolved Packet Core (EPC) can help the EPC to better estimate the probability of proximity of two UEs, and thus improve the discovery probability [54]. For example, Xenakis *et al.* [154] analyzed the discovery probability of two D2D UEs under different knowledge levels of the network layout (i.e., full or partial).

b: ENERGY EFFICIENT

Periodical discovery signal broadcasting improves energy efficiency in the discovery phase compared with continuous discovery signal transmission. In addition, location-based device discovery can reduce the energy consumption by only allowing the discovery when devices are in approximate range. To this end, Prasad *et al.* [122] leveraged the concept of pre-defined proximity area to avoid continuous discover while maintaining the same level of accuracy. The pre-defined proximity area means that the geographic area includes multiple UEs with the same ProSe service. Within the proximity area, the UEs have higher discovery probability among each other.

To leverage the concept of proximity area, dynamic location tracking is the key technique, which records the information of UE, cell ID, application, grouping, and others. The UE turns on the ProSe discovery function, announcing and monitoring nearby UEs when it gets into the proximity area. The UEs in the proximity area discover each other and set up connections in a high discovery probability. After leaving the proximity area, the UE turns off the ProSe discovery function to save energy. In addition to the location-based discovery, the careful design of the discovery beacon can significantly improve energy efficiency. The traditional packet-based discovery schemes are complex and resource-intensive due to the large size of the discovery packets. To address this problem, Zou *et al.* [174] proposed the signature-based discovery scheme, in which the discovery signal contains less UE information to obtain a higher resource efficiency and discovery performance.

c: INTERFERENCE COORDINATION

To mitigate the interference between two UEs during discovery, Hu [70] proposed a network-centric location-based resource allocation scheme. The network assigns the discovery resource blocks (DRBs) to the UE with the consideration of its location to minimize mutual interference. For instance, the reassigned DRB to the UE that has maximum distance to nearby UEs so that spatial reuse can be improved. Their experimental results demonstrated the effectiveness of the location-based scheme over the device-centric scheme (i.e., each UE picks the DRB randomly). Nonetheless, the limitations of this work include the additional overhead from location reporting, and the necessary coverage of the existing network. To mitigate the inter-cell interference (ICI), caused by the use of the same frequency resources from UE and cellular network, Babun *et al.* [19] leveraged the Almost Blank Subframes (ABS) in the context of D2D discovery. The ABS enables transmission mutation in the subframes to reduce interference. Extensive evaluations demonstrate the performance improvement on device discovery with different ABS rates under various scenarios.

It is worth mentioning that Table 3 provides the detailed description, investigation and comparison of key device discovery approaches (i.e., localization estimation, discovery message broadcasting, and clustering). Localization estimation indicates that the control center collects various localization information, including AoA, receiving power, etc., and then performs the location estimation for UEs. The discovery message broadcasting indicates that the control center announces and listens to discovery messages. The clustering-based device discovery involves the distributed clustering process to discover UEs with the same interests in a given geographical region.

TABLE 3. Categorization of schemes for device discovery.

Device Discovery Approaches	Description	Representatives	Pros	Cons
Localization Estimating	The UE's location is estimated by the combination of localization information (e.g., AoA), transmission and received power	[54], [154]	Does not require additional discovery resources (i.e., channel, power supply)	Not applicable in out-of-coverage scenarios
Discovery Message Broadcasting	The UE broadcasts its location information, cell ID, grouping, etc., to nearby UEs through discovery message	[174], [122]	Not constrained by network coverage Can perform in a self-organizing way	High energy consumption due to broadcasting Not optimal discovery performance
Clustering Based	UE can form clusters based on its location or service interests The discovery can be performed cluster-wise	[100]	Effective in out-of-coverage scenarios with a large number of UEs	Needs efficient algorithms in order to achieve optimal discovery performance.

2) D2D COMMUNICATION

Research on D2D communication in conventional cellular networks for commercial use is extensive, and tends to show improvements in the capacity, reliability, extensibility, and efficiency of the network. The taxonomy design is extremely important in classifying and integrating the massive research efforts on D2D communication. Existing taxonomy designs are based on the purposes of D2D communication (capacity improvement, coverage extension, and others), resource utilization (in-band D2D and out-band D2D), network performance (network delay, resource efficiency, system throughput, and others), and applications [17], [54], [90].

In the context of public safety, the proposed taxonomy of D2D communication is cellular-assisting and infrastructure free. In small-scale public safety emergencies, cellular-assisting D2D communication can be applicable to serve the purpose of traffic offloading with the functional cellular system. In the large-scale natural disasters, the infrastructure-free D2D communication can provide communication service for disaster relief when the cellular system is partially or fully dysfunctional due to the physical damage or network congestion.

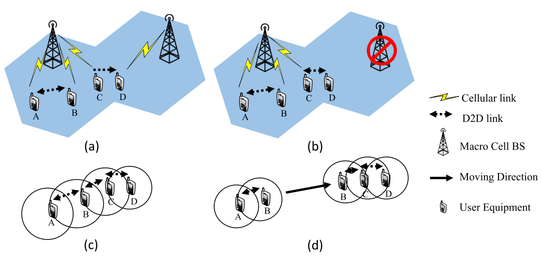

FIGURE 5. (a): Data sharing (A-B), Traffic offloading (C to D), (b): Extend coverage (C-D), (c): Ad Hoc networking (A-B-C-D), (d): Mobility based data delivery (B as moving terminal).

Particularly, in the context of public safety, the D2D communication has two key functions, traffic offloading and coverage extension, as shown in Fig. 5. Particularly, Fig. 5 (a) illustrates an example of traffic offloading, and Fig. 5 (b) shows the coverage extension. Fig. 5 (c) and Fig. 5 (d) show examples of infrastructure-free D2D connection. In the following, we review the cellular-assisting D2D communication with two key components: (i) *spectral efficiency* and (ii) *energy efficiency*, in detail.

a: SPECTRUM EFFICIENCY

Table 4 illustrates the categorization of the key approaches to improve spectrum efficiency, including spectrum resource allocation, D2D/cellular mode selection, etc. In addition, the description and comparison are illustrated.

Resource Allocation: Sharing spectrum resources between D2D and cellular communication can improve spectral efficiency in cellular networks. Effective spectral management schemes are critical to avoid interference between D2D to cellular and cellular to D2D [161], [175]. For instance, Yu *et al.* [161] conducted analysis on the optimal power control and resource allocation under two resource sharing modes (i.e., non-orthogonal and orthogonal) in a centralized manner. For the non-orthogonal mode, in which cellular UE and D2D UE use the same spectrum resource, the optimum power control was derived towards the sum-rate maximization with various constraints. For the orthogonal mode, in which D2D obtains dedicated resources, the optimum closed-form resource allocation between the D2D UE and cellular UE achieves cell throughput. In addition, Le [82] addressed the fairness issue in resource sharing between the cellular UE and D2D UE. The author proposed a two-phase allocation scheme that can be used to carry out the cellular UE and D2D UE resource allocation separately (i.e., fair resource allocation and primary-secondary sharing).

D2D/Cellular Mode Selection: There are a number of schemes developed to address D2D/Cellular model selection [27], [38]. For instance, towards the maximization of the sum-rate by the utilization of D2D communication in the overlay network, Chen *et al.* [38] proposed the interference limited area and resource allocation scheme to constrain the interference from cellular UE to D2D UE in the downlink. The interference limited areas were first derived for D2D-Tx and D2D-Rx to control the interference with the constraints on interference over thermal level. Within the interference limited areas, the resource dedicated to the cellular UE will not be shared with the D2D UE to suppress interference.

Towards resource sharing in the underlay non-orthogonal mode, ElSawy *et al.* [52] proposed an analytical framework to model the mode selection (i.e., the mode selection of the direct communication or the cellular communication) of the UE with regard to the network performance. Lee *et al.* [83] proposed the centralized and distributed power control schemes for the D2D UE underlaying to improve the network throughput. In addition, Lin *et al.* [91] addressed the issues of D2D spectrum sharing-based D2D mode selection

TABLE 4. Categorization of schemes for spectrum efficiency.

Spectrum Efficiency in D2D	Description	Representatives	Pros	Cons
Spatial Domain	Design the areas that restrict interference due to spectrum sharing from cellular UE to D2D UE to improve the system performance and spectrum efficiency	[38]	The spatial domain approach is effective and the implementation is cost-friendly	The approach relies on global knowledge of the interference level of cellular UEs Due to the UE mobility, the performance may be degraded
Resource Allocation	The scheduling algorithms of the Resource Blocks (RBs) can reduce the interference among cellular UE and D2D UE, and thus improve the spectrum efficiency	[175], [121]	The design of resource allocation algorithms is driven by interference, as well as many other system performance metrics	The effectiveness is bounded by the amount of spectrum resource
Power Control	The power control on the transmission in non-orthogonal channels can avoid interference from spectrum sharing and improve the spectrum efficiency	[52], [83]	Power control can be effective for spectrum sharing on the same frequency band	The algorithm design is complex
Joint Power Control and Resource Allocation	The power control method and resource allocation can be optimized jointly to improve the spectrum sharing and system performance	[161], [27]	Can obtain better performance in system level The joint optimization problem is more general and applicable to many scenarios	Complexity in designing the joint optimization problem as well as the implementation

TABLE 5. Categorization of schemes for energy efficiency.

Energy Efficiency in D2D	Description	Representatives	Pros	Cons
Power control	The power control scheme can allocate power consumption towards energy efficiency with regard to system performance (throughput, delay, etc.)	[153]	Power control schemes can directly improve the energy efficiency	Power control is usually combined with D2D system performance as a tradeoff problem
Joint power control and resource allocation	Joint optimization of the power level of each sub-channel of UE can determine the optimal spectrum and power allocation	[129], [72], [148], [139]	The joint optimization problem can be utilized to address the tradeoff problem of energy efficiency and various performance objectives The performance of the energy efficiency is optimum	The computing and implementation complexity rises when number of the D2D UE increased
Clustering	The clustering procedure, including CH selection and grouping, can improve the energy efficiency due to group computation and reduced beacon transmission	[55]	The clustering of D2D communication is efficient in reducing the cost of communication	The performance may not be optimal when lacking global knowledge The implementation complexity also presents challenges
Wireless Energy Transfer	Enabling the wireless powered communication network (WPCN) that can effectively address the energy constraints in public safety communication	[42]	The effectiveness of providing a sustainable power supply can address the battery limitation issues in public safety scenarios	The implementation complexity and cost is challenging, as well as the security issues of the energy transfer

in overlay and underlay topology. A proof-of-concept analysis and evaluation on the D2D communication, as well as the cellular communication in both overlay and underlay showed promising results.

It is worth mentioning that we compared the key approaches to improve the spectrum efficiency for D2D communication in Table 4. Spectrum allocation is a straightforward approach to manage spectrum resources between D2D UE and cellular UE to avoid interference to both sides. In network-centric D2D communication, resource sharing can be managed in a centralized way with regard to the fairness, QoS, and others [82], [121], [161], [175]. Additionally, mode selection (i.e., D2D/cellular mode of UE) enables the UE to be operated in either D2D or cellular mode. In spatial domain schemes, the geographic interference-limited areas are leveraged to control interference [38]. Power control schemes, in contrast, mitigate the interference to other UEs via the control of the transmitter power (e.g., ON/OFF control [52], [83]). Finally, joint optimization of power control and resource allocation can improve the performance of cell throughout via mode selections and the RB assignment [27], [161].

b: ENERGY EFFICIENCY

Due to the battery limitations of UEs, energy efficiency has attracted a significant amount of research. Particularly, the centralized schemes toward energy efficiency in the D2D overlay communication were investigated in [72], [139], [148], and [150]. Table 5 illustrates the categorization, description and comparison on the key approaches toward energy efficiency in D2D communication, including power control, joint power control and resource allocation, clustering, and wireless energy transfer.

Power Control: With respect to power control, a number of research efforts have been carried out [98], [142], [147], [148], [150], [172]. For example, Zhou *et al.* [172] proposed a game theory-based scheme to address the resource allocation problem for energy efficiency maximization (i.e., with the consideration of interference). The underlying assumption is that both the D2D UEs and cellular UEs are selfish (i.e., maximizing energy efficiency). Considering the significant energy consumption of the multimedia service in D2D communication, Wu *et al.* [150] proposed a game theory-based framework and designed a distributed coalition formation algorithm to model and analyze the joint mode selection and resource sharing towards the optimal energy efficiency.

Joint Optimization of Power Control and Resource Allocation: With respect to joint optimization, there have been several notable research efforts [72], [128], [129], [139], [142]. For example, Sheng *et al.* [129] studied the joint optimization of the tradeoff between energy efficiency and latency. The optimization objective is the energy efficiency with the constraints of average power, interference, and stability. They using fractional programming as the solution to address this optimization problem. Jiang *et al.* [72] formulated the joint allocation problem as a non-convex optimization problem, and transferred it into the subtractive form equivalent optimization problem with a tractable solution.

Cluster and Energy Transfer: Some studies have been devoted to clustering and energy transfer [42], [55]. For example, Fodor *et al.* [55] proposed a network controlled clustering procedure for D2D communication. The clustering procedure, which contains the Cluster Head (CH) selection and grouping, tends to improve the performance of the coverage ratio and energy efficiency. Notice that the CH plays the role of resource management and handles communication between inter- and intra-clusters. The cluster grouping was formed by the non-CH UEs, based on their received quality of beacon signals. Two Stackelberg games model the interference pricing and the energy trading. The optimal strategies for the utility optimization of both UE and BS, and the Stackelberg equilibrium was derived.

C. D2D OUT-OF-COVERAGE

Without the presence of network infrastructure, the device-centric discovery schemes are applicable to discover out-of-coverage devices, due to their self-organizing capabilities. Nonetheless, the device-centric schemes may cause local-optima and interference due to a lack of global knowledge compared to the network-centric schemes. In particular, the D2D UE plays two roles in proximity discovery: (i) *announcing* and (ii) *monitoring*. In the announcing role, the UE transmits proximity discovery messages periodically. In the monitoring role, the UE listens to the messages from the announcing UEs and responds to them.

1) DIRECT DISCOVERY

The discovery performance (i.e., discovery probability, resource efficiency) faces the challenges of both limited resources and high device density in public safety emergencies.

a: CLUSTERS

One possible way to address these challenges is to carry out the clustering process in the direct discovery phase. The D2D UEs form clusters with proximity on geolocations or in the interests of service. For instance, the rescue team may want to directly communicate with their team member instead of all other people in the area. The clusters have two types of operations: (i) master-slaves, and (ii) the uniform-UE. The master-slaves indicates that only a limited number of UEs can be the Cluster Head (CHs) for connection and resource management. The uniform-UE type indicates that every UE can be the CH and perform the clustering and management.

Relevant to clustering, Lu *et al.* [100] proposed a three-phase clustering scheme for device discovery in out-of-coverage scenarios (i.e., CH selection, UE grouping, and connection). In the CH selection process, the probability transmission avoids collision during discovery. Also, each UE stores the local information of nearby UEs. By the local awareness, the UE with the highest discovery performance will be selected as CH. In the UE grouping, the CH will broadcast its discovery performance with beacons. The UEs with lower discovery performances will set up connection with the CH as slaves. By using the clustering scheme for the device discovery, the discovery probability, resource efficiency and network performance can be improved.

b: DISCOVERY PROCESS

Collisions during the discovery phase could degrade the discovery performance in D2D direct discovery [64], [111], [170]. For instance, to avoid collisions of two discovery messages, Zhang *et al.* [170] applied the random back-off strategy in device discovery to reduce collisions and increase discovery probability. Generally, when two UEs select the same resource block and transmit discovery messages, a collision could occur and result in discovery failure. Then, with the random back-off, the UE randomly selects a back-off time to retransmit the discovery message. Thus, the D2D discovery probability increases. In addition, Griffith *et al.* [64] proposed a theoretical model for analyzing the process of UE discovery of all other UEs in a group by Markov chain process. The theoretical model captures the distribution of discovery time, which is highly dependent on the group size and discovery resources. Finally, with the derived model, the maximum group size can be determined for a given discovery time and discovery resources.

2) D2D COMMUNICATION

Due to the lack of network infrastructure and limited transmission distance of UEs, D2D communication is critical for out-of-coverage devices. Multi-hop relay, which provides the receive-and-forward function, is a critical communication technique to support public safety communications, as it improves the connection, coverage, and capacity of D2D communication. In addition, clustering is an important technique for out-of-courage D2D communication.

a: MULTI-HOP RELAY

Relevant research efforts can be categorized as relay selection, multi-hop relaying, and relay assignment. To be specific, the relay selection schemes consider receiving power, throughput, and QoS. In addition, the multi-hop relaying schemes (the shortest-path, maximum-rate, interference-aware, etc.) support various application scenarios. The relay assignment focuses on the performance maximization through different mechanisms, including aggregation, max-min UE performance, and greedy [86], [115], [167]. For instance, Nishiyama *et al.* [115] systematically reviewed the multi-hop D2D in the disaster area, which enables communication among mobile devices without functional network infrastructure. Particularly, the key techniques that played important roles to realize multi-hop D2D were investigated, including air interference, routing protocol, interconnectivity, security and compatibility of the various operating platforms. In addition, an experimental prototype of the multi-hop D2D to support emergency communication was developed and tested in a real-world testing environment.

b: CLUSTERING

Regarding clustering, Laha *et al.* [81] proposed a clustering algorithm to improve energy efficiency by introducing the concept of pseudo groups in the multi-hop

D2D communication system. One assumption is that the close distance transmission reduces energy consumption. The general processes of the multi-hop routing protocols include device grouping, group owner selection, and group owner transfer. The selected group owners establish the connection between two groups of devices, and act as terminals for the far-away devices. The aggregated traffic from the entire group propagates through the group owners.

Notice that D2D communication for out-of-coverage UEs is more challenging than in-coverage due to the lack of global knowledge of UEs and limited transmission power. In this case, clustering-based schemes and multi-hop relay-based schemes, which provide the functions of UE grouping and message forwarding, are the key approaches. The clustering-based scheme can form different groups and connect individual groups via cluster heads. In this way, network coverage and energy efficiency can be greatly improved [81]. The multi-hop relay-based scheme is another important technique to extend the communication distance of D2D via the receive-and-forward function. Relay selection and multi-hop routing are critical problems for multi-hop relays in D2D communication [115], [167].

D. EXISTING PROGRESS IN D2D

In the following, we further discuss existing progress in the development and implementation of D2D, including the standardization, D2D over cellular network and non-cellular network.

1) STANDARDIZATION OF D2D

The standardization of D2D is critical to improving the interoperability of D2D techniques in the emerging marketplace, and can further improve the stable and rapid evolution of D2D techniques in wireless networks. In this subsection, we review the standardization progress of D2D communication techniques in wireless networks. Lin *et al.* [90] conducted an overview on the standardization activities of D2D in LTE cellular networks by 3GPP. From the perspectives of both network performance and cost-effectiveness, D2D communication brings multiple benefits to the LTE cellular network. Particularly, D2D communication can improve network throughput, end-to-end delay, resource use efficiency, energy efficiency, etc. D2D also supports a number of applications, such as social networking services, data sharing, gaming, and so on. Thus, enabling D2D in LTE can greatly improve network performance and commercial competitiveness.

In LTE Release 12, the 3GPP specified use cases, system architecture, channel models, performance evaluation, and others for D2D as the 3GPP Proximity Service (ProSe) [4], [5]. Broadly, the use cases for ProSe service are public safety communication under three cases (i.e., all BSs are available, partial BSs are available, and no BSs are available). These cases cover the three scenarios in D2D services (i.e., in-coverage, partial-coverage and out-of-coverage), which represent the range of UEs to be covered by LTE cellular networks. D2D discovery and D2D communications are the critical functions to support ProSe D2D service. The D2D system architecture that supports the ProSe service, including D2D discovery and communication, was studied by 3GPP in [4] and [6]. The reference architectures of non-roaming, roaming, one-to-many communication, and others were introduced in [5]. In addition, some 3GPP factors investigations include the dual mobility, low antenna height, inter-link correlation, etc., to make the D2D propagation channel model more realistic to D2D scenarios.

In LTE release 13, the 3GPP further enhanced and extended D2D/ProSe and mission critical communication use cases, alongside other subjects, including the spectrum bands, resource efficiency, small cells, HetNet, and others. Particularly, the public safety functionalities initiated in Release 12, including the LTE-based D2D discovery and D2D communication, public safety requirements, etc., continued in Release 13. Release 13 also enhanced D2D communication in coverage extension for partial coverage and out-of-coverage scenarios, and public safety use cases, such as mission critical push-to-talk (MCPTT), and voice and video applications. For instance, the coverage extension for the ProSe can be improved thorough relays (i.e., UE-Network relays and UE-UE relays).

2) D2D OVER CELLULAR NETWORK

Given the 3GPP standardization progress on the ProSe service, D2D communication over cellular network (e.g., LTE) becomes feasible [50], [84], [134], [151]. For example, Lei *et al.* [84] studied usage cases and business models, and provided design considerations for D2D communication in the LTE network. The D2D use cases consist of the local voice service, data service, multimedia sharing, gaming, machine-to-machine communication, and more. The business models referred to the services that have business values, including identity management, QoS, security, context information, and so on. The power control and resource allocation mitigate interference between cellular communication and D2D communication. Tang *et al.* [134] studied the neighbor discovery problem of D2D in LTE networks. The potential discovered D2D UE resulted from listening to cellular uplink channels. When the discovering UE finds the transmitters to exist in proximity, these transmission UEs can be identified as potential D2D UEs. This work conducted statistical models for the joint neighbor discovery and D2D channel estimation in the structure of sounding reference signal (SRS) channel. Various discovery methods were discussed and performance evaluations were conducted in the LTE environment.

3) D2D OVER NON-CELLULAR NETWORK

The rapid increase of data traffic from resource consuming applications, such as video streaming, gaming, etc., over the past few years and for the foreseeable future pose great challenges to wireless networks. The enabling of direct data sharing between devices for such applications can reduce the traffic load to APs and improve overall user experience.

TABLE 6. Categorization of schemes for DWN deployment.

Deployment approach	Description	Representatives	Pros	Cons
Compound System	A mobile site, which consists of power, network infrastructure and recovery services, can be deployed when needed	[7], [110]	The great durability of the complex site can improve the recovery performance, and support related activities	Due to the size, the accessibility and mobility is low, and may not be applicable in some public safety scenarios
Automated Ground mobile BS Network	For large scale emergencies, deploying the COWs to support the heavy network traffic	[31], [124]	Compared with compound system and UAV, the durability, payload, and the mobility are reasonable	The accessibility is highly reliant on the ground accessibility
Multi-UAV-based Network	The UAV can be deployed rapidly for various purposes, and benefits from the high accessibility and mobility	[106], [107], [157]	The high accessibility in the air Better communication channel quality for air-to-air and air-to-ground	Due the limited payload and energy supply, the durability is one main challenge
Hybrid deployment	Utilize both ground mobile BSs and UAVs in-the-air to form a cooperative network that can improve the system capacity and coverage.	[103], [102], [18]	Both the accessibility and durability of the DWN can be improved	The cooperation, implementation, and efficiency of the hybrid network are challenging The accessibility of mobile BSs rely on ground accessibility

Supported by WiFi technology, WiFi direct enables the direct communication between D2D UEs. With the WiFi direct mode, a UE discovers candidate UEs and establishes D2D links through sensing and accessing available channels. Particularly, the UE that plays the role of group owner connects various D2D UEs and forms a group to carry out information sharing [21]. For instance, Conti *et al.* [43] conducted various experiments to evaluate the discovery and grouping performance with different protocols and configurations under a WiFi direct framework.

In public safety application scenarios, the failure of mobile networks (e.g., congested or damaged) causes the UEs to be out-of-coverage and further affects network connectivity. To address such a problem, the establishment of D2D links to reroute traffic to nearby access points (APs) is one viable method. The UEs can establish D2D links to reroute the data through the out-of-coverage UEs to the available APs. In order to reroute the traffic, the network elements (i.e., APs and UEs) shall first exchange availability information, capacity information, and others. Then, the optimal paths selection supports rerouting. For example, Karvounas *et al.* [74] proposed the IEEE 802.11s-based testbed to construct D2D communication for coverage expansion.

IV. COMMUNICATION TECHNIQUES AND EXISTING PROGRESS: DWN DEPLOYMENT FOR PUBLIC SAFETY

In this section, we review the DWN as a critical network-side communication technique for public safety. In particular, we investigate the approaches for ground mobile BS, UAV-based mobile BS and hybrid networks. We also review the existing progress in UAV-based network.

A. OVERVIEW

Recall that two public safety scenarios (i.e., Baltimore Riots in 2015 and Hurricane Harvey in 2017) led to overloaded networks and damaged network infrastructure. In such a situation, in the affected area, the normal communication functions of UEs, including data transmission and streaming, are no longer functional. To establish a temporary/dynamic communication network, a portable network infrastructure establishes communications for out-of-coverage UEs and improve network capacity. Ground-based vehicles and Unmanned Aerial Vehicles (UAVs) are the key payload transport technologies, carrying light-weight cellular base stations to the emergency area to rapidly support massive communication. As an area of significant interest, there have been a number of research investigations into the use of mobile base stations to support network infrastructure.

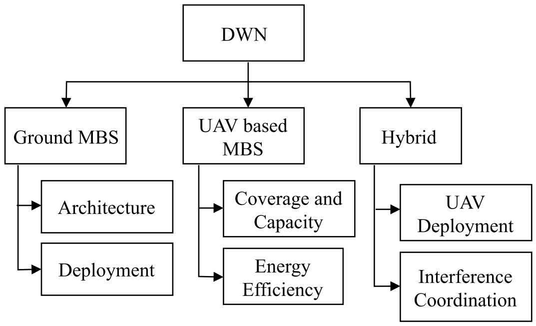

FIGURE 6. Network-side communication technique: DWN deployment.

In the following, we review research efforts on DWN deployment strategies for ground mobile BSs, UAV-based mobile BSs, and hybrid network that enable the cellular network establishment in emergency areas. Particularly, we design a taxonomy, as shown in Fig. 6, to understand and categorize the state-of-the-art in DWN deployment as a network-side communication solution. In addition, we illustrate the categorization, description and comparison of the schemes toward DWN establishment in Table 6. Further, we review the standardization progress for the UAV-based network, the UAV-based network over cellular and non-cellular network, and the UAV-based network in real-world implementation.

B. GROUND MOBILE BS

1) ARCHITECTURE

Various network architectures were developed to serve the different application scenarios of mobile BSs [7], [39], [110]. For instance, Morrison [110] proposed a mobile recovery site deployed for disaster response. The proposed mobile recovery site emergency responder system consists of the combined telecommunication infrastructure, customizable software applications, and responder team. In addition, Chen *et al.* [39] proposed a network architecture for the dedicated public safety network, which deploys stationary BSs to support light traffic from routine activities, and mobile BSs to support heavy traffic from incidents. The premise was that the mobile BSs would be equipped nationwide and dispatched by vehicles when needed. The study conducted throughput analysis of both the stationary BSs for routine activity and mobile BSs for disaster emergencies.

2) DEPLOYMENT

Dynamic deployment can adapt to the traffic variances under large-scale public safety emergencies, and help in offloading peaks in traffic [31], [124]. For instance, Bhattarai *et al.* [31] proposed a dynamic deployment scheme to optimize the deployment of mobile BSs (e.g., cell-on-wheels (COWs)). The developed scheme minimizes travel distance and reduces the total travel time of all COWs during relocation by comparing all possible schedules. Rabieekenari *et al.* [124] proposed a distributed location algorithm to allocate COWs autonomously. The underlying assumption is that the COWs can obtain location information and capacity constraints of other nearby COWs.

While the deployment of mobile BSs can be used to extend coverage for public safety responders and victims, there are other BS placement efforts that consider different factors, including interference mitigation, energy efficiency, and others [12], [95], [108], [126]. For example, to improve the energy efficiency for mobile devices, Liu *et al.* [95] studied the joint optimization problem of deploying femtocell BSs and power control in commercial buildings. The cellular deployment optimization improved network performance, with concern for energy efficiency. The BS deployment on force fields considers both coverage and interference as optimization constraints in [126]. Moreover, in wireless sensor networks, the BS placement optimized to improve the network lifetime (i.e., energy efficiency of sensors). Moh'd Alia [108] proposed a relocation algorithm to relocate mobile BSs to reduce the communication distance between BSs and cluster heads in the network, leading to improved energy efficiency of the network.

C. UAV-BASED MOBILE BS

Compared to ground mobile BSs, low-altitude UAVs have the advantages of better accessibility, faster deployment, and a higher chance of establishing line-of-sight (LOS) channels in disaster recovery areas. The UAV carries a light-weight BS to provide network infrastructure in the air for communication with ground UEs. Multiple UAVs can form a temporary network to extend communication coverage. With the deployment of the UAV-based network, UEs can communicate inside and outside the disaster area.

1) COVERAGE AND CAPACITY

Related to coverage and capacity improvements, there has been a body of research in this area [13], [34], [73], [106], [107], [157]. For example, Merwaday *et al.* [107] proposed centralized Genetic Algorithm (GA)-based UAV deployment schemes towards throughput optimization in both large-scale and small-scale scenarios. The proposed GA algorithm can achieve higher time efficiency on finding a global optimal solution compared to other optimization approaches (e.g., brute-force search). Yang *et al.* [157] proposed the deployment of UAV-cells to handle flash crowd traffic in three scenarios (i.e., stadium, parade, and gathering). A hybrid distribution model accurately described user locations in both time and spatial domains. A prediction mechanism estimated the trend of user density. With the user information collected, the cluster-based deployment scheme computed the number of UAVs and the deployment locations. Assuming 3-dimensional freedom for UAV positioning, Bor-Yaliniz *et al.* [34] proposed an efficient 3-dimensional (3D) UAV deployment (i.e., positioning the UAVs by (x, y, z)) based on network revenue maximization (e.g., the number of covered users). Particularly, the air-to-ground channel variance changed with the dynamics of UAV altitude. Then, 3D deployment was an optimization problem with the consideration of the coverage radius of UAVs (depending on altitude) and UE locations. Alzenad *et al.* [13] extended efforts on optimal 3D UAV deployment in a way that considers different QoS requirements.

2) ENERGY EFFICIENCY

As a significant drawback of UAV deployment, battery-powered UAVs have limited energy capacity, reducing the durability and performance of the UAV-based network. There have been a number of research efforts devoted to improving the energy efficiency of UAV mobile BS networks [78], [137]. For instance, Kumbhar *et al.* [78] leveraged the optimization of the scheduling of beacon signal transmissions for air-ground communication to improve the energy efficiency of the UAV-based network. A non-cooperative game modeled the beaconing of two UAVs to optimize scheduling. In the non-cooperative game, the strategy of UAVs is the duty cycle of the beaconing. The game model Nash equilibrium was unique. Finally, a distributed learning algorithm converges towards the equilibrium beaconing cycle.

In addition, one solution to extend the durability of energy limited UAVs is to recharge the UAVs in a round robin manner. For example, Trotta *et al.* [137] investigated the scheduling problem of persistent UAV coverage for the target area. The performance of the scheduling solution included network lifetime and the number of swaps to recharge UAV.

D. HYBRID NETWORK

The hybrid network deployment consists of both UAVs in the air and mobile BSs on the ground, such that the advantages of both (i.e., high mobility of UAVs and durability of ground BSs) can be realized. In the following, we first illustrate the UAV deployment and interference coordination in the hybrid network, and then show an example of a hybrid network for public safety.

1) UAV DEPLOYMENT

There have been a number of investigations into UAV deployment [102], [103]. For example, considering the scenario that uses UAVs to cover ground terminals (GTs), Lyu *et al.* [103] designed an algorithm to sequentially place the minimum number of UAVs for coverage of group GTs. In their proposed scheme, the UAVs were initially placed by satisfying the condition that at least one UAV covers each GT to minimize cost (i.e., the number of UAVs deployed). The placement then starts from the boundary area of the group GTs, and covers all GTs in an inward spiral manner towards the center of the GT group. Compared with other benchmark schemes, the proposed algorithm demonstrates better performance in both time complexity and the number of UAVs deployed. Considering the cycling of mobile UAVs, Lyu *et al.* [102] explored the cyclical patterns in the air-to-ground channel, and proposed Cyclical Multiple Access (CMA) for the communication scheduling in the time domain.

2) INTERFERENCE COORDINATION

Interference coordination is critical to ensure that network performance persists. A number of interference coordination schemes exist. For instance, Athukoralage *et al.* [18] studied issues surrounding the co-existence of LTE (unlicensed)-based UAVs in the air and WiFi-based Access Points (APs) on the ground. The interference from the co-existing AP and UAV transmissions highly degrades the communication quality. Particularly, the cell-edge UEs receive strong downlink signals from both the AP and UAV, and AP UEs receive strong UAV signals. To minimize the interference, a regret learning-based algorithm was proposed to dynamically select the duty cycle of the transmission gaps for the UAVs in terms of maximizing throughput.

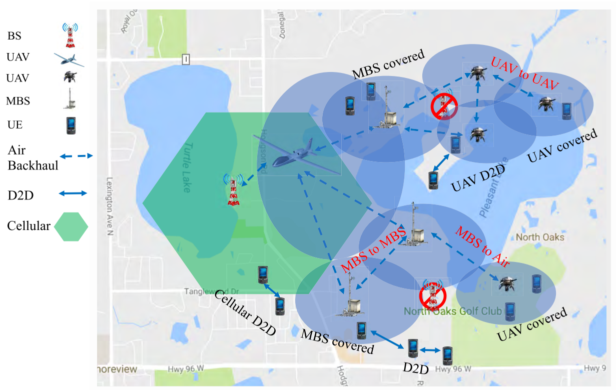

FIGURE 7. An example of public safety with D2D and DWN.

3) A DEPLOYMENT EXAMPLE

Fig. 7 illustrates an example of hybrid deployment, which leverages the UAVs, ground mobile BSs, and D2D communication. The cellular BS is dysfunctional in the area that ground mobile BSs are not accessible. The UAVs can form a DWN to provide coverage for UEs. In addition, in the area that the ground mobile BSs are accessible, the ground mobile BSs, which have large capacity and coverage, deployable for extended coverage. Also, the ground mobile BS and UAV-based BS can be jointly deployed, such that the ground mobile BS plays the role of relay terminal. Further, D2D communication is established when users are completely out of coverage.

Notice that establishing a temporary network infrastructure dynamically in an emergency area can support the communication of both victims and first responders. The dynamic deployment is highly affected by the accessibility, durability and efficiency of ground/aerial vehicles. Ground vehicle-based deployment carries mobile communication infrastructure on ground vehicles to establish wireless network coverage, the COW being one example [31], [110], [124]. Drawbacks of ground-based deployment are the deployment speed and accessibility, as terrain and impediments will hinder the speed and ability to reach a given emergency area. UAVs are more flexible and highly deployable to hostile environments. The unimpeded airway and air-to-ground channel are the main advantages of the UAV-based network deployment. Nonetheless, UAV-based network deployment has several significant challenges, including the coverage, capacity and energy efficiency [13], [34], [73], [107], [157]. Thus, hybrid deployment should also be considered, as it leverages the advantages from both ground vehicles and UAV in-the-air [18], [102], [103].

E. EXISTING PROGRESS IN DWN

In the following, we first review the standardization progress of UAV-based networks. We then discuss the existing research efforts on the UAV-based network over cellular and non-cellular networks. Finally, we review real-world applications and specifications for UAV-based networks.

1) STANDARDIZATION OF UAV-BASED NETWORKS

The 3GPP began the standardization process for using LTE to support UAVs in May 2017. The main purpose of the effort is to investigate the feasibility of enabling LTE to support connectivity for low-altitude UAVs [6], [94]. In particular, the 3GPP studies deployment scenarios, performance requirements and metrics, impacts of interference, channel models (NLOS and LOS), mobility performance (handover performance, robustness, etc.), and energy efficiency [6]. A technical report in [6] documented the progress of performance enhancement of LTE for aerial vehicles. For instance, it specified the deployment scenarios, including the maximum height (300 m above ground level) and horizontal speed (160 km/h) of UAVs, the service requirements (data type, latency, data rate, reliability, etc.) and performance metrics (throughput, interference, and reliability, etc.).

In addition, enhancements to interference detection and mitigation were investigated [6]. To be specific, interference detection at the UE side via measurement report from the UE enhances from new events, using additional measurement results, enhancing triggering conditions, etc. At the network side, the interference detection improves by information exchange, including scheduling information, transmission power, path loss of uplink aerial UE, as well as the UE's measurement report. In addition, interference mitigation results via directional antenna, receive beamforming, power control and intra-site Joint Transmission Coordinated Multi-Point (JT CoMP) transmission in LTE. The mobility performance improves for aerial vehicle-based networks, including the mobility history reporting, state estimation, and others.

2) UAV-BASED NETWORK OVER CELLULAR NETWORK

There have been a number of research efforts leveraging cellular networks (LTE, etc.) to establish the connection for UAV-based network [93], [94]. Toward this direction, Lin *et al.* [94] identified the connectivity requirements for the UAV-based network, and investigated the characteristics of aerial channels, including LOS and NLOS via simulation studies. In addition, efforts investigate the feasibility of using LTE to support the communication of UAVs. Particularly, the performance measurements assessed, include the SINR distribution, downlink coupling gain, uplink resource utilization, and user throughput of different deployment scenarios in an LTE network. Lin *et al.* [93] leveraged the LTE network to control an increasing number of drones, and presented a simulation study on the network performance (i.e., the latency of serving a large number of drones).

3) UAV-BASED NETWORK OVER NON-CELLULAR NETWORK

In public safety scenarios, it is critical to establish network coverage when the network infrastructure is not functional. Naturally, quickly establishing a UAV-based network over non-cellular network is one effective way to provide network connections for the disconnected UEs. In this regard, moving vehicles have the capability of carrying attachable APs over a long distance. In addition, multiple vehicles interconnected by a mesh network exchange information and support public safety communications. For example, Cesana *et al.* [37] developed a vehicular mesh network testbed, which leverages both IEEE 802.11p (vehicular communication environment) and WiFi-based mesh network. Here, the roadside infrastructure provides network coverage to vehicles via WiFi APs.

In addition, another viable solution is the use of UAVs to deploy a temporary wireless mesh network rapidly and provide connection to UEs. Compared to the ground deployment, in public safety scenarios, the main advantages of UAVs are the high mobility and accessibility. In this regard, Morgenthaler *et al.* [109] proposed a framework that can establish a wireless mesh network based on IEEE 802.11s with multiple UAVs. The UAVs carry light-weight mesh nodes in the air and play the role of APs, which provide coverage to user-devices via IEEE 802.11g channel. Moreover, the multiple UAVs easily interconnect to form an aerial wireless mesh network.

4) UAV-BASED NETWORK IN REAL-WORLD

The increasingly small size and sophistication of UAVs have made the platform cost-friendly and easily applied to both civilian and commercial use compared to the traditional mega UAVs that have been widely used in military applications. In general, small-size UAVs can be categorized into two types, fixed-wing UAVs and rotary-wing UAVs, which are naturally quite different in terms of payload, mobility, and stability. Compared to fixed-wing UAVs, rotary-wing UAVs, such as quadcopters, can perform hovering maneuvers to remain stationary and are generally more flexible. Puri [123] surveyed UAV-assisted traffic surveillance systems, which included a detailed investigation of various types of UAVs and existing UAV systems. For example, the Aerisonde fixed-wing UAV, which flies over 32 hours at a range of 300 to 20000 feet above ground, was adopted to capture video of highway traffic, and transmitted the data via microwave links [123]. In addition, Khan *et al.* [75] proposed a UAV testbed that enables the control and management of multiple UAVs via vision-based tracking and autonomous navigation. Also, Motlagh *et al.* [112] adopted UAVs to support the target service, i.e., crowd surveillance via face recognition.

The payloads of UAVs can range from only a few grams to many hundreds of kilograms, depending on the types of UAV and the required application. The endurance of any UAV, then, is highly dependent on its payload, which may include a battery as the main power resource. If we consider a scenario in which the battery shall power both the UAV and a BS, the BS should satisfy some specified target network requirements (e.g., communication distance), and the information of the BS, such as weight, size and power supply will be known. To improve the energy efficiency of UAV-based networks, Gupta *et al.* [66] reviewed the routing protocols in the network layer, i.e., path selection, node section and clustering, as well as other mechanisms on the data link layer and physical layer. In addition to addressing inefficiencies in these mechanisms, the application of automatic battery replacement and recharge techniques, and solar power, could be effective to extend the life of UAV-based networks [133].

V. CHALLENGES, POSSIBLE SOLUTIONS AND FUTURE DIRECTIONS

In the following, we first outline the challenges and possible solutions to D2D communication, DWN, security and resilience, and performance evaluation platforms for public safety networks, as shown in Fig. 8. We then discuss the possible integration of state-of-the-art computing and communication technologies into the public safety network in the future.

A. CHALLENGES AND POSSIBLE SOLUTIONS

We now describe four critical challenges, including (i) *efficient D2D techniques in public safety*, (ii) *efficient network deployment in public safety*, (iii) *security and resilience*, and (iv) *performance evaluation of public safety communication*

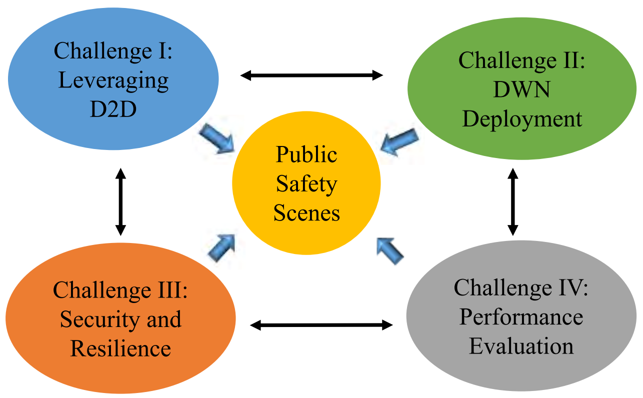

FIGURE 8. Challenges in the public safety.

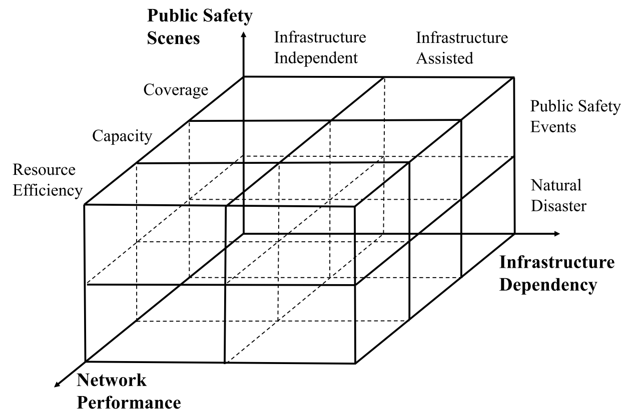

FIGURE 9. Design space for D2D.

networks. For each challenge, we discuss and outline potential solutions.

1) CHALLENGES TO EFFECTIVE D2D TECHNIQUES IN REALISTIC PUBLIC SAFETY SCENARIOS

Recall that, when disasters occur, the communication infrastructure becomes congested or damaged, disabling communication services. This calls for adopting D2D communication among the multiple public safety responders and victims to enable communication in local areas. While a number of research efforts on D2D communication exist, most research is aimed at improving network performance (spectrum efficiency, energy efficiency, coverage, and others). Nonetheless, the effectiveness of D2D communication as a user-side solution tailored to realistic public safety remains unsolved.

It is critical to systematically study the gap between existing solutions on D2D communications and the requirements of D2D in public safety emergency support. To design D2D communication system specifically for public safety support, the various representative real-world public safety scenarios (natural disasters and public safety events) should first model, and investigate D2D techniques based on those scenarios should then be designed. Particularly, the first step is to systematically conduct an investigation into the public safety conditions surrounding various representative examples, such as the 2015 Baltimore Riots [2], [77], [120], [149] and 2017 Hurricane Harvey [1], [146], and derive models from real-world data. The datasets related to these public safety incidents must be carefully analyzed and evaluated, including time-frame, damage area, personal injuries, communication disabled range, the information of BSs in incident affected areas, and others.

In particular, we illustrate the design space of D2D communication, clarifying the main characteristics in public safety. Fig. 9 illustrates the design space of D2D communication, including infrastructure dependency, network performance, and public safety scenes. Infrastructure dependency indicates whether or not the D2D communication is dependent on the existing traditional network infrastructure (e.g., infrastructure independent or infrastructure assisted). Network performance indicates the performance perspective of leveraging D2D in the public safety network (i.e., performance improvement on coverage, capacity, and resource efficiency). Lastly, we consider the public safety scenarios that D2D communications address (natural disasters, public safety events, etc.). For example, a model leveraging D2D communication to improve the coverage for first responder teams in Hurricane scenarios can be allocated to the <infrastructure independent, coverage, natural disaster> space. In addition, the modeling of mobility and traffic in the responder teams utilizing real-world datasets is critical. The mobility of the responders will be different during search, delivery, and rescue in the disaster relief phase, and traffic intensity and distribution will vary as well.

Summary: Recall the review of D2D communication in Section III, which mainly focuses on in-coverage and out-of-coverage D2D communication to cope with public safety scenarios. The majority of existing research efforts on D2D communication are intended to address interference and improve the energy efficiency in broad wireless networks instead of the specific public safety network. There are clear gaps between the general efforts on D2D communication and applying D2D in a public safety setting. Indeed, further research efforts are highly necessary to enable and improve D2D such that it can be applicable and efficient in various public safety scenarios. We thus propose the problem space for D2D in Fig. 9, which is intended to fulfill the research gap and direct future research efforts. The problem space for D2D is designed based on existing research efforts in this direction and provides a roadmap for further research. For example, the work in [115], which can be allocated in <infrastructure independent, coverage, natural disaster>, tried to provide coverage by D2D communication without communication infrastructure in the aftermath of a natural disaster. Despite a number of other existing research efforts ([55], [167], etc.), the unoccupied boxes in Fig. 9 can be specified as research gaps or directions that demand further investigation.

2) CHALLENGES TO EFFICIENT DEPLOYMENT FOR REALISTIC PUBLIC SAFETY SCENARIOS

It is worth mentioning that existing commercial networks are not designed with the consideration of public safety needs. The typical design objective is to gain the maximal revenue (i.e., overall utility) by allocating a minimum amount of resources that are necessary to satisfy user's performance requirements [118]. Nonetheless, during an emergency, the incident location experiences a spike in traffic from both public users and public safety responders. The resulting congestion can affect the communication QoS of users involved, even the public safety responders. This calls for the design of techniques that can rapidly and cost-effectively deploy mobile wireless networks via mobile ground BSs and UAV-based BSs, meeting the dynamic traffic needs to support public safety. The dynamically deployed mobile wireless network can provide coverage for public safety responders and victims, support high traffic loads, reduce end-to-end delay, avoid congestion, and improve the efficiency of network resource use in incident areas.

In addition, the deployed network needs to be resilient to various failures and cyber-attacks. With limited resources (bandwidth, power, etc.), limited coverage range, and geographically and temporally dynamic traffic, optimally deploying mobile BSs and UAV-based BSs in public safety scenarios to meet requirements (maximizing throughput, ensuring strict and diverse QoS requirements, improving network resilience to failures and 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 public safety responders (victims can be included in some cases) in the disaster area. To improve the resilience of the deployed network, more than one UAV should be deployed within the communication distance of public safety responders, which may need to deliver massive amounts of traffic and urgent information with very high reliability and strict QoS requirements. In addition, when public safety settings change rapidly in the disaster area, and emergency responders are mobile, traffic intensity will change rapidly, posing additional challenges to the adaptability of the deployed network. Furthermore, deployed networks can be affected by failures and cyber-threats due to the nature of public safety, the open wireless medium, DWN topology, and components lacking tamper-resistant hardware having an increased possibility of being compromised.

To address these challenges, techniques for rapidly, cost-effectively, and resiliently deploying both mobile BSs and UAV-based BSs should be designed with consideration for the dynamics of traffic, user density distribution, realistic constraints (geo-restriction, information availability, etc.), deployment costs, coverage and QoS for public safety users, and the specifics of public safety models. Fig. 10 illustrates the problem space for the dynamic deployment of wireless networks, including deployment components, communication requirements, and public safety scenarios. The deployment component indicates that the equipment actually deployed depends upon the distinct requirements and situations (e.g., ground mobile BSs, UAV-based BSs, and hybrid). The communication requirements indicate the different perspectives on leveraging dynamic deployment, such as requirements on coverage, QoS, and resilience. Last, the design is highly adaptive towards public safety scenarios (i.e., natural disaster and public safety events), as mentioned previously. Based on the outlined problem space, designing schemes for optimal deployment of ground mobile BSs and/or UAV-based BSs is paramount. Then, novel schemes to find optimal locations for flying UAV-based BSs and mobile ground BSs should be designed in a hybrid manner, which aims at minimizing deployment time and cost while guaranteeing QoS for public safety responders. Finally, further design is required of techniques to make deployed networks resilient to failures and cyber-attacks.

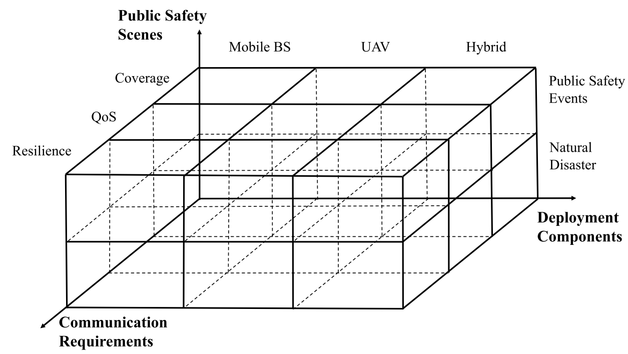

FIGURE 10. Problem space of DWN deployment.

a: DEPLOYING GROUND MOBILE BSs

Location: To ensure that public safety responders are covered by ground mobile BSs, we need to place at least one BS inside each region. One goal in the deployment is to balance the signal-to-noise ratio (SNR) across the covered region. Then, the optimal position of a ground mobile BS is the "center" of a disk covering the target region, which ensures that the SNR inside the region is balanced. Nonetheless, one ground mobile BS can be located at the intersection of multiple disks to cover users. Thus, we will define the areas formed by disks and their intersections. One optimization problem is how to select the minimum number of areas to deploy ground mobile BSs for coverage. This problem can be formalized as the minimum set coverage problem, aiming to find the minimum number of subsets to cover the whole area. Cost-effective algorithms solve this problem, which select the subset that provides maximum coverage for public safety responders. In addition to the coverage problem, there are other factors to consider while conducting the BS deployment optimization, including the interference mitigation, energy efficiency, users' priorities and others. Recall in Section IV-B, that the optimization of the

BS deployment considers the factors as constraints to find the minimum number of BSs and their locations.

Relocation: In a large-scale incident, the intensity of network traffic could approach to a level so that the initially deployed mobile BSs are not capable of handling the latest imposed users and associated network traffic. When this occurs, mobile BSs deploy to more locations. After selecting the area to place a BS, to determine the exact position for the next move, relocation mechanisms (e.g., Hungarian method [61], etc.) could be adopted for minimizing the total travel distance of all ground mobile BSs.

Nonetheless, deployment needs to consider practical constraints. Particularly, when we apply 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, using a real-world geographical map of the incident area to determine the next appropriate candidate location for deployment is ideal. This may also have an effect on the coverage and interfere with other BSs. Thus, determining the most appropriate candidate locations is another important issue for deployment in restricted areas. To deal with this, one possible solution is to let ground mobile BSs perform a random-walk with obstacle avoidance [76]. On reaching the positions that maximizes local communication area coverage, navigation stops and the stationary mobile BSs become references for others to spread further.

b: DEPLOYING UAV-BASED BSs

Location: The connectivity and coverage problem between UAV-based BSs and public safety responders require attention. In terms of connectivity, a realistic public safety scenario considers all public safety responders and victims connected using the minimum number of UAV-based BSs. In terms of coverage, the coverage solution should provide performance guarantees to public safety responders and victims with the consideration of data rate from participants and the capacity of UAV-based BSs, while the objective is to deploy the minimum number of UAV-based BSs. In addition, the deployment of UAV-based BSs needs to consider the deployment scenarios of urban and rural areas and coverage areas with even terrain and uneven terrain. To this end, efficient algorithms compute the optimal number of UAV-based BSs and their optimal locations for connectivity and coverage in realistic public safety scenes.

Deployment Scenarios: Particularly, the following three scenarios should be considered: (i) *Scenario I:* Given the location, traffic, and required traffic priorities of public safety responders, the minimum number of UAV-based BSs needed, and their locations, should be found. Additionally, when the traffic intensity fluctuates dramatically, we must find the mobility pattern to relocate UAVs with minimal travel distance. (ii) *Scenario II:* Given a limited number of UAV-based BSs, the maximization of the coverage and QoS satisfaction rates of public safety responders should be resolved, with the consideration of traffic per public safety responder and priority. As a result, the UAV-based BSs must adapt to the dynamic nature of traffic intensity, provide coverage, guarantee the QoS of public safety responders and victims, satisfy the priority traffic requirements, and further improve the resilience of the DWN (i.e., providing backup UAVs for traffic with different priorities). (iii) *Scenario III:* With the best satisfaction provided from the limited number of UAV-based BSs, some public safety responders may not be adequately satisfied due to limited resources. Considering the limited resources of UAV-based BSs, other problems to be addressed lie in resource sharing and scheduling to fulfill the requirements of all responders (coverage, QoS aware, and resilience).

c: HYBRID DEPLOYMENT

The joint deployment of mobile ground BSs and UAV-based BSs enhance the performance of deployed networks to adapt to public safety scenarios and improve the resilience of communication. The ground mobile BS, which provides efficiency, reliability, and durability due to its rich power supply and high network capacity, is limited in topographical accessibility, as well as reaction time. In contrast, the UAV-based BS has the advantages of rapid response, high accessibility, and adaptability. By leveraging the advantages of both ground mobile BSs and UAV-based BSs, it is imperative that joint deployment be studied in the following three cases.

First, with the initial deployment of ground mobile BSs, the network can be further improved by enlisting the support of UAV-based BSs when the mobile BSs are not capable of meeting the QoS requirements of public safety responders. For instance, the ground mobile BSs may be blocked by rioters in some extreme cases, and the UAV-based BSs could be deployed to recover the network in such an area. Second, with the UAV-based BSs initially deployed to quickly respond to an emergency, the network efficiency, reliability, and durability can be enhanced by leveraging additional ground mobile BSs. For example, when an emergency (e.g., wildfire) suddenly occurs, the UAV-based BSs deploy quickly as the first to arrive, and then ground mobile BSs can participate in further improving and supporting network coverage. Lastly, the ground mobile BSs and UAV-based BSs deploy concurrently and coexist to establish an ideal network in the cases of public safety events and natural disasters.

Summary: The DWN that rapidly establishes the communication infrastructure is one viable way to provide connections for both first responders and victims for time-critical information delivery. Dynamic network deployment consists of the ground mobile BS deployment, UAV-based BS deployment, and hybrid deployment. The different deployment strategies have various advantages and shortcomings in durability, capability and rapidness. We identified different problems based on different deployment strategies for public safety (e.g., the deployment and redeployment problem for ground mobile BSs). We designed the problem space to help in the design of DWN to establish communications for public safety in Fig. 10. The problem space indicates that research efforts towards the DWN for public safety must consider different deployment components, communication requirements, and public safety scenes in the three outlined dimensions. A number of existing research efforts on DWN deployment ([18], [31], [102], [103], [106], [107], [124], [157], etc.) can be categorized into the target problem space. For example, the work in [31] can be allocated in the cube of <Mobile BS, QoS, Public Safety Events>. In addition, the unaddressed areas in Fig. 10 shall be explored to fill research gaps between the existing research efforts and the applicability of DWN for public safety.

3) CHALLENGE OF SECURITY AND RESILIENCE IN PUBLIC SAFETY NETWORKS

As security is of prime importance in a dynamic wireless network, the challenges for DWN and D2D security and resilience must be fully understood and addressed. There are a number of security and resilience challenges in dynamic wireless networks because of the open nature of the wireless communication medium, DWN topology, lack of common security policies used by network operators, resource constraints of mobile devices, and others [26], [29], [30], [47], [89], [101], [113], [143]. The dynamic wireless networks could operate in hostile environments and components that lack tamper-resistant hardware could increase the chance of the system being compromised. After a node in the network is compromised, the adversary can further access the restricted information on the node. Recall that, in the case of the deployment challenge, we consider the solution to be the development of techniques that could address optimal deployment and efficient data transmission in dynamic wireless networks. Nonetheless, the effectiveness of the optimal deployment schemes developed largely depend on real-time network state information (traffic change, user distribution, etc.). With compromised nodes, the adversary could inject false measurements to make the deployment schemes ineffective.

To address the security issues and enable a resilient dynamic wireless network, a theoretical framework is highly needed, enabling an exploration of the space of attacks, and a detailed investigation of these attacks, to understand their impacts and develop effective mitigation schemes (i.e., countermeasures) against them. The attack space is illustrated in Fig. 11, composed of three dimensions (i.e., attack plane, attack target and attack objective). To be specific, the attack target consists of ground device, aerial device, or end-user device. The attack plane separates into the control plane and data plane. The control plane represents the management to ensure coordination among components of DWN through related information. The data plane is responsible for efficiently delivering user data over the network. The attack objectives are denoted as availability, integrity and confidentiality.

a: UNDERSTANDING ATTACKS

Fig. 11 outlines the attack space in three dimensions. Based on this model, we systematically investigate the attack targets

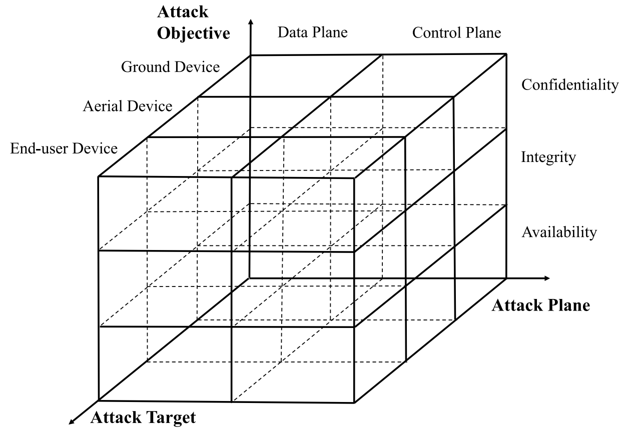

FIGURE 11. Attack space on public safety communication.

and provide some common examples. Recall in Fig. 10, the components of the dynamic wireless network primarily include end-user devices (e.g., UE devices, femtocells), ground devices (e.g., ground base stations, eNodeBs), and aerial devices (e.g., UAVs). All these components can be targets to the adversary. For instance, as smart mobile devices become popular and use rich applications, these compromised UE devices launch attacks against dynamic wireless networks. Femtocells can be a security loophole because these devices are not fully controlled by the network operator [15], [65], [160]. For instance, when data encryption is terminated at a femtocell, the confidential information associated with legitimate users can be exposed to the adversary via hardware tampering [29], [32], [41], [51]. Also, concerning ground base stations, eNodeBs may be compromised and send misleading information to neighboring nodes, ultimately disrupting dynamic wireless network operations. Malicious nodes could cause collisions with the channel access of others, leading the victim nodes to conduct exponential back-off on packet loss, giving the free channel to the malicious nodes. A malicious node could also join a route during the route discovery process, and intentionally fail to forward packets correctly.

In the control plane, attacks tend to disrupt the coordination of devices and degrade the performance of DWN. Within the data plane, the adversary could manipulate data packets and further sends them through the network to further disrupt the efficiency of data transmission (e.g., disrupting the efficiency of network coding [173]). For example, the adversary used some nodes to inject manipulated packets into the network traffic flow, posing the effectiveness of data transmission and affecting network performance with respect to throughput, packet loss, latency, etc.

In addition to attack targets and attack planes, the attack objectives includes confidentiality, integrity, and availability. **Confidentiality** concerns the protection of information from disclosure to unauthorized individuals, whereas authorized individuals are granted access. As an example, in a passive masquerading attack in a dynamic wireless network, an adversary could behavior as a legitimate eNodeB (Ground mobile BS or UAV-based BS). After authorization, a user may select the compromised ground or UAV-based BS to use. When this occurs, the adversary can use the malicious ground or UAV-based BS to gain confidential information from the connected user.

Integrity refers to the guarantee that information is accurate, reliable, and tamper-proof. As such, the designed dynamic wireless network needs to maintain the consistency, accuracy, and trustworthiness of its data, and to ensure that data cannot be changed during transmission. If the integrity of data is compromised, the information is no longer reliable or accurate. For instance, data integrity attacks against network components to manipulate transmitted information need to be addressed [159]. As a large amount of false data injected by compromised nodes is transmitted through the network via multi-hop routes, the communication can be increasingly overloaded.

Availability refers to ensuring that information, services and assets are accessible. For instance, jamming threats against the DWN are <end user & ground device, control plane & data plane, availability>. Based on the derived theoretical framework, different attack scenarios evaluate the effectiveness of various jamming attacks. Examples include non-coordinated attacks with non-optimally deployed jamming devices, non-coordinated attacks with optimally deployed jamming devices, coordinated attacks with non-optimally deployed jamming devices, and coordinated attacks with optimally deployed jamming devices [30]. When optimally deploying jamming devices to maximize the attack impact on network performance, geographically and temporally, the optimal deployment schemes developed in Section V-A.2 should be used.

Finally, considering the worst-case attack, in which the adversary obtains complete knowledge, the active identification of the network deployment infrastructure (topology, mobility pattern of nodes, etc.) is possible. Then, various attack techniques (jamming, traffic analysis, false data injection, etc.) launch to disrupt services. With the consideration of the complete and partial information of network infrastructure, the adversary selects optimal strategies to attack nodes or links to achieve maximum damage (e.g., disrupting the optimal routing decision). The optimal attack objectives (disrupting network availability, causing the network to operation in a non-optimal manner, and others) must be investigated. With those objectives in place, the systematic modeling and simulation of attacks with different settings assess the consequences of such attacks.

b: DEVELOPING EFFECTIVE COUNTERMEASURES

To address the issue of attacks in dynamically deployed networks, defensive countermeasures design incorporates the following perspectives: attack prevention, detection, and response.

Prevention: The development of effective schemes to make dynamic wireless networks resilient is critical to preventing attacks. Based on the optimal deployment solutions, the device significance and criticality assessment defines metrics for measuring network survivability after devices are compromised or fail. The results would lead to the development of a highly resilient DWN deployment strategy that can increase the cost of attacks. Another method is to establish trustworthy infrastructure in dynamic wireless networks, which enables the control plane to measure the security risk of individual nodes and network regions, compute the security risk of discovered routes, and meet the QoS requirements for users. As an example, routes in the network satisfy QoS requirements for users. Then, select the route with the highest confidence in trustworthiness. In addition, developing novel and efficient low-cost filtering mechanisms can dynamically and rapidly filter misleading information injected by compromised nodes or misbehaving nodes, and achieve a high resilience to the number of compromised nodes when 3D wireless networks operate in hostile environments [159].

Detection and Response: To accurately detect attacks, it is necessary for threat monitoring systems for the dynamic wireless network to be developed. Implementing and deploying monitoring and detection agents or tools can effectively and proactively discover exploitable vulnerabilities on various devices (end user devices, ground mobile BSs and UAVs) to make the dynamic wireless network resilient to attacks. To be specific, effective threat collection through a detection agent collects real-time information (e.g., system logs, security logs, application logs, and traffic logs) and transmits them to the management center for analysis and detection. The investigation of anomaly-based detection schemes to defend against unknown attacks is critical and necessary for public safety networks. For example, network sensor-based intrusion detection frameworks to detect bots via network traffic monitoring, and malware monitoring of app behaviors on smart mobile device hosts through timing correlation, are possible strategies [80], [85], [162]. Machine learning techniques (Support Vector Machine, Naïve Bayes, Neural Networks, etc.), statistically-based detection schemes (hypothesis sequential testing, etc.), as well as the recent development of deep learning schemes can establish a robust set of features to detect anomalies [35], [56], [60], [85], [119], [131], [138], [158], [162], [163]. Finally, there are many examples of the application of the above mechanisms to detect cyber threats [28], [158], [162], [163], [166], [171].

The effectiveness of detection schemes include the true positive rate, false positive rate, detection time, and other metrics. For instance, a light-weight scheme was developed to identify the adversary that could launch pollution attack against network coding scheme [173]. In a public safety communication network, via fully using the broadcasting nature of the wireless transmit media, the downstream neighbor nodes monitor by a node that cooperates with other nearby nodes. In this regard, we should design schemes that could hierarchically organize the network into various levels. Then, in each level, multiple nodes nearby in the same level can check downstream level nodes cooperatively. By doing this, when a compromised node maliciously transmits a corrupted packet that is received by its next-level nodes, the detection scheme can be leveraged to recognize corrupted packet and further identify the corresponding malicious node.

Summary: The security and resilience of the public safety network are critical due to not only the open access nature of wireless communication networks, but also the limited resources of various nodes and devices in public safety, as well as the unpredictable consequences and losses after being compromised. Considering existing studies on security and resilience from the dimensions of attack objects, attack planes and attack targets for public safety networks ([15], [26], [29], [30], [32], [41], [51], [65], [160], etc.), we designed an attack space for public safety communications in Fig. 11. The various effective countermeasures to detect, prevent and respond to various attacks that consider attack objects, planes and targets of the public safety network should be developed. To fulfill the research gaps, we shall first explore attacks based on the designed attack space for public safety networks. In addition, with the understanding of attacks in public safety networks, we shall develop defensive countermeasures to prevent, detect and respond to those attacks.

4) CHALLENGES FOR PERFORMANCE EVALUATION

To validate the effectiveness of the proposed schemes outlined in D2D and DWN deployment, various tools and simulation platforms(ns-3 simulator [45], Vienna LTE Simulator [135], etc.), the Common Open Research Emulator (CORE) [9] support an emulation platform. Likewise a Software Defined Radio (SDR)-based LTE network testbed should be implemented to provide a real-world test platform [68]. Particularly, Vienna LTE simulator [135] implemented in a MATLAB environment and can support both link and system level simulations of LTE. CORE [9] is an emulation framework, which provides a GUI for users to build and emulate a network that consists of a number of virtual nodes and a different methods configure to connecting the virtual nodes.

In an SDR testbed, the SDR nodes play the role of UEs and eNodeBs in the LTE network to experiment with mobile vehicles and UAVs with eNodeBs based on real public safety scenarios. To optimize a testbed based on real public safety models, eNodeBs should be carried by vehicles (as ground mobile BSs) and UAVs, and evaluation of the performance and feasibility of the designed schemes should be carried out. Fig. 12 illustrates a framework to integrate modeling, simulations, emulation, and testbed for public safety. The designed experiments consider both the public safety events (Baltimore Riots) and natural disasters (Hurricane Harvey) and integrate the selected and developed schemes. While simulations enable the evaluation of modeling and techniques in large-scale networks, emulation focuses on real-world environments. In emulation, each emulated object runs real code in the real environment, meaning that we can implement and test the actual implementation of target algorithms

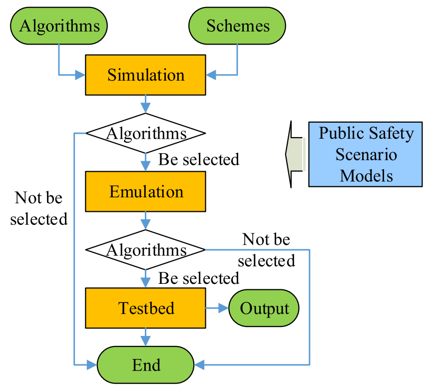

FIGURE 12. Integration of modeling and simulation, emulation and testbed.

and schemes. In addition, emulation is more flexible, with less cost to adjust and correct the implementations and parameters than in using a real testbed.

The candidate D2D communication and DWN deployment schemes outlined require real-world public safety scenario models. Then, the selected schemes run in the emulation platform, and the real-world testbed should likewise be implemented based on the investigated public safety scenario models. In the following, we outline the solutions in detail.

a: DEVELOPING SIMULATION SCENARIOS

The 3rd Generation Partnership Project (3GPP) has released the specification for D2D communication based on ProSe under LTE networks [3]. LENA [22], [23] is an integration module of LTE and EPC in ns-3. The main function of LENA is to support the performance assessment of LTE systems with respect to radio-level performance and end-to-end Quality of Experience (QoE). It can also support prototypes that include QoS-aware packet scheduling, resource management, inter-cell interference coordination, and others. Thus, the ns-3 simulator with the D2D module investigates LTE-based D2D communication. Nonetheless, the D2D communication module in ns-3 has not yet been fully implemented, though a number of researchers have been contributing to its development. For instance, work in [46] released the modified version of ns-3 for D2D simulation, providing EPC-level user device discovery, LTE-Direct communication (UE to UE), and others. In addition, the Wireless Networks Division at the National Institute of Standards and Technology (NIST) conducted research to simulate the LTE-based D2D discovery and communication in different topologies covering both indoor and outdoor scenarios [127].

In addition to ns-3, Vienna LTE simulators [135], which are implemented in MATLAB environment, are capable of supporting both link and system level simulation of the universal Mobile Telecommunications System (UMTS) in LTE. The simulator tests existing or new schemes and algorithms in either link level or system level supported by the tool. The modularity of the Vienna LTE simulator makes it more user-friendly, easier to include additional features (e.g., D2D discovery and communication), and easy to integrate with a testbed. From physical layer modeling, such as link quality and performance models, to link-to-system mapping, channel and antenna modeling, all are implemented with different scenarios in separate code blocks. Since Vienna is implemented in MATLAB, the SDR toolbox in MATLAB can also be used for HIL (Hardware in the Loop) testing and evaluation. Combining simulation, emulation and testbed equipment, D2D communication performance analysis for public safety scenarios can be performed.

Several relevant topics regarding the D2D communication module in ns-3 have been investigated. For instance, some inherent features may cause overhead problems (e.g., the TCP three-way hand shake, and the large header of TCP being, at minimum, 20 bytes). Looking to other protocols, there is a comprehensive new protocol called CoAP [59]. By using CoAP over UDP, the overhead is significantly reduce in comparison with HTTP over TCP. In addition, there are a number of schemes that available for LTE networks. Nonetheless, when the environment changes, the eNodeB may not have enough capacity (either the eNodeB is overloaded with too many devices, or there is partial or no coverage). For example, Fodor *et al.* [54] described an out-of-coverage UE to UE communication scenario. The solution develops algorithms to efficiently manage D2D communications. The developed algorithm in [92] showed a traceable optimal model to optimize multicasting for D2D by selecting optimal multicast rate and re-transmission time. While a number of research efforts have contributed to the D2D communication module in ns-3, consideration of realistic public safety scenarios (Rioting & Hurricane) using both ns-3 and Vienna LTE simulators to investigate the effectiveness of the developed algorithms and protocols is critical.

We now briefly describe how to design and implement these scenarios in the ns-3 and Vienna LTE simulators to evaluate D2D and deployment techniques for public safety scenarios. With respect to the riot scenario in an urban area, the simulation of an urban area identifies D2D communication and dynamic mobile BS and UAV deployment for diverse public safety settings. Notice that RoutesMobilityModel in ns-3 and site locations of real-world BSs [69] can be used to deploy maps related to public safety scenarios. For example, based on the satellite map of Baltimore city, cellular tower distribution map, Baltimore population density map, and Baltimore rioting event data logs, we can consider that (i) the communication infrastructures in the area are partially damaged, and (ii) the density of mobile devices exceeds cellular tower capabilities. Similarly, based on hurricane Harvey's recorded path of travel, related data logs, and other data, the damage of network infrastructure and communication conditions can be modeled and considered via simulations. For example, cellular tower availabilities in the hurricane affected area can be evaluated. Based on the released data, we could assume that the damage to cellular towers is 90 % in Harvey's wind path, and 50 %, in the towers that are far away from the hurricane path. The more cellular towers damaged or disabled, the more critical public safety communication support will necessarily be.

b: DEVELOPING EMULATION TOOLS

CORE, initially developed by Boeing, and currently supported by the Naval Research Laboratory [9] is a python framework. It has a graphical user interface to configure emulated networks. The emulated environment works with a number of virtual nodes, as well as methods for connecting these virtual nodes. On individual emulated nodes, applications, protocols, and scripts (e.g., mobility patterns) extend the capability. Combining individual nodes enhances the evaluation environment realism. In addition, CORE enables the connection between emulated networks and live networks. The languages awk (a programming language designed for text processing), *R* (an open source programming and software environment for statistic computing and graphics), and MATLAB, can help with network emulation, and then performance evaluations can be further developed. For example, performance evaluations of the NetConf protocol, the CoAP protocol, and multi path data streaming in mobile wireless networks have been conducted with CORE [58], [59], [114].

c: DEVELOPING AN SDR-BASED TESTBED

Radio frequency bands are over-employed, and a new age of radio networking calls for the development of software radio technologies to provide self-adaptive radio systems. Generally speaking, SDR-based testbeds allow researchers to test, evaluate, and validate the effectiveness and feasibility of new technologies, such as digital video broadcasting [24], telecommunication networks [25], [36], [62], navigation applications, and wireless networks [33], [36] like WLAN, WiFi, etc. There are a number of implementations of SDR testbeds [21], [104], [116], [117], which can be used for wireless network research.

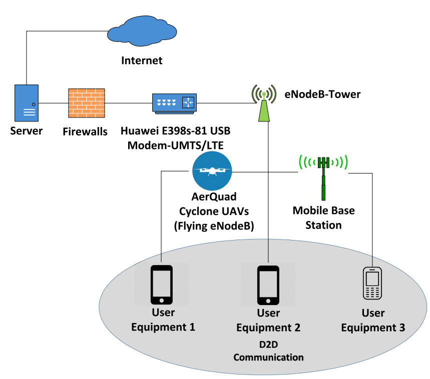

FIGURE 13. SDR-based testbed for public safety communication.

Fig. 13 illustrates one example setup for experimentation directed at public safety scenarios, which uses four SDR nodes (also eNodeBs can be deployed in a moving vehicle to represent a ground mobile BSs and UAV-BSs).

Particularly, the four SDR nodes include: (i) one stationary, acting as an LTE tower, (ii) two mobile UEs acting as first responder teams, such as police and fire crews, and (iii) one airborne, flying on a quad copter (UAV), acting as an alternative LTE network coverage provider. To create an SDR node, the Ettus Research Lab SDR board (USRP B205mini-i) can be leveraged to be an RF radio backend. Also, an Intel NUC (NUC5I5RYH) compact computer can be used to carry out the RF signal processing. The SDR board can be set up by connecting it to a USB 3.0 port for both power and data transfer. The RF front-end is Single Input Single Output (SISO) with two Omni-directional antennas (VERT900 1.8 Ghz), a transmitter, and a receiver, used for full-duplex transmission.

In addition, to create a basic LTE network for evaluation, the open source srsLTE and srsUE libraries can be used, which were written in C, and use the VOLK library for signal processing on NUC computers. These libraries are highly interchangeable with almost no external or inter-module dependencies. The testbed can be adjusted based on each public safety scenario, including UAVs with eNodeBs, ground mobile BSs, and UEs as necessary. The D2D and network deployment test cases implemented by the SDR-based testbed to evaluate the results of the investigated schemes. The data collected from the testbed can be further processed for visualization and detailed analysis. The results provide a proof-of-concept of the proposed schemes, and scheme performance across different scenarios can be compared.

Summary: The research efforts towards D2D, DWN, and security and resilience for public safety, including algorithms, strategies, and schemes, shall be well examined and evaluated before real-world implementation can occur. Extensive existing research efforts on evaluation platforms in [3], [9], [21]–[23], [46], [54], [58], [59], [92], [104], [114], [116], [117], [127], and [135] established some support to evaluate the performance of various approaches for public safety networks. Those research works focus primarily on the performance evaluation of technical approaches for communication networks. Nonetheless, the establishment of performance evaluation platforms that particularly address public safety networks demands further research endeavors. Thus, we have outlined the simulation (ns-3 simulator, Vienna LTE Simulator, etc.), emulation (CORE) and testbed (SDR-based LTE network testbed) components, which can be leveraged to evaluate technical approaches for D2D and DWN for public safety use.

B. FUTURE DIRECTIONS: INTEGRATING STATE-OF-THE-ART COMMUNICATION AND COMPUTING TECHNOLOGIES IN PUBLIC SAFETY NETWORKS

In the following, we discuss how to integrate state-of-the-art communication and computing technologies to improve the public safety, including IoT to improve the interconnectivity, cloud/edge computing to improve computation capabilities and 5G to improve network capacity.

1) INTERNET-OF-THINGS (IoT) FOR INTERCONNECTIVITY

IoT integrates sensors, actuators, and computing and network technologies to connect massively deployed IoT devices, and data collection and application systems, over cyber and physical spaces. With IoT, various devices (sensors, actuators, etc.) and networks (HetNet, wireless sensor network (WSN), mobile ad hoc network (MANET), wireless mesh networks, etc.) can be interconnected. In addition, via the support of IoT, not only will ubiquitous devices, sensors and facilities be interconnected, but information about the world and human activities will be transmitted and available, anytime and anywhere [89], [132].

To support interconnectivity, the IoT infrastructure has two significant features: (i) the interoperability of the various networks, and (ii) the interconnection of a variety of objects. While existing research efforts on IoT system development has focused on the specific applications with intranet/extranet, there is a distinct lack of interconnection between them [44], [152]. One critical issue of the IoT infrastructure is the design of a generalized network infrastructure and relevant techniques to support various heterogeneous networks and objects, such that all IoT systems and applications can efficiently utilize the network resources via the generalized network infrastructure and provide a wide-variety of services [165], [168].

The four-layer Service-oriented Architecture (SoA) in a top-down structure (i.e., application, service, network, and perception) is one possible solution to support IoT [10], [44]. The application layer, as the top of the IoT architecture, contains the specific applications, including the smart grid [155] and smart transportation [88], among others, and performs the application functions and operations. The service layer is the middleware that connects the application layer and network layer, which mainly provides the data service, storage service, and analytical service. The network layer mainly routes the transmitted data and information to the various devices (i.e., IoT hub, gateway, and devices) via the integrated protocols and communication technologies, such as WiFi and LTE. The bottom layer (i.e., perception layer), also named the sensor layer, interacts with the physical devices and the network layer, and primarily measures, collects and transmits information to the upper layer.

With highly interconnected devices, sensors, and facilities, as well as the highly integrated network, IoT can contribute to public safety through situational awareness in the disaster prevention, emergency management, and disaster relief phases. To be specific, in the disaster prevention phase, the interconnected things (i.e., devices, sensors, human behaviors, and other objects) quickly and thoroughly collect information concerning both situational awareness and preparedness. Rapidly, based on the information collected from the IoT devices, the responders can be better prepared for the public safety scenarios in the emergency management phase. For instance, the sensors, monitoring devices, transportation equipment, and human activities can describe and report the dynamics of the ongoing public safety events and the resulting damage in a rapid manner. Then, the responses from the responders can be updated accurately with the awareness of the dynamics of the ongoing public safety scenarios. In the disaster relief phase, the interconnected IoT devices can help in situation awareness for the responders via extensive information collection and transmission. With the knowledge that the interconnectivity of IoT can greatly assist the public safety emergency response, extensive research efforts are still necessary to realize IoT towards public safety applications.

2) EDGE/CLOUD COMPUTING FOR BIG COMPUTING

The well-known cloud computing infrastructure can provide unprecedented computing resources (i.e., storage and compute), and enable the ubiquitous access to support both situational awareness and crisis communication in public safety scenarios. The powerful cloud computing platform can be viewed as a centralized datacenter, able to process the data, storage, and computing in a faster and more efficient manner [16], [105]. Regarding situation awareness, cloud computing can store and compute information from millions of IoT devices and sensors rapidly. Then, utilizing the powerful computing system, the optimal responses (DWN deployment, responder team allocation, etc.) evaluate timeliness. For crisis communication, cloud computing can improve the effectiveness and efficiency of time-critical information delivery due to its high storage capability. All relevant and necessary data will be pushed to the cloud, and thus can be accessed broadly and rapidly. The main limitations of cloud computing include transmission delay and the communication bandwidth, due to the centralized distant cloud servers.

With the support of other techniques such as software defined networking, etc., edge computing leverages the computing capabilities of devices at the network edge (gateways, switches, etc.) and retains the computing and storage locally, near the users [71], [144]. Thus, it can loosen the communication bandwidth requirements and improve latency performance, leading to efficient network resource use. One possible three-layer hierarchical architecture, including far-end, near-end, and front-end was studied in [71] and [136]. At the top level, the far-end layer includes the cloud datacenters, which are located far from the end-users, but provide the most powerful compute, storage, and analysis capabilities. The near-end layer includes the gateways, switches, and other edge devices, which still have greater computing capabilities than mobile devices, in general, and includes data processing, computing, storage and caching. Due to the large number of near-end devices, the computing capacity is sufficient for the local computing and analysis, and thus, reduces the transmission delay. In the front-end layer, the deployed IoT devices and actuators perform lightweight computations, and respond in real-time. Due to their limited capacity, however, additional resources can be requested from a higher layer when needed. The high computing capacity and the low latency of edge computing can potentially improve situation awareness and crisis communication in public safety scenarios effectively and efficiently. On top of the computing power provided by cloud/edge computing infrastructure, effective deep learning [60], [67], [119], [130], other data analysis schemes [48], [156], as well as streaming analysis [40] can be provisioned, further supporting the situation awareness of public safety scenarios. Despite progressive advances in these areas, significant work is still necessary, especially with respect to supporting emergency response.

3) 5G FOR BIG NETWORK

The increasing demands on network capacity, throughput, end-to-end delay, and the resource efficiency of the communication network stem from the massive number of user devices and demanding applications (i.e., smartphones and heavy data traffic from multimedia services). To fulfill these demands, the 5G wireless communication network, which consists of the ultra-dense deployment of small-cell BSs, the rich spectrum resources from high frequency band millimeter Wave (mmWave) communication, and the massive multiple-input and multiple-output (MIMO) techniques of large-scale antenna systems, has been attracting significant interest and research efforts [8], [14], [164].

For example, ultra-dense small cells, which consist of a large number of small-cell BSs and access points at a level approximately equal to the number of user devices, is the main paradigm to improve the network capacity. The main reason for this is the 2700-fold network capacity increase from 1950 to 2000, which is the result of cell size reduction and decreases in communication distance [97], [164]. Due to spectrum scarcity, the 300 MHz - 3 GHZ band in the legacy communication system cannot accommodate the demand of the exponentially growing volume of devices and traffic. The mmWave band, which ranges from 30 to 300 GHz, has rarely been utilized for the commercial communication networking, because of the strong path loss, low penetration performance, hardware costs, and others. Nonetheless, with cost reductions in hardware and adoption of small cell BSs for closer communication distance to lower transmission power, the utilization of the rich spectrum resource of mmWave becomes appealing. In addition, MIMO, indicating the multiple receive/transmit antennas on BSs, can improve system performance with regard to array gain and diversity gain via beamforming and transmit diversity. Massive MIMO, known as large scale antenna systems, can significantly enhance resource efficiency and improve system capacity [8], [99].

With a set of 5G-related technologies, the 5G network is expected to introduce a Big Network that enables the interconnection of millions of IoT devices and smartphones with high transmission speed and resource efficiency, and low latency. In public safety scenarios, the situation awareness based on information collection and transmission through such a big network will no longer face the same speed limitations and throughput constraints. Instead, the situation awareness will be much more informative and efficient to support public safety. For instance, in the process of large-scale information collection, the legacy wireless network is very likely to be overloaded due to the limited network capacity, whereas the 5G network can support significantly greater network capacity and can offload the traffic spikes.

In addition, for large-scale natural disasters, a Big Network such as 5G can handle traffic peaks from three main stages: information collection from the victims and IoT devices, communication traffic between the affected area and outside regions, and response distribution to the victims and responders. The 5G communication techniques can also support crisis communication. For example, temporary networks formed between the responders and small-cell BSs results from their lightweight nature and large network throughput. In addition, mmWave and massive MIMO in small-cell BSs can improve backhauling performance, due to the rich spectrum resource, directional transmission and diversity gain. Thus, while the research and development of 5G networks is ongoing, how to leverage 5G network technologies to support public safety use remains a critical research area.

VI. FINAL REMARKS

In this paper, we addressed the issues of public safety communication. Particularly, we first designed a layered structure, which consists of public safety service layer, time-critical information delivery layer, and physical object layer, to subdivide public safety system into its key components. We then extensively reviewed existing research efforts toward communication techniques (user-side solutions, i.e., D2D, and network-side solutions, i.e., DWN deployment), which enable and support time-critical information delivery in public safety scenarios. We specifically reviewed the approaches and existing progress in D2D and DWN for public safety.

While existing research efforts on both D2D and DWN deployment are extensive in legacy/commercial communication networks for the purposes of traffic offloading, coverage extension, and effective network establishment, there are significant gaps in the research efforts on D2D and DWN as applied to support public emergency response scenarios. We thus outlined the challenges and possible solutions for D2D, DWN, security and resilience, and performance evaluation for the public safety network. We also discussed the future directions toward integrating state-of-the-art technologies, including IoT, cloud/edge computing, and 5G into public safety networks. We hope that this survey is helpful for readers and researchers to comprehensively understand the components public safety communication, user-side and network-side communication techniques, and their challenges in application. We believe that, with the outlined solutions and prospective future needs, research and development supporting more effective and efficient public safety response will be thoroughly conducted to overcome critical challenges in the future.

REFERENCES

[1] (Aug. 22, 2017). *Guyana: Emergency Situation at Jawalla Village, Region 7*. [Online]. Available: https://reliefweb.int/report/guyana/guyana-emergency-situation-jawalla-village-region-7

[2] (Sep. 2015). *Lessons Learned From the 2015 Civil Unrest in Baltimore*. [Online]. Available: https://assets.documentcloud.org/documents/2514212/independent-report-on-baltimore-police-response.pdf

[3] *Proximity-Based Services (Prose); Stage 2*, document G.T.23.303, Dec. 2016. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=840

[4] 3GPP, "Feasibility study for proximity services (ProSe) TR 22.803," Tech. Rep., 2012.

[5] 3GPP, "Study on architecture enhancements to support proximity-based services (ProSe) TR 23.703," Tech. Rep., 2013.

[6] 3GPP, "Study on enhanced LTE support for aerial vehicles TR 36.777," Tech. Rep., 2017.

[7] D. Abusch-Magder, P. Bosch, T. E. Klein, P. A. Polakos, L. G. Samuel, and H. Viswanathan, "911-NOW: A network on wheels for emergency response and disaster recovery operations," *Bell Labs Tech. J.*, vol. 11, no. 4, pp. 113–133, Winter 2007.

[8] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[9] J. Ahrenholz, "Comparison of CORE network emulation platforms," in *Proc. IEEE Military Commun. Conf.*, Oct./Nov. 2010, pp. 166–171.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[11] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[12] E. Altman, A. Kumar, C. Singh, and R. Sundaresan, "Spatial SINR games of base station placement and mobile association," *IEEE/ACM Trans. Netw.*, vol. 20, no. 6, pp. 1856–1869, Dec. 2012.

[13] M. Alzenad, A. El-Keyi, and H. Yanikomeroglu, "3-D placement of an unmanned aerial vehicle base station for maximum coverage of users with different QoS requirements," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 38–41, Feb. 2018.

[14] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[15] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, "Femtocells: Past, present, and future," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 497–508, Apr. 2012.

[16] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[17] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, Nov. 2014.

[18] D. Athukoralage, I. Guvenc, W. Saad, and M. Bennis, "Regret based learning for UAV assisted LTE-U/WiFi public safety networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–7.

[19] L. Babun, M. Simsek, and I. Güvenc, "Intercell interference coordination for D2D discovery in LTE-A HetNets," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 2202–2207.

[20] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 619–641, 2nd Quart., 2014.

[21] G. Baldini, T. Sturman, A. Dalode, A. Kropp, and C. Sacchi, "An emergency communication system based on software-defined radio," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 169, 2014.

[22] N. Baldo, "The ns-3 LTE module by the LENA project," Tech. Rep., 2011.

[23] N. Baldo, M. Miozzo, M. Requena-Esteso, and J. Nin-Guerrero, "An open source product-oriented LTE network simulator based on ns-3," in *Proc. 14th ACM Int. Conf. Model., Anal. Simulation Wireless Mobile Syst.*, 2011, pp. 293–298.

[24] G. Baruffa, L. Rugini, and P. Banelli, "Design and validation of a software defined radio testbed for DVB-T transmission," *Radioengineering*, vol. 23, no. 1, p. 387, 2014.

[25] D. Bates, S. Henriksen, B. Ninness, and S. R. Weller, "A 4 × 4 FPGA-based wireless testbed for LTE applications," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2008, pp. 1–5.

[26] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2011, pp. 96–111.

[27] M. Belleschi, G. Fodor, and A. Abrardo, "Performance analysis of a distributed resource allocation scheme for D2D communications," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 358–362.

[28] A. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, "Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian networks," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 98–103.

[29] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu, and X. Fu, "On simulation studies of cyber attacks against LTE networks," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2014, pp. 1–8.

[30] S. Bhattarai, S. Wei, S. Rook, W. Yu, R. F. Erbacher, and H. Cam, "On simulation studies of jamming threats against LTE networks," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 99–103.

[31] S. Bhattarai, S. Wei, S. Rook, W. Yu, D. Griffith, and N. Golmie, "Optimizing the location deployment of dynamic mobile base stations," in *Proc. IEEE Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 579–583.

[32] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux, "Security issues in next generation mobile networks: LTE and femtocells," in *Proc. 2nd Int. Femtocell Workshop*, 2010, p. EPFL-POSTER-149153.

[33] B. Bloessl, C. Leitner, F. Dressler, and C. Sommer, "A GNU radio-based IEEE 802.15. 4 testbed," in *Proc. GI/ITG KuVS Fachgespräch Drahtlose Sensornetze (FGSN)*, 2013, pp. 37–40.

[34] R. I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-D placement of an aerial base station in next generation cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–5.

[35] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[36] C. Capretti, F. Gringoli, N. Facchi, and P. Patras, "LTE/Wi-Fi co-existence under scrutiny: An empirical study," in *Proc. WiNTECH MobiCom*, 2016, pp. 33–40.

[37] M. Cesana, L. Fratta, M. Gerla, E. Giordano, and G. Pau, "C-VeT the UCLA campus vehicular testbed: Integration of VANET and Mesh networks," in *Proc. Eur. Wireless Conf. (EW)*, 2010, pp. 689–695.

[38] X. Chen, L. Chen, M. Zeng, X. Zhang, and D. Yang, "Downlink resource allocation for Device-to-Device communication underlaying cellular networks," in *Proc. IEEE 23rd Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 232–237.

[39] X. Chen, D. Guo, and J. Grosspietsch, "The public safety broadband network: A novel architecture with mobile base stations," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 3328–3332.

[40] Z. Chen, H. Zhang, W. G. Hatcher, J. Nguyen, and W. Yu, "A streaming-based network monitoring and threat detection system," in *Proc. IEEE 14th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, Jun. 2016, pp. 31–37.

[41] S.-M. Cheng, Y.-J. Wang, and Y.-C. Chen, "Secure location tracking of femtocells in heterogeneous cellular networks," in *Proc. IEEE Conf. Dependable Secure Comput.*, Aug. 2017, pp. 267–272.

[42] Z. Chu *et al.*, "Game theory based secure wireless powered D2D communications with cooperative jamming," in *Proc. Wireless Days*, Mar. 2017, pp. 95–98.

[43] M. Conti, F. Delmastro, G. Minutiello, and R. Paris, "Experimenting opportunistic networks with WiFi Direct," in *Proc. IEEE Wireless Days (WD)*, Nov. 2013, pp. 1–6.

[44] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[45] L. B. Dan Morse. (2017). *Ns-3 Tutorial Release Ns-3.21*. [Online]. Available: http://www.nsnam.org/docs/release/3.21/tutorial/ns-3-tutorial.pdf

[46] M. Diouf. *LTE-A Proximity-Based Services, Device-to-Device Communication Module for Ns-3*. [Online]. Available: https://github.com/makhtardiouf/d2d

[47] C. T. Do *et al.*, "Game theory for cyber security and privacy," *ACM Comput. Surv.*, vol. 50, no. 2, p. 30, Jun. 2017.

[48] S. Dolev, P. Florissi, E. Gudes, S. Sharma, and I. Singer, "A survey on geographically distributed big-data processing using MapReduce," *IEEE Trans. Big Data*, to be published.

[49] K. Dong, H. Ye, W. Wu, M. Yang, Z. Ling, and W. Yu, "Canoe: An autonomous infrastructure-free indoor navigation system," *Sensors*, vol. 17, no. 5, p. 996, 2017.

[50] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[51] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[52] H. ElSawy, E. Hossain, and M. S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 11, pp. 4147–4161, Nov. 2014.

[53] FCC. (Aug. 26, 2017). *Communications Status Report for Areas Impacted by Hurricane Harvey*. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DOC-346368A1.pdf

[54] G. Fodor *et al.*, "Design aspects of network assisted device-to-device communications," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 170–177, Mar. 2012.

[55] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, and N. Brahmi, "Device-to-device communications for national security and public safety," *IEEE Access*, vol. 2, pp. 1510–1520, Dec. 2014.

[56] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3049–3058, 2016.

[57] P. Gandotra *et al.*, "A survey on device-to-device (D2D) communication: Architecture and security issues," *J. Netw. Comput. Appl.*, vol. 78, pp. 9–29, Jan. 2017.

[58] W. Gao, J. Nguyen, D. Ku, H. Zhang, and W. Yu, "Performance evaluation of NETCONF protocol in MANET using emulation," in *Software Engineering Research, Management and Applications*. Springer, 2016.

[59] W. Gao, J. Nguyen, W. Yu, C. Lu, and D. Ku, "Assessing performance of constrained application protocol (CoAP) in MANET using emulation," in *Proc. Int. Conf. Res. Adapt. Convergent Syst.*, 2016, pp. 103–108.

[60] M. Gheisari, G. Wang, and M. Z. A. Bhuiyan, "A survey on deep learning in big data," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE) IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Jul. 2017, pp. 173–180.

[61] S. Giordani, M. Lujak, and F. Martinelli, "A distributed algorithm for the multi-robot task allocation problem," in *Proc. Int. Conf. Ind., Eng. Appl. Appl. Intell. Syst.*. Springer, 2010.

[62] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: An open-source platform for LTE evolution and experimentation," in *Proc. 10th ACM Int. Workshop Wireless Netw. Testbeds, Experim. Eval., Characterization*, 2016, pp. 25–32.

[63] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012.

[64] D. W. Griffith, A. Ben Mosbah, and R. Rouil, "Group discovery time in device-to-device (D2D) proximity services (ProSe) networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2017, pp. 1–9.

[65] M. J. Guezguez, S. Rekhis, and N. Boudriga, "Observation-based detection of femtocell attacks in wireless mobile networks," in *Proc. Symp. Appl. Comput.*, 2017, pp. 529–534.

[66] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 2, pp. 1123–1152,

[67] H. He and E. A. Garcia, "Learning from imbalanced data," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 9, pp. 1263–1284, Sep. 2009.

[68] A. Hematian, J. Nguyen, C. Lu, W. Yu, and D. Ku, "Software defined radio testbed setup and experimentation," in *Proc. ACM Int. Conf. Reliable Convergent Syst. (RACS)*, 2017, pp. 172–177.

[69] A. Hematian, W. Yu, C. Lu, D. Griffith, and N. Golmie, "A clustering-based device-to-device communication to support diverse applications," in *Proc. Int. Conf. Res. Adapt. Convergent Syst.*, 2016, pp. 97–102.

[70] L. Hu, "Resource allocation for network-assisted device-to-device discovery," in *Proc. 4th Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. (VITAE)*, May 2014, pp. 1–5.

[71] Y. Jararweh, A. Doulat, O. AlQudah, E. Ahmed, M. Al-Ayyoub, and E. Benkhelifa, "The future of mobile cloud computing: Integrating cloudlets and Mobile Edge Computing," in *Proc. 23rd IEEE Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–5.

[72] Y. Jiang, Q. Liu, F. Zheng, X. Gao, and X. You, "Energy-efficient joint resource allocation and power control for D2D communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6119–6127, Aug. 2016.
[73] F. J. Torra, "A service-constrained positioning strategy for an autonomous fleet of airborne base stations," M.S. thesis, Polytech. Univ. Catalonia, Barcelona, Spain, 2017.
[74] D. Karvounas, A. Georgakopoulos, K. Tsagkaris, V. Stavroulaki, and P. Demestichas, "Smart management of D2D constructs: An experiment-based approach," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 82–89, Apr. 2014.
[75] M. Khan, S. Alam, A. Mohamed, and K. A. Harras, "Simulating drone-be-gone: Agile low-cost cyber-physical UAV testbed," in *Proc. Int. Conf. Auto. Agents Multiagent Syst.*, 2016, pp. 1–2.
[76] I. Khoufi, P. Minet, A. Laouiti, and E. Livolant, "A simple method for the deployment of wireless sensors to ensure full coverage of an irregular area with obstacles," in *Proc. 17th ACM Int. Conf. Modeling, Anal. Simulation Wireless Mobile Syst.*, 2014, pp. 203–210.
[77] C. Krishnadev. *Maryland Governor Lifts State of Emergency in Baltimore*. Accessed: Aug. 14, 2015. [Online]. Available: https://www.npr.org/sections/thetwo-way/2015/05/06/404675117/maryland-governor-lifts-state-of-emergency-in-baltimore
[78] A. Kumbhar, I. Guvenc, S. Singh, and A. Tuncer. (2017). "Exploiting LTE-advanced HetNets and FeICIC for UAV-assisted public safety communications." [Online]. Available: https://arxiv.org/abs/1708.01226
[79] A. Kumbhar, F. Koohifar, I. Güvenç, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 97–124, 1st Quart., 2017.
[80] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," in *Cluster Computing*. Springer, 2017, pp. 1–13.
[81] A. Laha, X. Cao, W. Shen, X. Tian, and Y. Cheng, "An energy efficient routing protocol for device-to-device based multihop smartphone networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 5448–5453.
[82] L. B. Le, "Fair resource allocation for device-to-device communications in wireless cellular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 5451–5456.
[83] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, Jr., "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1–13, Jan. 2015.
[84] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96–104, Jun. 2012.
[85] Q. Li, Z. Tan, A. Jamdagni, P. Nanda, X. He, and W. Han, "An intrusion detection system based on polynomial feature correlation analysis," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 978–983.
[86] Y. Li, Z. Zhang, H. Wang, and Q. Yang, "SERS: Social-aware energy-efficient relay selection in D2D communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5331–5345, Jun. 2018.
[87] R. Liebhart, D. Chandramouli, C. Wong, and J. Merkel, *LTE for Public Safety*. Wiley, 2015.
[88] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2551–2566, Mar. 2017.
[89] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[90] X. Lin, J. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 40–48, Apr. 2014.
[91] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec. 2014.
[92] X. Lin, R. Ratasuk, A. Ghosh, and J. G. Andrews, "Modeling, analysis, and optimization of multicast device-to-device transmissions," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4346–4359, Apr. 2014.
[93] X. Lin *et al.* (2018). "Mobile networks connected drones: Field trials, simulations, and design insights." [Online]. Available: https://arxiv.org/abs/1801.10508
[94] X. Lin *et al.* (2017). "The sky is not the limit: LTE for unmanned aerial vehicles." [Online]. Available: https://arxiv.org/abs/1707.07534
[95] J. Liu, Q. Chen, and H. D. Sherali, "Algorithm design for femtocell base station placement in commercial building environments," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2951–2955.
[96] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1923–1940, 4th Quart., 2015.
[97] D. López-Pérez, M. Ding, H. Claussen, and A. H. Jafari, "Towards 1 Gbps/UE in cellular systems: Understanding ultra-dense small cell deployments," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2078–2101, 4th Quart., 2015.
[98] J. Lu *et al.* (2017). "Dynamic multi-arm bandit game based multi-agents spectrum sharing strategy design." [Online]. Available: https://arxiv.org/abs/1711.04365
[99] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct. 2014.
[100] Q. Lu, Q. Miao, G. Fodor, and N. Brahmi, "Clustering schemes for D2D communications under partial/no network coverage," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–5.
[101] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, and Z. Han, "Applications of economic and pricing models for wireless network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2735–2767, 4th Quart., 2017.
[102] J. Lyu, Y. Zeng, and R. Zhang, "Cyclical multiple access in UAV-aided communications: A throughput-delay tradeoff," *IEEE Wireless Commun. Lett.*, vol. 5, no. 6, pp. 600–603, Dec. 2016.
[103] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, "Placement optimization of UAV-mounted mobile base stations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 604–607, Mar. 2017.
[104] V. Mancuso, C. Vitale, R. Gupta, K. Rathi, and A. Morelli, "A prototyping methodology for SDN-controlled LTE using SDR," Tech. Rep., 2014.
[105] P. Mell *et al.*, "The NIST definition of cloud computing," Tech. Rep., 2011.
[106] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Mar. 2015, pp. 329–334.
[107] A. Merwaday, A. Tuncer, A. Kumbhar, and I. Guvenc, "Improved throughput coverage in natural disasters: Unmanned aerial base stations for public-safety communications," *IEEE Veh. Technol. Mag.*, vol. 11, no. 4, pp. 53–60, Dec. 2016.
[108] O. M. Alia, "Dynamic relocation of mobile base station in wireless sensor networks using a cluster-based harmony search algorithm," *Inf. Sci.*, vols. 385–386, pp. 76–95, Apr. 2017.
[109] S. Morgenthaler, T. Braun, Z. Zhao, T. Staub, and M. Anwander, "UAVNet: A mobile wireless mesh network using unmanned aerial vehicles," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2012, pp. 1603–1608.
[110] K. T. Morrison, "Rapidly recovering from the catastrophic loss of a major telecommunications office," *IEEE Commun. Mag.*, vol. 49, no. 1, pp. 28–35, Jan. 2011.
[111] A. B. Mosbah, D. Griffith, and R. Rouil, "A novel adaptive transmission algorithm for device-to-device direct discovery," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 177–182.
[112] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.
[113] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.
[114] J. Nguyen, Y. Wu, W. Gao, W. Yu, C. Lu, and D. Ku, "On optimal relay nodes position and selection for multi-path data streaming," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.
[115] H. Nishiyama, M. Ito, and N. Kato, "Relay-by-smartphone: Realizing multihop device-to-device communications," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 56–65, Apr. 2014.
[116] J.-S. Park, H. Yoon, and B.-J. Jang, "SDR-based frequency interference analysis test-bed considering time domain characteristics of interferer," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan./Feb. 2016, pp. 517–521.
[117] J.-S. Park, H. Yoon, and B.-J. Jang, "Software defined radio architecture survey for cognitive testbeds," in *Proc. 8th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2016, pp. 189–194.

[118] J. Peha, W. Johnston, P. Amodio, and T. Peters, "The public safety nationwide interoperable broadband network: A new model for capacity, performance and cost," Federal Commun. Commission, Washington, DC, USA, Tech. Rep. DOC-298799, 2010.
[119] K. Pei, Y. Cao, J. Yang, and S. Jana, "DeepXplore: Automated whitebox testing of deep learning systems," in *Proc. ACM Symp. Oper. Syst. Principles (SOSP)*, 2017, pp. 1–18.
[120] T. M. Phelps. *Baltimore Violence Updates: 10 Arrested After Curfew, Police Say*. Accessed: Apr. 28, 2015. [Online]. Available: http://www.latimes.com/nation/la-na-nn-baltimore-freddie-gray-20150427-htmlstory.html
[121] P. Phunchongharn, E. Hossain, and D. I. Kim, "Resource allocation for device-to-device communications underlaying LTE-advanced networks," *IEEE Wireless Commun.*, vol. 20, no. 4, pp. 91–100, Aug. 2013.
[122] A. Prasad, A. Kunz, G. Velev, K. Samdanis, and J. Song, "Energy-efficient D2D discovery for proximity services in 3GPP LTE-advanced networks: ProSe discovery mechanisms," *IEEE Veh. Technol. Mag.*, vol. 9, no. 4, pp. 40–50, Dec. 2014.
[123] A. Puri, "A survey of unmanned aerial vehicles (UAV) for traffic surveillance," Dept. Comput. Sci. Eng., Univ. South Florida, Tampa, FL, USA, Tech. Rep., 2005, pp. 1–29.
[124] L. Rabieekenari, K. Sayrafian, and J. S. Baras, "Autonomous relocation strategies for cells on wheels in public safety networks," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 41–44.
[125] T. D. Räty, "Survey on contemporary remote surveillance systems for public safety," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 40, no. 5, pp. 493–515, Sep. 2010.
[126] F. Richter and G. Fettweis, "Base station placement based on force fields," in *Proc. 75th IEEE Veh. Technol. Conf. (VTC Spring)*, May 2012, pp. 1–5.
[127] R. Rouil, F. Cintrón, A. Ben Mosbah, and S. G. Quintiliani, "A long term evolution (LTE) device-to-device module for ns-3," in *Proc. Workshop NS-3 (WNS3)*, 2016.
[128] A. Shahid, K. S. Kim, E. De Poorter, and I. Moerman, "Self-organized energy-efficient cross-layer optimization for device to device communication in heterogeneous cellular networks," *IEEE Access*, vol. 5, pp. 1117–1128, 2017.
[129] M. Sheng, Y. Li, X. Wang, J. Li, and Y. Shi, "Energy efficiency and delay tradeoff in device-to-device communications underlaying cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 1, pp. 92–106, Jan. 2016.
[130] D. Silver *et al.*, "Mastering the game of go without human knowledge," *Nature*, vol. 550, no. 7676, pp. 354–359, 2017.
[131] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2010, pp. 305–316.
[132] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.
[133] K. A. Suzuki, P. K. Filho, and J. R. Morrison, "Automatic battery replacement system for UAVs: Analysis and design," *J. Intell. Robot. Syst.*, vol. 65, nos. 1–4, pp. 563–586, 2012.
[134] H. Tang, Z. Ding, and B. C. Levy, "Enabling D2D communications through neighbor discovery in LTE cellular networks," *IEEE Trans. Signal Process.*, vol. 62, no. 19, pp. 5157–5170, Oct. 2014.
[135] M. Taranetz, T. Blazek, T. Kropfreiter, M. K. Müller, S. Schwarz, and M. Rupp, "Runtime precoding: Enabling multipoint transmission in LTE-advanced system-level simulations," *IEEE Access*, vol. 3, pp. 725–736, 2015.
[136] L. Tong, Y. Li, and W. Gao, "A hierarchical edge cloud architecture for mobile computing," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.
[137] A. Trotta, M. Di Felice, K. R. Chowdhury, and L. Bononi, "Fly and recharge: Achieving persistent coverage using small unmanned aerial vehicles (SUAVs)," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.
[138] E. Viegas, A. Santin, V. Abreu, and L. S. Oliveira, "Stream learning and anomaly-based intrusion detection in the adversarial settings," in *Proc. IEEE Symp. Comput. Commun.(ISCC)*, Jul. 2017, pp. 773–778.
[139] F. Wang, C. Xu, L. Song, and Z. Han, "Energy-efficient resource allocation for device-to-device underlay communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 2082–2092, Apr. 2015.
[140] G. Wang *et al.*, "Cognitive radio unified spectral efficiency and energy efficiency trade-off analysis," in *Proc. IEEE Military Commun. Conf.*, Oct. 2015, pp. 244–249.
[141] J. Wang, Y. Chen, X. Fu, J. Wang, W. Yu, and N. Zhang, "3DLoc: Three dimensional wireless localization toolkit," in *Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst.*, Jun. 2010, pp. 30–39.
[142] Q. Wang, W. Wang, S. Jin, H. Zhu, and N. T. Zhang, "Quality-optimized joint source selection and power control for wireless multimedia D2D communication using Stackelberg game," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3755–3769, Aug. 2015.
[143] R. Wang, K. Liu, D. Wu, H. Wang, and J. Yan, "Malicious-behavior-aware D2D link selection mechanism," *IEEE Access*, vol. 5, pp. 15162–15173, 2017.
[144] R. Wang, J. Yan, D. Wu, H. Wang, and Q. Yang, "Knowledge-centric edge computing based on virtualized D2D communication systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 32–38, May 2018.
[145] R. Wang, H. Yang, H. Wang, and D. Wu, "Social overlapping community-aware neighbor discovery for D2D communications," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 28–34, Aug. 2016.
[146] P. J. Weber and C. Lauer. *Hurricane Harvey Death Toll Hits 70*. Accessed: Sep. 7, 2017. [Online]. Available: https://www.nbcdfw.com/news/local/Hurricane-Harvey-Death-Toll-Hits-70-442918503.html
[147] S. Wei *et al.*, "On effectiveness of game theoretic modeling and analysis against cyber threats for avionic systems," in *Proc. 34th IEEE/AIAA Digit. Avionics Syst. Conf. (DASC)*, Sep. 2015, pp. 4B2-1–4B2-13.
[148] S. Wen, X. Zhu, Z. Lin, X. Zhang, and D. Yang, "Energy efficient power allocation schemes for device-to-device (D2D) communication," in *Proc. IEEE 78th Veh. Technol. Conf. (VTC Fall)*, Sep. 2013, pp. 1–5.
[149] Y. Wenger. *Damage to Businesses From Baltimore Rioting Estimated at About $9 Million*. Accessed: Aug. 14, 2015. [Online]. Available: https://www.washingtonpost.com/local/damage-to-businesses-from-baltimore-rioting-estimated-at-9-million/2015/05/13/5848c3fe-f9a8-11e4-a13c-193b1241d51a_story.html?utm_term=.534f561f7525
[150] D. Wu, J. Wang, R. Q. Hu, Y. Cai, and L. Zhou, "Energy-efficient resource sharing for mobile device-to-device multimedia communications," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2093–2103, Jun. 2014.
[151] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," *IEEE Trans. Multimedia*, vol. 19, no. 8, pp. 1908–1920, Aug. 2017.
[152] J. Wu and W. Zhao, "Design and realization of Internet: From net of things to Internet of Things," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 1, p. 2, Feb. 2016.
[153] Y. Wu, J. Wang, L. Qian, and R. Schober, "Optimal power control for energy efficient D2D communication and its distributed implementation," *IEEE Commun. Lett.*, vol. 19, no. 5, pp. 815–818, May 2015.
[154] D. Xenakis, M. Kountouris, L. Merakos, N. Passas, and C. Verikoukis, "Performance analysis of network-assisted D2D discovery in random spatial networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5695–5707, Aug. 2016.
[155] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema, "Toward integrating distributed energy resources and storage devices in smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 192–204, Feb. 2017.
[156] B. Yadranjiaghdam, N. Pool, and N. Tabrizi, "A survey on real-time big data analytics: Applications and tools," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2016, pp. 404–409.
[157] P. Yang, X. Cao, C. Yin, Z. Xiao, X. Xi, and D. Wu, "Proactive drone-cell deployment: Overload relief for a cellular network under flash crowd traffic," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2877–2892, Oct. 2017.
[158] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[159] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.
[160] J. Yoon, M. Y. Arslan, K. Sundaresan, S. V. Krishnamurthy, and S. Banerjee, "Self-organizing resource management framework in OFDMA femtocells," *IEEE Trans. Mobile Comput.*, vol. 14, no. 4, pp. 843–857, Apr. 2015.

[161] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.

[162] W. Yu, Z. Chen, G. Xu, S. Wei, and N. Ekedebe, "A threat monitoring system in enterprise networks with mobile devices," in *Proc. ACM Int. Conf. Reliable Convergent Syst. (RACS)*, 2013, pp. 300–305.

[163] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie, "An integrated detection system against false data injection attacks in the smart grid," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 91–109, 2015.

[164] W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie, "Ultra-dense networks: Survey of state of the art and future directions," in *Proc. 25th IEEE Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–10.

[165] W. Yu, H. Zhang, Y. Wu, D. Griffith, and N. Golmie, "A framework to enable multiple coexisting Internet of Things applications," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 637–641.

[166] W. Yu, N. Zhang, X. Fu, and W. Zhao, "Self-disciplinary worms and countermeasures: Modeling and analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 10, pp. 1501–1514, Oct. 2010.

[167] H. Yuan, W. Guo, and S. Wang, "Emergency route selection for D2D cellular communications during an urban terrorist attack," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 237–242.

[168] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[169] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[170] J. Zhang, L. Deng, X. Li, Y. Zhou, Y. Liang, and Y. Liu, "Novel device-to-device discovery scheme based on random backoff in LTE-advanced networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11404–11408, Dec. 2017.

[171] N. Zhang, W. Yu, X. Fu, and S. K. Das, "Maintaining defender's reputation in anomaly detection against insider attacks," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 3, pp. 597–611, Jun. 2010.

[172] Z. Zhou, M. Dong, K. Ota, R. Shi, Z. Liu, and T. Sato, "Game-theoretic approach to energy-efficient resource allocation in device-to-device underlay communications," *IET Commun.*, vol. 9, no. 3, pp. 375–385, 2015.

[173] D. Zhu, X. Yang, and W. Yu, "SPAIS: A novel self-checking pollution attackers identification scheme in network coding-based wireless mesh networks," *Comput. Netw.*, vol. 91, pp. 376–389, Nov. 2015.

[174] K. J. Zou *et al.*, "Proximity discovery for device-to-device communications over a cellular network," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 98–107, Jun. 2014.

[175] M. Zulhasnine, C. Huang, and A. Srinivasan, "Efficient resource allocation for device-to-device communication underlaying LTE network," in *Proc. IEEE 6th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2010, pp. 368–375.

WEI YU received the B.S. degree in electrical engineering from the Nanjing University of Technology, Nanjing, China, in 1992, the M.S. degree in electrical engineering from Tongji University, Shanghai, China, in 1995, and the Ph.D. degree in computer engineering from Texas A&M University in 2008. He is currently an Associate Professor with the Department of Computer and Information Sciences, Towson University, Towson, MD, USA. Before joining Towson University, he was with Cisco Systems Inc. for nine years. His research interests include cyberspace security and privacy, computer networks, cyber-physical systems, and distributed computing. He was a recipient of the 2014 NSF CAREER Award, the 2015 University System of Maryland (USM) Regents' Faculty Award for Excellence in Scholarship, Research, or Creative Activity, and the University System of Maryland (USM)'s Wilson H. Elkins Professorship Award in 2016. His work has also received Best Paper Awards from the IEEE ICC 2008, ICC 2013, the IEEE IPCCC 2016, and WASA 2017.

HANSONG XU received the B.S. degree from the City College, Xi'an Jiaotong University, Xi'an, China, in 2013, and the M.S. degree in electrical engineering from Lawrence Technological University in 2016. He is currently pursuing the Ph.D. degree at Towson University. His research interests include computer networks, Internet of Things, and machine learning. He received the Graduate Student Research Award and the Doctorial Research Fellowship in 2018.

JAMES H. NGUYEN received the B.S. degree in computer science from California State University, Hayward, CA, USA, in 2003, and the M.S. degree in telecommunications from the University of Denver in 2006. He is currently a Research Scientist with the U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC) at Aberdeen Proving Ground, MD, USA. Before he joined the U.S. Army, he worked at AT&T Bell Labs, Cisco Systems Inc., and Hi-Media Fotolog Inc., from 1997 to 2010. His research interests are Internet of Things, Internet architecture, routing, transport protocols, network management, and cyber security.

ERIK P. BLASCH (S'98–M'99–SM'05) received the B.S. degree in mechanical engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1992, the master's degrees in mechanical engineering in 1994, health science in 1995, and industrial engineering (human factors) in 1995 from Georgia Tech, Atlanta, GA, USA, and the Ph.D. degree in electrical engineering from Wright State University, Dayton, OH, USA, in 1999. He is currently a Principal Scientist with the United States Air Force Research Laboratory, Information Directorate, Rome, NY, USA. He has authored more than 650 scientific papers and book chapters. His research interests include information fusion, target tracking, pattern recognition, and robotics. He is a fellow of SPIE and an Associate Fellow of AIAA.

AMIRSHAHRAM HEMATIAN received the B.S. degree in computer's hardware engineering from the Azad University of Maybod, Yazd, Iran, in 2007, the M.S. degree in software engineering from University Teknologi Malaysia, Kuala Lumpur, Malaysia, in 2013. He is currently pursuing the Ph.D. degree in information technology at Towson University. From 2007 to 2011, he was in industry working on video broadcasting equipment and CAD/CAM systems. His research interests include wireless networks, biometrics, robotics, and signal processing. His current research encompasses device-to-device communication in LTE networks adopting software-defined radio systems and clustered mesh networks.

WEICHAO GAO received the B.S. degree from Fudan University, Shanghai, China, in 2005, the M.B.A. degree from the University of Michigan, Michigan, MI, USA, in 2011, and the M.S. degree in computer science and technology from Towson University, Towson, MD, USA, in 2017, where he is currently pursuing the Ph.D. degree. His research interests include Internet-of-Things, cyberspace security and privacy, and computer networks.