Physical Communication 41 (2020) 101109

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Surveying pervasive public safety communication technologies in the context of terrorist attacks

Ali Masood [a,*], Davide Scazzoli [b], Navuday Sharma [a], Yannick Le Moullec [a], Rizwan Ahmad [c], Luca Reggiani [b], Maurizio Magarini [b], Muhammad Mahtab Alam [a]

[a] Thomas Johann Seebeck Department of Electronics, Tallinn University of Technology, 12616 Tallinn, Estonia
[b] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Italy
[c] School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 12 December 2019
Received in revised form 17 April 2020
Accepted 27 April 2020
Available online 29 April 2020

Keywords:
Pervasive public safety communication (PPSC)
Critical communication
Long-term evolution (LTE) sidelink
Device-to-device (D2D) communication
Unmanned aerial vehicles (UAVs)
Localization
Beamforming
Software-defined networking
Routing protocols

ABSTRACT

Existing public safety networks (PSNs) are not designed to cope with disasters such as terrorist attacks, consequently leading to long delays and intolerable response times. First responders' life threats when accessing the attacked zone are more severe in comparison to other disasters and the accuracy of basic information such as the number of terrorists, the number of trapped people, their locations and identity, etc., is vital to the reduction of the response time. Recent technologies for PSNs are designed to manage natural disaster scenarios; these are not best suited for situations like terrorist attacks because a proper communication infrastructure is required for operating most of the classical PSNs. This serious concern makes it highly desirable to develop reliable and adaptive pervasive public safety communication technologies to counter such a kind of emergency situation. Device-to-device (D2D) communication can be a vital paradigm to design PSNs that are fit for dealing with terrorist attacks thanks to long-term evolution (LTE)-sidelink, which could allow the devices that people carry with themselves in the attacked zone to communicate directly. To our best knowledge, this is the first survey paper on public safety communication in the context of terrorist attacks. We discuss PSN scenarios, architectures, 3rd generation partnership project (3GPP) standards, and recent or ongoing related projects. We briefly describe a system architecture for disseminating the critical information, and we provide an extensive literature review of the technologies that could have a significant impact in public safety scenarios especially in terrorist attacks, such as beamforming and localization for unmanned aerial vehicles (UAVs), LTE sidelink for both centralized (base-station assisted) and decentralized (without base-station) architectures, multi-hop D2D routing for PSN, and jamming and anti-jamming in mobile networks. Furthermore, we also cover the channel models available in the literature to evaluate the performance of D2D communication in different contexts. Finally, we discuss the open challenges when applying these technologies for PSN.

1. Introduction

Pervasive public safety communication (PPSC) is critical in disaster scenarios such as terrorist attacks. Terrorism is an ominous threat worldwide. Terrorist attacks have not only damaged infrastructures and taken many innocent lives but also created long-term social and psychological repercussions on people. The number of attacks has raised significantly worldwide, especially after 2001 [1]. Recently, in Western Europe only, a record number of attacks (*i.e.*, 211) was reported in 2015 [2]. In 2016, 151 deaths and 548 injuries happened due to terror attacks in Belgium, France, Turkey, and Germany alone [3]. During 2003–2017, over 750 civilians have died because of terrorism in Europe [4]. The economic losses are huge; Belgium suffered losses up to 1 billion USD in 2016 [5]; in the same year the estimated loss in Paris region was of 858 million USD [6]. In particular, the tourism industry, which amounts to 10% of the European Union (EU) gross domestic product (GDP) [7], is suffering significantly. Similarly, in Asia and Africa, many lives were lost and significantly negative financial impacts are reported especially in Afghanistan, Iraq, Pakistan, Syria, and Nigeria [8,9].

Terrorist attacks are more critical than predictable emergency scenarios (e.g. floods, hurricanes). In predictable disasters, first responders have a reasonable time to prepare for expected incidents and can access the affected area during the emergency

* Corresponding author.
E-mail addresses: ali.masood@taltech.ee (A. Masood), davide.scazzoli@polimi.it (D. Scazzoli), navuday.sharma@taltech.ee (N. Sharma), yannickle.moullec@taltech.ee (Y.L. Moullec), rizwan.ahmad@seecs.edu.pk (R. Ahmad), luca.reggiani@polimi.it (L. Reggiani), maurizio.magarini@polimi.it (M. Magarini), muhammadmahtab.alam@taltech.ee (M.M. Alam).

https://doi.org/10.1016/j.phycom.2020.101109

Table 1
Comparison with existing surveys on emergency PSNs.

Ref.	PSN architecture		3GPP standards	On going projects	D2D communication		Beamforming/ Localization	Multi-Hop Routing	Jamming
	Natural disaster	Terrorist attacks			Centralized	Decentralized			
[10] 2013	[c]								
[11] 2014	[c]	[a]		[a]	[a]				
[12] 2017	[c]				[b]		[a]		
[13] 2018	[c]	[a]	[b]		[c]	[a]	[a]		
[14] 2019	[c]				[a]				
[15] 2019	[c]				[c]			[a]	
Our Survey	[c]	[c]	[c]	[c]	[c]	[c]	[c]	[c]	[c]

[a] Narrowly addressed.
[b] Partially addressed.
[c] Extensively addressed.

situation with some calculated life threats and take quick actions to rescue affected people. In contrast, one of the fundamental issues in most of the unpredictable emergency scenarios, especially in terrorist attacks, is the slow response time, as it is observed that, even after many hours, police and law enforcement agencies often remain unable to take immediate actions against terrorists due to serious life threats, unclear information, and situational facts such as the number of people trapped inside the affected zone, the number of terrorists, their location, the type of weapons, etc. [16,17].

From an information and communication technologies (ICT) point of view, which is the main focus of this paper, existing land mobile radio systems (LMRS) and LTE-based public safety networks (PSNs) are not designed and are not able to deal with the challenges of unpredictable emergency scenarios like terrorist attacks. Communication technologies like mission-critical push-to-talk (MC-PTT) [18], M-Urgency and Safe-City [19,20] are facilitating victims to share mobile data and live video streaming during disaster situations but require the proper network infrastructure. WiFi-Direct is an established technology that brings a solution to overcome such challenges by creating ad-hoc communication. However, WiFi-Direct faces connectivity problems when communicating with more than two devices [21]. During emergency scenarios, common social media websites like Facebook and Twitter become flooded with messages for help requests [22]. Such massive numbers of requests degrade the quality of service (QoS) of the existing network. Many researchers have proposed extended coverage approaches [23–25] to connect the out-of-coverage user equipment (UE) with the nearest base stations using relay communication for the public safety application. However, this is not useful in such disaster situations because the response time would be increased and rescue teams would not be able to take proper actions due to scattered information.

The main challenges in unpredictable emergency scenarios, such as terrorist attacks and earthquakes, are to establish connectivity when the base station is not available and send important information from an affected area to public safety services [16,17]. To establish and maintain connectivity in such non-trivial situations, long-term evolution (LTE) sidelink allows two devices to communicate directly with each other regardless of the base station [26,27]. To send important information to public safety services, it is important to disseminate basic information over the multi-hop device-to-device (D2D) network [23,25], connecting with unmanned aerial vehicles (UAVs) and, finally, reaching the deployed command center [28,29]. Once the fundamental information about the on-scene available (OS-A) devices is gathered, devices should conserve their energy to remain available for a long period of time. Such dynamic adaptation and intelligence at the device level are important in order to reduce the dissemination of redundant information. These challenges must be dealt with efficient routing, accurate positioning and, at the same time, a reliable communication network.

To cover the above-mentioned challenges in the given terror context, a comprehensive survey is provided with the following key contributions:

- A comprehensive description of scenarios, architectures, contributions from standards, as well as up-to-date list of funded projects.
- A survey of the technologies necessary for the given context including the point of view of direct communication between (i) on-ground devices, (ii) on-ground devices and UAVs, and (iii) UAVs. Important aspects such as localization, beamforming, suitable channel models, jamming and routing approaches are described in detail.
- Open challenges, which highlight the limitations and way-forward in terms of execution of the application scenario, architectures, and technologies.

There is a relatively limited number of surveys on emergency PSNs in the literature. In [10], the authors discussed future PSNs to provide voice communications to first responders. In generic terms, voice communications over LTE standard, known as VoLTE, can be implemented using four different methods: (i) circuit switched fallback (CSFB), (ii) One Voice/VoLTE, (iii) simultaneous voice LTE (SV-LTE), and (iv) voice over LTE via generic access network (VoLGA). The authors provided a detailed history of LMRS and a discussion on VoLTE as a vital feature of PSNs. Recommendations for implementing and testing the PSN according to the FirstNet architectures are given. The survey in [14] provides a basic overview of LMRS, LTE, and the 700 MHz radio spectrum for public safety. The existing non-mission-critical and mission-critical public safety services over LTE are briefly discussed. Advanced enabling technologies for PSNs, such as software-defined radio (SDR) access network and radio access network slicing, are presented. A comparative survey is presented in [12] with numerical simulation analysis of LMRS and LTE using the network simulator-3 (NS-3) simulator. In addition, the challenges involved with existing PSNs and the benefits of LTE based PSNs over LMRS are discussed. The development of PSN is presented along with the spectrum allocation for PSNs across all the frequency bands in the United States. In [11], the authors surveyed the status of many wireless technologies, e.g. TETRA, APCO 25, TETRAPOL, satellite networks, digital mobile radio, etc. for PSNs. The current regulatory, standardization and research activities are discussed to identify the recent challenges faced by PSNs in Europe and United States. A high-level overview of future wireless communication technologies, e.g. SDRs, cognitive radio and LTE, is provided. The authors of [13] present an overview of the existing literature on D2D communication and dynamic wireless networks (DWN) to support public safety communication. Open challenges and possible

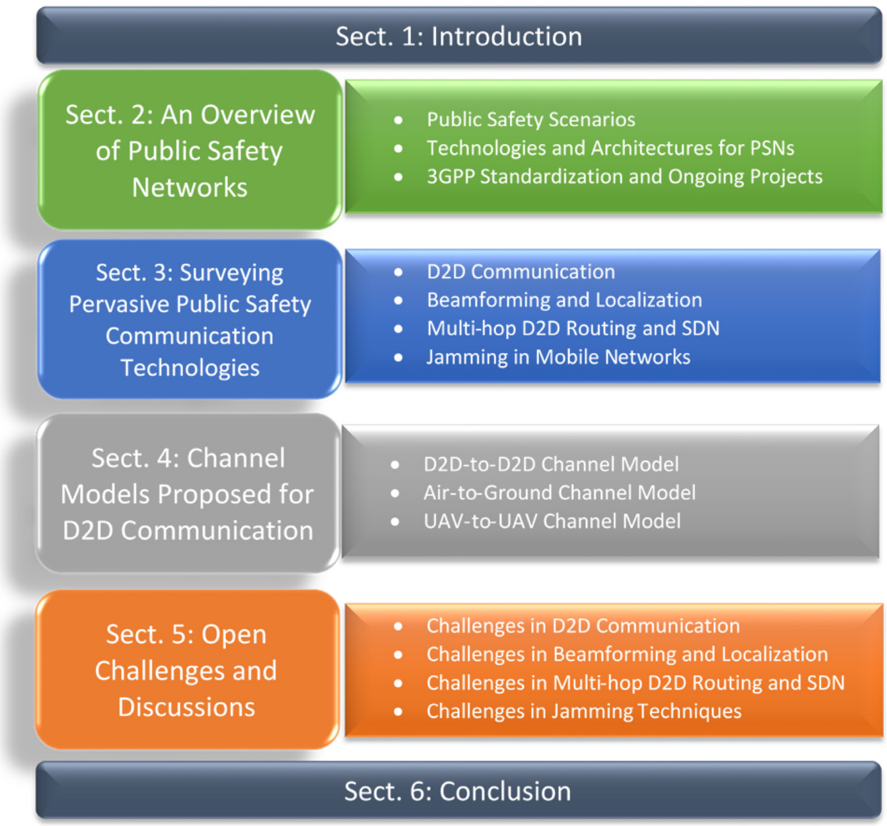

Fig. 1. An outline of this paper.

solutions for D2D communication, DWN deployment, modeling, security and resilience, modeling, performance evaluation, and emerging techniques for PSNs, e.g. IoT and cloud/edge computing, are discussed. Another survey in [15] provides the history of LMRS and LTE based PSNs, rapid emergency deployment, spectrum allocation and management requirements for public safety, architecture of LTE-based PSNs, and radio resource management schemes in PSNs.

We summarize and compare the contributions of different survey papers on PSNs in Table 1 to position the present paper. It can be seen from the table that all the existing papers focus on emerging technologies for predictable safety events (e.g. large-scale gatherings, and concerts); only two papers [11,13] barely discussed the architectures and technologies for unpredictable safety events such as terrorist attacks; more details about different emergency scenarios will be provided in Section 2.1. On the other hand, this survey provides a detailed description of the architecture and the possible technologies for predictable as well as for unpredictable dangerous events as, for example, in the case of terrorist attacks.

Moreover, the existing studies [11,13–15] cover many details about D2D communication in the in-coverage scenarios when the base station works properly. In comparison, to the best of our knowledge, this is the first survey paper presenting a detailed review of D2D communication for both in-coverage and out-coverage scenarios, along with up-to-date standards and projects. Additionally, we provide an extensive literature review of the technologies that could have a significant impact in advance PSNs, such as beamforming and localization for UAVs, multi-hop D2D routing, and jamming and anti-jamming in mobile networks.

The remainder of this paper is organized as follows. In Section 2, we discuss PSN scenarios, architectures, 3GPP standards and recent, or ongoing, related projects. Section 3 is devoted to the technologies with a potential impact in this scenario and it is divided into the Physical, MAC and Network layer subsections. In Section 3.1 – the physical layer – device discovery, beamforming for UAVs and localization are discussed as the technologies with the greatest expectations and challenges to the specific terrorist scenario. In Section 3.2 – the MAC layer – D2D communication in centralized and decentralized modes, resource, and power allocation approaches are considered as playing a crucial role in the achievement of an efficient communication. In Section 3.4 - the network layer - multi-hop D2D routing for PSN is carefully discussed as a key enabling technology for the system. In Section 3.5, the main characteristics of jamming are discussed together with a survey of the recent literature. Then Section 4 is dedicated to the channel models proposed for D2D communication in the literature. Finally, in Section 5, we discuss the open challenges in the context of these technologies applied to PSN in the case of terrorist attacks. Concluding remarks are given in Section 6. Fig. 1 shows an outline of the paper.

2. Public safety scenarios, architecture, standards, projects

2.1. Public safety scenarios

Each year, thousands of people suffer because of disasters and this situation worsens if public safety services are not able to take proper actions on time. Any emergency situation can be referred to as a disaster that can affect the routine procedures causing deaths, illness, injuries and property damage [30,31]. For classification purposes, disasters are categorized into two main groups: natural and man-made disasters. Both of them can be further divided into different subgroups [32–34]. as shown in Fig. 2.

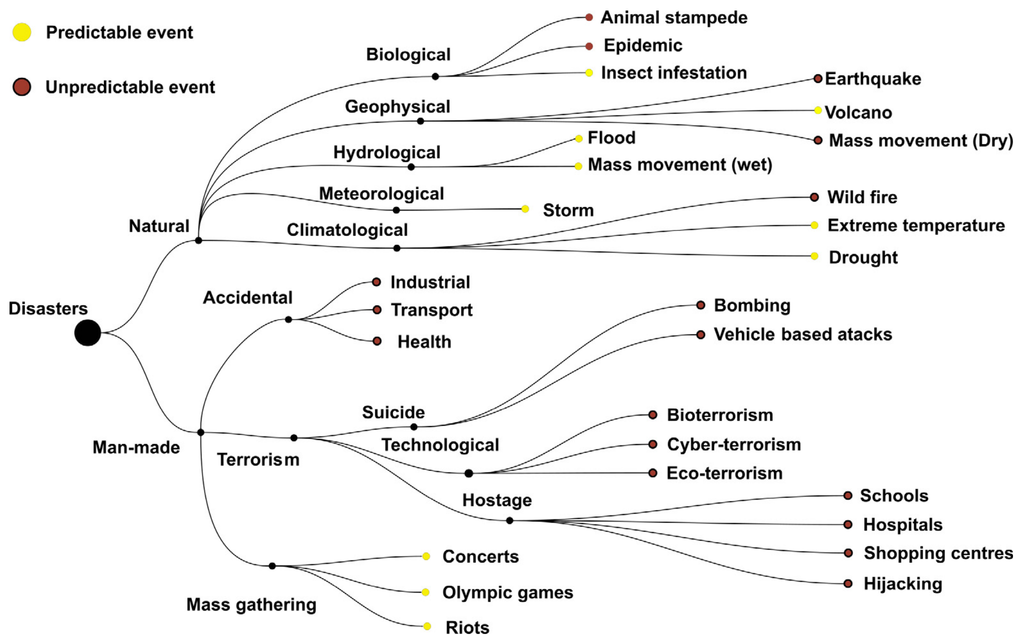

Fig. 2. A taxonomy of disaster types.

2.1.1. *Natural disasters*

People depend on key facilities for ensuring viable and safe societies; such facilities include e.g. transportation systems, energy and fuel subsistence systems, information and communications infrastructure, schools, hospitals, emergency rescue services, etc. [35–37]. It is observed that natural disasters can disable some of the key infrastructure facilities in affected areas up to 72 h or even longer, which not only threatens the lives of people but can also isolate such areas from the outside world [38]. Risk management techniques help to manage natural disasters, estimating which areas will become isolated or not. Studies assess the conditions of key facilities before, during, and after disasters, which can help to manage and reduce their consequences [39–42]. It is worth observing that people often use social media platforms to request aid during natural emergencies [43–45]. Information shared on social media is very ambiguous while rescue services using machine learning methods can differentiate between spam and clear signal, thus allowing to identify who actually needs aid [46–49].

- **Geophysical:** Disasters originating from solid earth are referred to as geophysical or geological disasters (e.g., ground movement, tsunami, landslide, lava flow, etc.). Such disasters cause deaths, injuries and infrastructure breakdown. It is observed in several disasters that damaged roads, bridges, and communication infrastructure are the main obstacles to providing emergency support and aid [50,51].
- **Hydrological:** Sudden distribution or movement of water (e.g., flood, debris flow, avalanche, etc.), possibly on dry land, causes hydrological disasters. Such disasters partially or fully disconnect the ground connection of affected areas, which is one of the main challenges faced by rescue teams [38,52].
- **Meteorological:** Short-lived disasters caused by intermediate atmospheric conditions (e.g., tornado, thunderstorm, dust storm, excessive rainfall, blizzard, etc.) are called meteorological disasters. Extreme weather conditions affect the rescue process causing long delays [53].
- **Climatological:** Long-lived disasters caused by extreme atmospheric conditions (e.g., frost, snow pressure, icing, etc.) are called climatological disasters. Such disasters cause economic loss, property damage, communications failures, and extreme burden on public safety services such as hospitals, fire, police, etc. [54].
- **Biological:** Biological disasters caused by the exposure of living organisms to germs and toxic substances such as viral diseases, bacterial diseases, fungal diseases, etc. A significant number of cases appear in a virus-free region, spread from affected areas. The challenge for public safety services in such cases is to provide antibiotics and vaccines for infection prevention and control [55]. It is also observed during the epidemic situation that public safety services use drones to monitor the movement of people to contain the virus outbreak [56].

2.1.2. *Man-made disasters*

Man-made disasters are the consequence of different human actions and can be categorized into two main subgroups: accidental, civil disobedience and terrorism.

Accidental disasters

Accidental disasters are caused by human error, negligence, and technological failure, for instance, fires, industrial and transport accidents, structural failures and collapses, and nuclear explosions or radiation. Many studies on risk assessment propose quantitative, qualitative, and hybrid techniques to examine and assess risk solutions to avoid such events [57–59].

Mass gathering

A mass gathering is an event for a common purpose when a large number of persons come close together at one place; it can take place indoor or outdoor. The gathering could be organized for a defined period, be instantaneously motivated by participants or organizers, or due to an emergency situation.

Terrorism

Terrorism is the deliberate use of violence for creating fear in order to achieve political and social objectives. Terrorist activities are diversified, having a large range of targets, including citizens, government officials, law enforcement officers, public building, or government buildings [60].

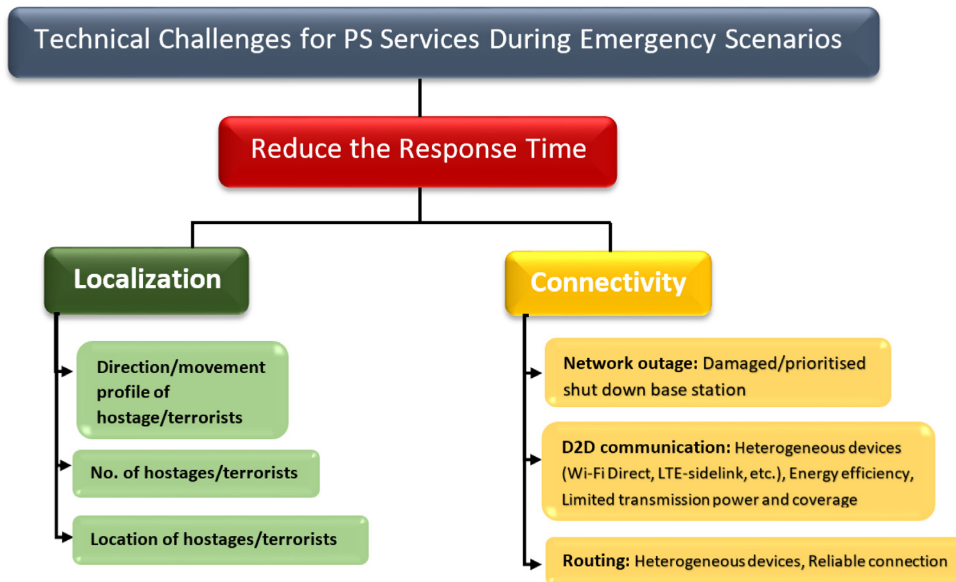

Fig. 3. Technical challenges for PS services during emergency scenarios.

- **Suicide Attacks:** in a suicide attack, a terrorist deliberately takes his own life to damage, harm, or destroy the target. Two counter tactics are used to fight against suicide terrorism: nonlethal preventive measures and lethal offensive measures. In nonlethal measures, law enforcement agencies arrest the terrorists and leaders, and drive information from them. In lethal offensive measures, agencies target the terrorist leaders or operators and kill them. Target killings appear to further increase the number of suicide attacks, while preemptive arrests seem to reduce such attacks [61, 62].
- **Technological Attacks:** such attacks attempt to expose, steal, alter, destroy, or gain unauthorized assets or access. Risk assessment strategies propose to prevent such activities, while it is challenging for law enforcement agencies to identify the criminals and their network [63–65].
- **Hostage Situation:**
  Hostage situation is considered as one of the most significant and newsworthy scenarios, which affects and challenges the actions of the authorities [16,66,67]. There are two main scenarios: (i) where hostages are captured by the terrorist or (ii) where hostages are hiding in the area controlled by the terrorists. Law enforcement agencies cannot take a proper action during hostage situations because they do not have critical information such as the number of terrorists, the number of trapped people, their identity and locations, etc. [16,17].

We further categorize the emergency scenarios, i.e. man-made and natural disasters, into two types of events: predictable and unpredictable. In predictable emergency scenarios, public safety services (rescue, fire, police, etc.) can foresee and have a reasonable time to prepare for expected incidents. Generally, public safety services put high efforts into disaster prevention in order to reduce the response time, thus, they will not have to put significant efforts into the disaster management and relief phase. For instance, in a predictable man-made disaster that could take place during e.g. a mass gathering, police departments arrange additional police force to provide security, implement safety arrangements for the crowd and ensure avoiding any undesired incident. Fire and rescue teams are also fully prepared to meet any incident. In a predictable natural disaster, for example floods, rescue teams evacuate the possible affected area for prevention, whereas during or after the emergency incident, damaged infrastructures are the major cause of the formation of isolated areas and a factor that slows down the rescue process. The emergency rescue teams gain access to the disaster site using e.g. rescue boats and helicopters with a slight (if not without) direct life threat and provide disaster relief immediately.

On the other hand, in unpredictable emergency scenarios, public safety services may not get enough time for disaster prevention due to the abruptness of the incident. Thus, a great amount of effort will have to be put into the disaster management and relief phase to reduce the response time. Typically, wildfires and earthquakes are considered as unpredictable natural disasters. Human failures and terrorist attacks are common examples of unpredictable man-made disasters. For instance, in the case of terrorist attacks, rescue and law enforcement teams remain unable to immediately step-in because of serious life threats, unclear information and situational facts (i.e., number of terrorists, their positions, the number and type of weapons used and severe consequences, etc.) Thus, the response time for disaster relief becomes very long.

Nowadays, concerns are raising for the design of highly reliable and adaptive PSNs. From an ICT point of view, the classical PSNs are not designed to cope with public safety services during emergency scenarios (e.g., floods, earthquakes, riots, terrorist attacks). The main challenge for public safety services is to reduce the response time in such cases, as illustrated in Fig. 3. We are discussing a system architecture in Section 2.2 for disseminating the up-to-date information and reduce the response time, exploring the technologies that could have a significant impact in such scenarios, such as beamforming and localization from UAVs, LTE sidelink for both centralized (base-station assisted) and decentralized (without base-station) architectures, and multi-hop D2D routing for reliable PSN.

2.2. Technologies and architecture for PSNs

Technologies for PSNs

When BSs are switched off or non-functional, mobile users are not able to communicate with first responders. A feasible solution to overcome this problem is to relay the signals via other devices that act as a link between users and operational BSs using D2D

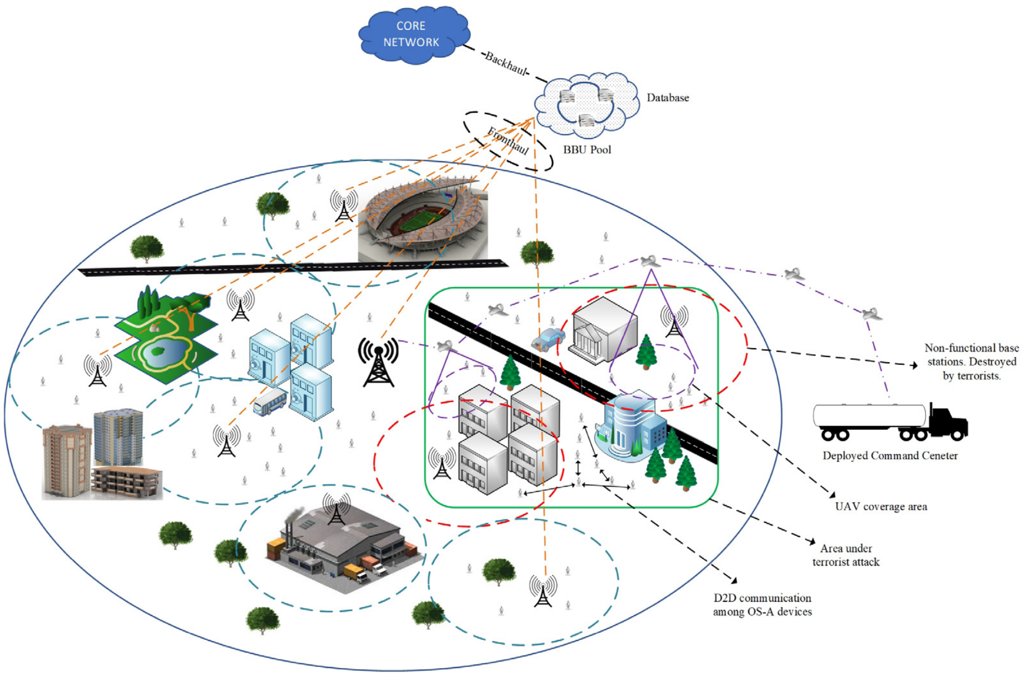

Fig. 4. Architecture for public safety scenarios.

communication. In particular, the UEs that are not in the coverage area of the BS can use the mobile devices that are in the coverage area as relays, thus accomplishing a multi-hop connection with the cellular network [68]. Under exceptional circumstances, these D2D links, standardized in the 3GPP Release 13, play an important role in filling coverage holes and providing seamless coverage. Due to the division of the transmission range into two or more hops using D2D relays, the reduction in power consumption of mobile devices becomes one of the major benefits of such relayed communication. Further, with low link distance between the D2D devices, the battery life of the devices is prolonged, which is highly beneficial especially in critical conditions.

Reference [69] proposes a relay selection scheme for D2D enabled relay communication, as a measure to fill coverage holes in public safety LTE (PS-LTE). The scheme is based on selecting an optimal relay terminal through an effective path throughput from an out-of-coverage terminal to a BS via in-coverage relay terminal. From the simulation results in [69], the proposed scheme is able to satisfy the throughput requirement for video transmission in case of a large number of users.

It is worth observing that relaying of signals can also be done through moving relays e.g. devices that are installed on moving vehicles such as UAVs or trucks. In [28], a cost-effective network architecture is proposed where a smart UAV enabled with D2D communication is deployed to carry a relay that provides the connection. The use of drones is more feasible when the risk factor is high. This allows public safety agents to deploy relays in some area, which is the case considered here of a terrorist attack.

A drone, or swarm of drones, is directed towards a certain location to connect the desired mobile devices that need coverage with a distant active BS, thus acting as a relay to bypass failed BSs. The drones are installed on-board the transceivers to transfer the signals from the mobile devices to the distant BSs, and vice-versa, thus realizing a multi-hop link. However, the number of drones that is required to cover the affected area depends on the cell coverage provided by each drone, which is lower as compared to terrestrial microcell BSs and further depends on its transmission power, drone altitude, interference effects, etc., as addressed in [70]. The problem of searching for the optimal UAV position to increase the end-to-end throughput performance is addressed in [29]. In contrast to methods that rely on propagation distance minimization and statistical models for the presence or absence of a line-of-sight (LoS) component, the proposed approach is capable of leveraging local topological information to guarantee better performance. The position of drones is set by utilizing GPS and location detection services in LTE.

Architecture for public safety scenarios

It is envisioned that smartphones, and/or OS-A devices, which have enabled direct communication features in the emergency scenarios (such as earthquakes, fire, terrorist attacks), can be exploited to get the fundamental and critical information to reduce the response time [26,27]. Inside the affected area, enabled OS-A devices with D2D functionality could cooperate with each other in a multi-hop communication fashion to improve the communication reliability in case of harsh propagation conditions and to ensure end-to-end network connectivity [23,25]. An external deployed command center and aerial platforms (APs), or UAVs, will be deployed near the attacked zone. Multiple APs/UAVs can provide reliable network connectivity, increased positioning accuracy in the OS-A devices, and relay communication to external deployed command center when the BS is not available, especially when the signal power is too weak to propagate [28,29]. Hence, this network architecture can disseminate up-to-date critical information to the deployed command center, thus allowing for a reduction of response time and the provisioning of a robust and reliable connectivity [71,72], as shown in Fig. 4.

The considered architecture is feasible for public safety scenarios, like fire, earthquake, terrorist attacks, etc., and can be divided into the following three parts:

1. **Mobile BS Architecture:** The central unit of command will have a system capable of enabling emergency responder personnel for obtaining a deep control of the operations; its architecture is shown in Fig. 5. An SDR based connection will emulate the BS connectivity services for scenarios where cellular connectivity is totally unavailable. Information coming from the drone fleet will be collected in a local

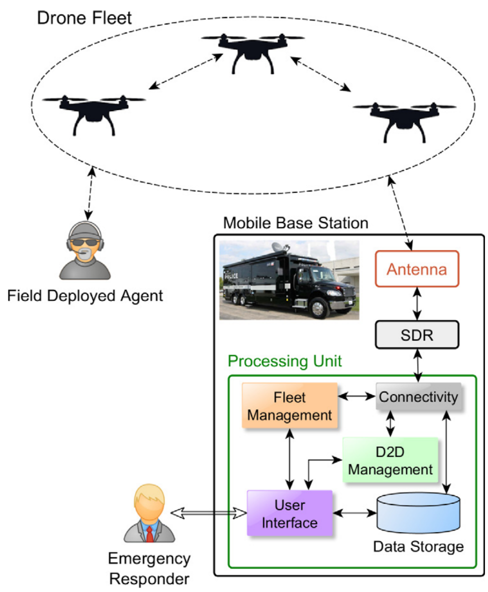

Fig. 5. Mobile BS main components and architecture.

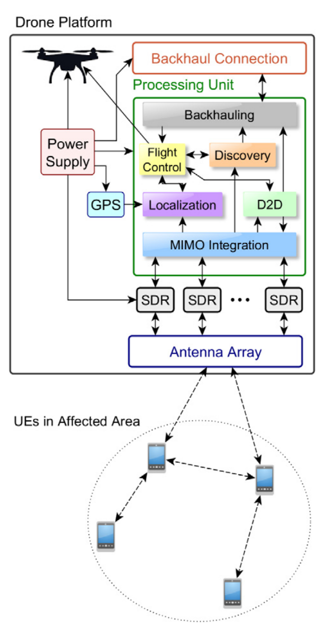

Fig. 6. UAV Remote Radio Head main components and architecture. Within the multiple-input-multiple-output (MIMO) integration block other sub-algorithms such as beamforming and weak signal detection will be included.

database. This information will include UE localization data as well as data coming from victims and field-deployed agents. A fleet management protocol will enable the emergency responders to deploy the UAV fleet where it is most needed during operations.

2. **UAV Unit Architecture:**
The system to be deployed on the UAV is shown in Fig. 6. It includes various components for achieving device discovery, beamforming, and localization. The system is divided into:

- an antenna array;
- an SDR component, responsible for the phase rotation to be applied on each antenna;

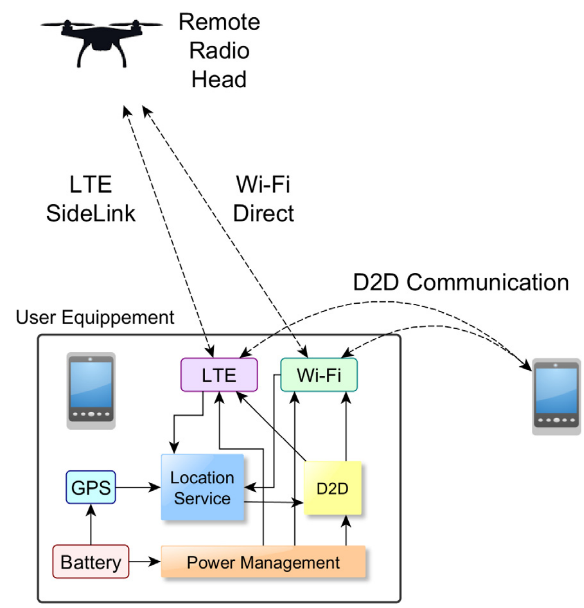

Fig. 7. Expected architecture and components for typical UEs.

- the main processing unit on which the algorithms developed in the project will be deployed and interact with drone flight controls. These algorithms will take the inputs of the MIMO antenna system and perform UE localization, beamforming, and D2D communication.

The priorities of the individual algorithms w.r.t. access to the flight controls will vary during the mission, with the initial phases prioritizing device discovery and localization and, later, the D2D and backhaul connectivity. The power supply will change the behavior of the UAV according to its charge levels. A separate connection from the main antenna array will be used to provide backhaul connectivity to the ground stations.

3. **UE Architecture:** The UE contains WiFi and/or LTE modules, able to provide D2D connectivity (Fig. 7). The D2D link can be established with the UAV or to other UEs in the area. User location services such as GPS can be used to aid in connectivity and localization if present and active.

2.3. 3GPP standardization and ongoing projects

In Release 12, the 3GPP recognized D2D communication as a potential contender to manage the network capacity/coverage problem, through ProSe [73,74]. Further enhancements in ProSe with integration to internet-of-things (IoT) and vehicle-to-everything (V2X) communications became a part of future releases as depicted in Fig. 8. D2D services can be exploited by introducing new features and functionalities in the current cellular architecture, which are addressed in this section. D2D is expected to be integrated into existing LTE-A cellular networks as presented in [75]. Further, the requirements of the features that would support such integration are addressed in [76] such as enhancement of the evolved packet core (EPC) with the addition of new interfaces and entities to support D2D services. Later, the results from [76] formed the foundation for the specification of 3GPP Release 12 [77]. With this release three main entities were introduced in the network: ProSe function, ProSe Application Server, and ProSe application at the UE.

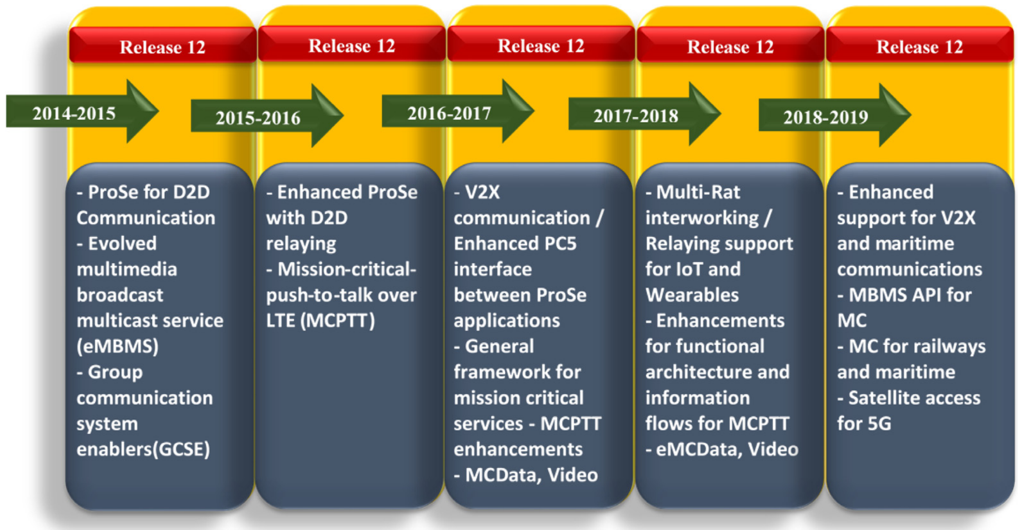

Fig. 8. Mission Critical and D2D service Enhancements with 3GPP releases.

The ProSe function is executed as a logical function, which further provides three sub-functions: Direct Provisioning, Direct Discovery Name Management, and EPC-level discovery ProSe function. Direct Provisioning function caters to D2D discovery and D2D communication. Such criteria, which are related to the authorization policy and radio parameter configuration of UE to perform D2D discovery and communication, are listed in [77]. The Direct Discovery Name Management Function supports the network operator for D2D discovery and application while the EPC-level Discovery ProSe Function provides some network functionalities such as subscriber information management and authorization etc. In 3GPP Release 12, only the ProSe function is considered. Therefore, management and cooperation among multiple ProSe functions are left as an open challenge.

Further, the ProSe application server [78] distributes services to different ProSe applications and maps the UEs to individual functions. The ProSe application server is connected to the ProSe function via a PC2 interface, which is responsible for enabling interaction between the two entities, as given in [78]. Also, UEs must be reconfigured to support D2D communication and relay functionality with extensions required to support D2D discovery and communication by the ProSe application. Such an authorization policy is managed over a PC3 interface as described in [79].

The basic architecture of 3GPP ProSe is shown in Fig. 9. Besides new entities, home subscriber server (HSS) and mobility management entity (MME) should also be enhanced in order to authorize user information regarding ProSe services [77]. To accomplish this, a new interface, PC4, has been introduced in [80] and is shown in Fig. 9. Also, the upgrade of the S6a interface is needed to enable information exchange related to ProSe subscription [77]. Such enhancements in interfaces and introduction of new entities lead to security threats and risks related to D2D communication; therefore, [81] proposes a key management system among common LTE-A and newly introduced entities.

Further, the 3GPP meeting for the integration of D2D services into IoT was discussed in [82], which would meet the requirements of longer battery life and better connectivity of IoT devices in close proximity by forming D2D connections.

Also, wearable devices for medical care systems for patient monitoring in hospitals and remote monitoring from homes and offices gained a lot of improvements from D2D communication. A review of multiple standards and technologies for D2D enabled wearable cognitive wireless systems is given in [83]. Enhancements have been also introduced to enable QoS, end-to-end security, and efficient path switching between LTE and D2D interfaces [84]. In Release 14, V2X was included for the first time in D2D communications with improvements done for safety-related scenarios and extended sensors local communication [85]. In addition to the above mentioned standardization activities, many completed or active research projects are summarized in Table 2.

- **BSA-D2D:** Base Station Aided D2D communication is an initiative of the European Commission (EC) [86]. The main aim of this project was to increase the system capacity by exploring network coding, interference alignment, regenerative storage codes, multiple description source coding and joint source-channel coding.
- **MCN:** Multilayered Communication Network is an initiative of the Japanese government for research in disaster Management [87]. The objective of this project was to establish an alternative communication route and technologies when the 3G network is not available.
- **ABSOLUTE:** Aerial BSs with Opportunistic Links For Unexpected and Temporary Events (ABSOLUTE) project is a Framework Programme 7 (FP7) initiative that aims to design and validate innovative rapidly deployable networks [88].
- **CODEC:** The Cellular Network based D2D Wireless Communication (CODEC) project is funded under FP7 framework [89]. It focuses on achieving QoS, energy and spectral efficiency through efficient resource management in D2D Cellular communications.
- **D2D-LTE:** Device-to-Device Communication: Fundamentals with Applications to LTE (D2D-LTE) is a project funded by the National Science Foundation (NSF), USA [90]. The key idea is to exploit direct communication between nearby devices to achieve throughout, improved spectrum utilization and energy efficiency. In addition, this project explores new peer-to-peer and location-based applications and services.
- **PSS:** Pervasive Spectrum Sharing (PSS) for public safety communications is an NSF funded project [91]. The main aim of the project is to improve spectral efficiency. The main idea is to provide incentives to users that opportunistically share their spectrum as substrates (*e.g.*, 3G data and WiFi connectivity), and open D2D protocols.

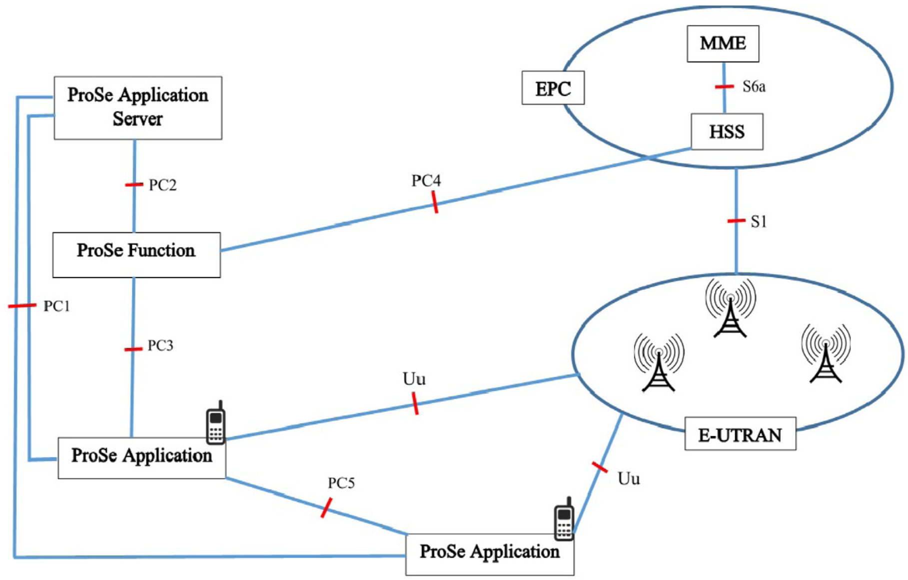

Fig. 9. D2D communication architecture with enhancements from LTE-A.

- **COHERENT:** The coordinated control and spectrum management for 5G heterogeneous radio access networks (COHERENT) framework aims at improving the existing control solutions for inter-network coordination [92]. The project is funded by Horizon 2020 (H2020) programme. It devises theories and methods to abstract network states and behaviors.
- **METIS:** Mobile and wireless communications Enablers for Twenty-twenty Information Society (METIS) is a research project funded by FP7 [93]. The objective of the project is to design a system concept that delivers the necessary scalability, efficiency, and versatility for a 5G wireless communications system. Direct D2D communication is one potential technology and is used to improve coverage in terms of availability, reliability and cost efficiency.
- **UAV4PSC:** CAREER: Towards Broadband and UAV-Assisted Heterogeneous Networks for Public Safety Communications (UAV4PSC) is an NSF funded project [71]. The main idea of this project is to use UAVs along with cellular technologies to ensure connectivity with potentially damaged network infrastructures, dynamically manage interference between UAV, BS, UE, and allow smooth handovers.
- **NICER:** Networked Infrastructure-less Cooperation for Emergency Response (NICER) is a LOEWE funded project [94]. It explores how infrastructure-less information and communications technology that can establish links between people in the event of a crisis, thus enabling them to work together to overcome the crisis.
- **BROADMAP:** BROADMAP is another H2020 funded project [95]. The project aims to develop next generation broadband inter-operable radio communication systems for public safety and security in the EU. BROADWAY [98] is a new project working on carrying forward BROADMAP initiatives.
- **LCMSSER:** Location-based Control and Management System for Safety and Emergency Rescuing Services using LTE D2D (LCMSSER) is a British Council funded project through its Newton Fund initiative [96]. The aim of the project is to support mobile users through the location-based system that provides emergency services in the event of disasters.
- **DDPS:** The DDPS project aims at providing mission-critical voice, 3GPP ProSe, one to one and one to many group communication as key services [97]. The project is funded by the National Institute of Standards and Technology (NIST) and the main partners are US Army Vencore Laboratory and Eurecom. The project involves building a complete ProSe stack for mission-critical voice based on 3GPP standard and open source OpenAirInterface (OAI) and demonstrate in a hardware test-bed.
- **COUNTER-TERROR:** COmmUNication in conTExt Related to Terror Attacks (COUNTER-TERROR) is a new project that has been recently funded by the North Atlantic Treaty Organization (NATO) within the science for peace and security (SPS) programme [72]. The project aims to establish and maintain connectivity in the case of terrorist attacks, which cause partial or total network failure, exploiting multi-hope D2D communication, beamforming and localization, and jamming and anti-jamming techniques for reliable PSN.

3. Surveying pervasive public safety communication technologies

3.1. Physical layer

The main physical layer technologies that make possible a decentralized communication and related services in an area that is concerned with a terrorist attack are:

- *Discovery* of the devices for establishing D2D communications, in particular with the support of aerial relaying stations. In fact, before setting up a direct D2D communications, user devices need to discover the presence of nearby devices, or UAVs, and identify whether the D2D pairs need to communicate with each other. This process, called device discovery or peer discovery, is particularly challenging when the infrastructure is not available.
- *Beamforming*, for enhancing signal quality in any context of the operations, from discovery and detection of the weak signals in the area of localization and communications. In particular, in the scenario considered here, the papers of interest are dedicated to the application of beamforming to UAVs that are deployed in the emergency area.
- *Localization* of the devices, useful for providing additional information about the positions of the persons involved in the attack.

The next subsections are devoted to the survey of the main recent papers in the above-mentioned areas.

Table 2
Summary of the up-to-date related funded Projects.

Projects	Year	Funding organization	Architecture	Standards	D2D communications	Protocols stack	Target applications
BSA-D2D [86]	2011–2012	FP7 Ref. Nr:274523	LTE	In-coverage	Improve network capacity	PHY layer	Cellular communication
MCN [87]	2011–2012	Japanese Government	WiFi Adhoc	Zigbee, Bluetooth, WiFi, LTE-A, WiGig	Delivery delay	Network Layer	Disaster management
ABSOLUTE [88]	2012–2015	FP7 Ref. Nr. ICT 318632	LTE-A	In-coverage mode: Direct and relay	Aerial BS to device	PHY layer	General purpose public safety
CODEC [89]	2014–2016	FP7 Ref. Nr: 630058	LTE- Re-lease 12	LTE-A, TETRA	Spectrum efficiency	PHY layer	Cellular communication
D2D-LTE [90]	2014–2016	NSF, USA Ref. Nr: CIF 1016649	LTE Release 12. ProSe design	In-coverage mode: Offloading, relay and direct	Spectrum, resource optimization	PHY layer	General purpose public safety
PSS [91]	2016–2019	NSF, USA Ref. Nr: NSF EARS2014–1443946	LTE	In-coverage mode, WiFi spectrum sharing	Spectrum efficiency	PHY layer	General purpose public safety
METIS-II [93]	2015–2017	H2020 Ref. Nr. 671680	5G	5G Hetnet	Spectrum, resource allocation	PHY layer	General purpose public safety
UAV4PSC [71]	2015–2020	NSF, USA Ref. Nr:CNS-1453678	5G	In-coverage mode:Offloading, relay and direct	UAVs to ensure connectivity	PHY and MAC layer	General purpose public safety
NICER [94]	2015-On going	LOEWE	5G	WiFi, LTE-A, LTE-U	Relays for out of coverage users	Network layer and security	Emergency response for disaster, terrorism and violence
BROADMAP [95]	2016–2017	H2020 Ref. Nr. 700380	Interoperable, broadband (LTE)	Multiple standards	Interoperability of devices	Interopera bility of different networks	Public safety in disasters
LCMSSER [96]	2016–2018	Newton Fund British Council	LTE	LTE	Relays for out of coverage users	PHY layer	Public safety in disasters
DDPS [97]	2017–2019	NIST	LTE-Release 14	On-network, Off-network, and Partial-on-network	Discovery, syn-chronization,	PHY, MAC, and Network layers	Public safety in disasters
COUNTER-TERROR [72]	2018–2021	NATO-SPS	LTE-Release 14 (ProSe design and evaluation)	Out-of-coverage mode:Direct, relay and multihop	Dynamic heterogeneous resource management, reliable and robust connectivity	PHY, MAC, and Network layers	Public safety in terrorist attack

3.1.1. Device discovery

In a disaster scenario, one of the main problems is the discovery and selection of the devices with the best signal-to-interference-and-noise ratio (SINR) and the implementation of algorithms that are able to guarantee a sufficient QoS.

According to 3GPP, "direct discovery" expresses the capability of communicating only among the UEs.

In general, devices that are announcing their presence to the neighbors broadcast discovery messages at pre-defined intervals, while devices that are monitoring these messages scan the pre-defined frequencies of broadcast [77]. The presence or absence of network coverage changes the D2D discovery mechanisms: in a network-controlled scenario, D2D depends on the core network. Therefore, the network can use specific control signals for the discovery process, coordinating time and frequency of the process without collisions. This approach obviously provides several advantages in all the steps of the D2D connection, from the synchronization to the communication setup [99].

In the out-of-coverage scenario, the discovery is made by the devices themselves through known synchronization or reference signal sequences. These specific packets, also known as beacons, advertise the presence of the device, which makes peer discovery possible independently from the BSs; this is a natural solution for PSNs [100].

The out-of-coverage D2D discovery process is characterized by the following features:

- direct discovery instead of discovery supported by the network;
- the possibility of leveraging discovery by underlaying coexisting technologies such as WiFi or Bluetooth;
- being, in general, an asynchronous process.

At the same time, the peculiarities and the main issues of the discovery process in PSNs are:

- typically to be tested in the worst-case scenario, *i.e.* out-of-coverage or decentralized;
- device discovery without network assistance is usually time and energy-consuming;
- the quality of the discovery process is determined by (i) high power efficiency, (ii) discovery range, (iii) spectral efficiency or low use of spectral resources, and (iv) rapidity.

In the literature, there are many studies focused on performance and energy efficiency for out-of-coverage conditions in D2D networks. In the past, several solutions have focused mainly on the optimization of the probing interval, *i.e.* with mechanisms for optimizing the duty cycle between sleeping and waking up phases. Other studies are specifically focused on wireless technologies such as WiFi and Bluetooth, which appear of interest for the possibility of using these underlying technologies as leverage for D2D discovery also in emergency scenarios.

General Discovery Approaches: In [101], an approach is proposed for adaptive wake-up schedule based on power-law distributed contacts; the key point of the proposed solution is that the nodes stay asleep when a contact is unlikely to happen and wake up only when the possibility of a successful contact is sufficiently high, guaranteeing a reduction of energy consumption in opportunistic networks (up to 30% w.r.t. other wake-up techniques).

Discovery for WiFi, Bluetooth: An overview and an experimental evaluation of WiFi Direct is provided in [102]. In [103], an energy efficient device discovery protocol is based on the underlying wireless technology Bluetooth. The protocol adapts the duration and interval of Bluetooth inquiry in dynamic environments, by using history information on discovered peers. The performance has been validated by an experimental prototype. In [104], the WiFi Neighbor Awareness Networking technology, standardized by the WiFi Alliance, is presented and evaluated using packet level simulations; this technology allows devices to continuously discover surrounding services and devices operating in a background energy-efficient way. In [105], the Bluetooth low energy (BLE) discovery mechanism is modeled and evaluated using intensive simulations and characterized through its discovery probability, latency, and energy consumption as a function of the parameter settings.

Discovery Approaches with UAVs: In [106], a scenario in which UAVs enhance public safety services is studied; the proposed ComProSe system is an innovative ProSe-enhanced multimedia communication framework, which makes use of UAVs as relays and provides direct discovery and QoS-aware communications between public safety UEs from different organizations. The paper presents interesting real-life tests concerning the cooperation between UAVs and public safety users.

3.1.2. Beamforming solutions for UAVs

An array of antennas, composed by linear, rectangular or circular series of simple antennas or elements, is used for controlling the array directivity function by adjusting the phases between different antennas. When the phases of signals coming or transmitted by the different elements are adjusted such that they combine coherently on a given direction in the space, the array forms the corresponding beam, directed with the maximum gain. The array and the beamforming are called adaptive when the phases (possibly also the gains) at the different elements are changed dynamically as a response to some feedback from the system, based on the maximization of the signal strength, SINR or the corresponding minimization of the interference. As an example, in the context of PSN and emergency scenarios, the adaptive array mounted on the relaying station, *e.g.* the UAV, should enhance the signals coming from some directions for discovery, communication or localization purposes, rejecting at the same time interference or other signals from other positions in the emergency area; this type of mechanism could maximize the output SINR.

Here we report the main recent works that have considered the application of beamforming to UAVs. Most of the papers are concerned with strategies for optimizing communications with devices on the ground. More recently, research has focused on channel impairments related to UAV mobility and energy efficiency aspects.

In [107], a UAV platform exploits beamforming for mitigating the mutual interference among mobile single-antenna devices on the ground and achieving spatial division multiple access. The work also addresses the control of the UAV using a Kalman filter for tracking the positions of the devices on the ground; according to the predicted positions, the system adjusts UAV's heading in order to optimize a bound on the achievable communication rate between the ground and the UAV. In [108], the UAV is used as a relay between single-antenna devices on the ground and a BS; in this context, the design of beamforming (BF) and UAV path for optimizing the signal-to-noise ratio (SNR) of the dual-hop relay link is presented. Numerical simulations show: (i) that the proposed method approaches the optimal flying path and outage performance; (ii) the impact of the number of antennas at the BS and of the UAV heading angle on system performance. In [109], UAVs are just considered as solutions for providing temporary wireless connectivity after disasters compromising communication infrastructures. Also, the optimal placement of UAVs making use of multi-antenna arrays is studied according to the principle of SNR maximization at ground nodes. The scenario considers the communication between two UAVs and two single users, in order to achieve maximum angular separation and maximum SINR. In [110], the UAV support to cellular networks is extended to mm-waves. Here, the beamforming phase selection is based on beamforming codebooks with a hierarchical structure, in order to enable fast training, tracking and reduce the challenging aspects related to the high frequencies. Among the interesting results of the paper, we can mention: (i) the study on the Doppler effect resulting from UAV movements, which could be potentially catastrophic especially for the high gain directions; (ii) the spatial-division multiple access potential at these frequencies; (iii) the proposition of an adaptive UAV cruising algorithms for contrasting signal blockage; and (iv) the study of the relationship between UAV positioning and user discovery with antenna arrays. In [111], a measurement study has been proposed for characterizing the air-to-ground channel at several frequencies, from 900 MHz and 1800 MHz to 5 GHz. Also, drone-based beamforming systems are investigated in terms of (i) channel reciprocity, (ii) feedback overhead, and (iii) update rate for channel estimation. Over the different bands, it is found that the optimal channel update rate is similar and the phase error depends on mobility, differently from the amplitude one. In [112], the coverage of a UAV-based BS has been optimized under the constraint of the transmitting power; the optimization problem is formulated w.r.t. the UAV altitude and beam angle, providing an interesting tool for relating the array weights patterns to the altitude for the coverage optimization with limited power consumption. Finally, in [113], an adaptive beamforming technique is exploited in a drone surveillance system; the weights adaptive algorithm is conceived for being robust to interference motion and array steering mismatch problems. Numerical results are used to validate the SINR performance improvement.

Table 3
Qualitative classification of localization technologies and approaches.

Method	Accuracy	Energy consumption	Localization method	Literature representation
RSSI	Low	Low	Trilateration	High
ToA/TDoA	High	High	Trilateration	Low
AOA	Low	High	Triangulatoin	Medium
Fingerprinting	High	Medium	Radio map	Low

3.1.3. Localization strategies

This section is devoted to the survey of novel localization solutions for PSN that exploit or may exploit UAVs. Localization is mainly based on measures that can be derived from the signal received by other devices or fixed reference points (usually denoted anchors or beacons), as the received signal strength indicator (RSS or RSSI), time of arrival (ToA), time difference of arrival (TDoA), and angle of arrival (AoA). The vast majority of practical techniques rely on RSSI or hybrid RSS/AoA techniques [114–118] and the reason is mostly due to constraints on hardware weight, which translates to constraints on precision for TDoA and ToA techniques. The most apparent contrast for traditional UE localization when UAVs are involved in their ability to move and quickly cover large distances. This ability allows the development of algorithms that define a flight plan for the drone to achieve the highest localization accuracy [114–116,118]. The main qualities of the most prominent localization strategies as well as their applicability are summarized in Table 3. Localization systems and their applications are becoming increasingly popular also in the context of 5G. With the 5G and the distribution of massive MIMO antennas, new localization schemes, based on the additional contribution of the AoA, are acquiring more interest than in the past [119]. In a terrorist attack scenario, in which UAVs have to cooperate for recovering the positions of the devices on the ground, a hybrid approach making use of all the available information and measures is surely one of the most reasonable approaches. In the sequel, the review of the state of the art follows a classification based on the type of measures used for the localization process.

UAV Based Localization Through RSSI: In [114], the authors present an AoA localization, based on RSSI measures, that is designed to be used on drones. The main strength of the work is the usage of Moxon antennas, cheaper and lighter than other commercial antennas. Their experimental solution is deployed on an SDR component installed on the RTL2832U chipset. The AoA is estimated through RSS measures from a front and a back antenna. Multiple measures are taken and a belief based algorithm refines the position based on current and past measures. A similar approach was used in [115] where multiple antennas are mounted on a drone and the user's bearing, with respect to the drone, is estimated by a weighted RSS algorithm. Yet another approach based on RSS is shown in [116], where the authors show an approach based on a single omni-directional antenna and RSS measures affected by stochastic channel fading and measurement noise. This work offers the joint evaluation of two localization algorithms, extended Kalman filter and recursive Bayesian estimator, alongside two-path planning algorithms, steepest gradient descent, and bio-inspired heuristic planning. One of the challenges of estimating the distance based on RSS measures is that transmitter power needs to be known in order to derive distance from RSS measures, because of this many works assume transmitter power known or constant. The authors of [118] show an approach to RSS localization when this assumption is not met, by employing a neural network-based algorithm to identify the most likely value of the transmitter power from a set of finite values. Then, this value is fed into the algorithm that performs target trilateration and makes the UAVs converge around it.

Localization with Hybrid AoA and RSSI: In [117], the authors study the signal discovery and localization in a huge disaster scenario with the purpose of life detection. The proposed hybrid RSS/AoA algorithm is based on the triangulation from AoA while using RSS information to improve the estimate. The AoA measures are evaluated according to the actual measured RSSIs, giving more importance to measures in which the difference between the maximum and minimum RSSI is higher. The work presents an experimental test bed usable on typical terminals such as UE.

Other Types of UAV Based Localization: The use of UAVs for the particular scenario of a terrorist attack can also be extended to the role of a mobile sensor platform, which can be used, for example, to locate shooters as shown in [120]. In the paper, the authors show a shooter localization algorithm that uses data coming from an array of microphones mounted on a flying UAV. The technique is similar to the AoA approach, where rather than radio waves the estimation is done by using sound waves. While the authors show a successful shooter localization, several constraints of this approach pose some concerns during hostile attacks. The main issues arise from the possible absence of LoS condition that precludes reliable localization and from the noise introduced by the UAV rotors, which is one of the largest impairments affecting the SNR of the measurements.

3.2. MAC Layer

3.2.1. Resource and power allocation schemes in centralized mode

As previously indicated, D2D communication can be operated in two modes: centralized, which is controlled by the BS and decentralized mode, which is not assisted by the BS [121]. Contrary to the traditional cellular network, where cellular users (CU) communicate via BS, D2D provides direct communication between users regardless of the network status. So, D2D communication can reduce the traffic load to the BS and provide better system throughput. However, interference is generated by D2D users. Therefore, appropriate power allocation and efficient resource allocation schemes can play a vital role to reduce the interference level, thereby significantly improving the overall throughput of the system [122]. In Table 4, a summary of classical schemes for centralized D2D communication is presented.

Matching Based Scheme: In [123], a resource allocation technique is proposed to guarantee the QoS of D2D pairs and CUs at the same time, to improve the overall network throughput which improves the spectral efficiency. The authors proposed a three-step scheme. The first step is to determine the D2D pair for each CU by ensuring the QoS by verifying the minimum SINR requirements. The second step determines the power allocation for CU and its D2D pair with the constraints on the minimum SINR requirements. The third, and last, step is the resource allocation for all D2D pairs, which consists of finding the best CU partner by using a maximum weight bipartite matching based scheme. In this scheme, a set of D2D and a set of CU partners are considered as two groups of vertices in the bipartite graph. The performance of D2D communications can be influenced by the cell radius, D2D user locations, the maximum power limitation for the D2D pairs and, the numbers of active CUs and D2D pairs [124].

Mixed Integer Nonlinear Programming: During the downlink (DL) phase, CU could suffer from interference produced by the D2D transmitter. While during the uplink (UL) phase, the BS could face interference by the D2D transmitter when random

Table 4
Summary of classical schemes for centralized D2D communication in cellular network.

Proposed scheme	KPI	Network architecture		Achieved performance	Drawback
		Architecture	UL/DL		
Matching based scheme [123]	QoS, power control, resource allocation, spectral efficiency and energy efficiency	LTE	UL	System throughput is enhanced 60% and access rate 10% compared with random allocation	Computationally complex and expensive
Mixed integer nonlinear programming [125]	Resource allocation	LTE	UL/DL	System throughput is improved up to 7% compared with random D2D allocation	Power control
Proportional fair and heuristic algorithm [126]	Resource allocation and QoS	LTE	DL	System throughput is improved up to 30% compared with random allocation	Power control
Game framework [127]	Power control, energy efficiency and QoS	LTE	UL	System throughput is improved	Computationally complex and expensive
Lagrangian dual decompositioN [128]	QoS, resource allocation, energy efficiency and power control	LTE	UL	System throughput is improved up to 35%	Computationally complex and expensive
Water-filling algorithm [129]	Resource allocation, power control and Spectral efficiency	LTE	UL/DL	Spectral efficiency is enhanced	Computationally expensive

allocation is used for radio resources [130]. In [125], the authors propose a mixed-integer-nonlinear programming (MINLP) scheme for D2D radio resource allocation, where the SINR values of CU and D2D pairs are found separately for UL and DL, and RBs are allocated with respect to SINR values. Numerical simulations show that D2D throughput, cellular throughput, and system throughput are improved with the proposed algorithm compared to random allocation.

Proportional Fair Algorithm: In [126], the authors propose a proportional fair (PF) algorithm for resource allocation to CUs and a greedy heuristic algorithm for resource reuse of D2D users. The PF algorithm follows a greedy rule, wherein the CU with the minimum normalized transmission rate is selected as the best subcarrier each time. Further, the second heuristic algorithm first determines whether the D2D mode is suitable or not, by doing path loss comparison. The resource allocation will be initiated if the SINR values of both CU and the D2D pair meet the minimum requirement of the allowed SINR. The results show that D2D and system throughput will improve with the increase in the number of D2D pairs.

Game Theory Framework: The work [127] proposes a joint scheduling method, power control, and channel allocation for D2D communication using a game theory approach. A technique named Stackelberg game framework is used, where cellular and D2D UE are grouped in a pair with a leader–follower combination. The CU acts as a leader while the follower is the D2D UE who purchases resources of the channel from the leader. The leader charges some dues from the follower for channel usage. So, the D2D user chooses the optimal power by utilizing the price given by cellular UE. The results imply that the throughput performance for both the D2D and cellular UEs can be improved with proposed method [131].

Lagrangian Dual Decomposition: In [128], the authors propose a two-phases based resource sharing algorithm for D2D communication. The first phase determines the channel allocation for each D2D UE. QoS is considered for both CUs and D2D UEs by defining a combined channel gain factor to assign channels to each D2D UE. In the second phase, the Lagrangian function is used to determine the optimal power for D2D UEs.

Water-Filling Algorithm: Water-filling algorithm is used to allocate the power for the subcarriers assigned to each separate D2D pair. The rule of water-filling method is that the transmit power will be distributed among all assigned devices [132]. The power allocation is proportional to the CSI of the D2D link of the respective sub-carrier.

3.2.2. Machine learning techniques for D2D communication

In case of absence of initial information, the problem of resource and power allocation for D2D communication in cellular networks is solved using Machine learning (ML) methods as proposed in [133–135] and presented in Table 5.

Cooperative Reinforcement Learning Algorithm: In [133], the authors present a cooperative reinforcement learning (RL) algorithm for resource allocation in D2D communication to improve the system throughput, also called state action reward state action (SARSA). The cooperation is achieved by sharing the value function between UEs and a neighboring factor. A set of actions is considered based on the transmission power level of a particular resource block. The reward function is defined by SINR and channel gains. The accuracy of the learning algorithm is increased by defining a set of states with a suitable number of system-defined variables. Simulation results show that the system throughput is improved with the proposed learning method as compared to the distributed reinforcement learning method. The shared learning policies between devices help to converge faster. D2D throughput is enhanced around 7% comparing with distributed reinforcement learning. A trade-off can be seen in D2D and CU throughput by changing the transmit power; higher transmit power will provide higher D2D throughput. It is also shown that D2D and the system throughput will improve by increasing the number of D2D UEs but cellular throughput decreases.

Distributed Reinforcement Learning: The work in [134] suggests two RL methods, team-Q and distributed-Q learning, to improve power control in a D2D under-laying cellular network. In the team-Q learning algorithm where all agents keep the same Q-value table. The complexity level of this approach increases exponentially according to the increasing number of D2D UEs. A distributed Q-learning is introduced to solve this problem. Distributed Q-learning breaks one big Q-value table in team-Q into several small tables. Now each agent has its own local Q-value table. Actions are sampled constantly during the learning process. So the Q-values in a table will only be updated once the next Q-value is greater than the existing Q-value. The agents, states, and actions also used for distributed-Q learning. Simulation results

Table 5
Summary of ML schemes for centralized D2D communication in cellular network.

Proposed scheme	KPI	Network architecture		Achieved performance	Drawback
		Architecture	UL/DL		
Cooperative reinforcement learning algorithm [133]	Power control, resource allocation, energy efficiency and spectral efficiency	LTE	UL	D2D throughput is enhanced around 6.2% as compared to the distributed reinforcement learning	Computationally complex and expensive
Team-Q learning and distributed Q learning [134,135]	Power control, QoS and spectral efficiency	LTE	UL/DL	System throughput is improved and convergence speed is enhanced	Computationally expensive
Proportional fair and heuristic algorithm [136]	Power control and energy efficiency	LTE	DL	Same throughout as compared to conventional method	Computationally complex and expensive

show that distributed-Q learning converges the Q-value faster than team-Q learning algorithm. It can also be seen that D2D throughout is more improved with distributed-Q learning than team-Q learning, with the increasing number of D2D UEs.

Deep Learning: The authors of [136] suggested a distributed transmit power allocation scheme using deep learning for every D2D UE. Each D2D transmitter can decide its transmit power considering both the D2D throughput and interference to the cellular system. D2D UE uses only its location to determine the transmit power to maximize the D2D throughput. Each D2D UE learns how to decide the transmit power to achieve the optimal system throughput based on locations considering the interference to BS. Deep learning is applied for the learning process using a cost function to meet the constraints. The cost function can be considered as a linear function to decide the appropriateness of output. The results show that the proposed method is appropriated to cover the edge users. However, it provides almost same throughout as compared to conventional methods by operating completely on distributed manner, and it is also computationally expensive.

3.3. D2D Communication in a decentralized mode

For the first time in cellular network, D2D communication was introduced in LTE Release 12. D2D communication allows direct communication between two UEs. The term sidelink was introduced by the 3GPP for ProSe. In ProSe three different LTE D2D functionalities are defined, i.e., direct discovery, direct communication, and synchronization. Despite of establishing a communication link in ProSe, the direct discovery functionality permits the UEs to advertise and detect the services or devices. Without routing the data to base station, the communication functionality permits two UEs to communicate by establishing a direct link between them. However, the synchronization functionality gives the required approaches to UEs to settle on mutual system information and is able to decode LTE sidelink transmission [77].

According to 3GPP, three scenarios are offered to operate D2D functionalities regardless of the network position of the UEs, i.e. in-coverage, partial coverage and out-of-coverage. In in-coverage scenario, the D2D communication is BS assisted and can also use pre-configured parameters. In the out-of-coverage scenario, UEs use preconfigured parameters for D2D communication. Finally, the partial coverage scenario is a combination of other two scenarios, where UEs inside the coverage area share system information with those out-of-coverage [137]. In Table 6, a summary of D2D communication in decentralized mode is presented.

3.3.1. Direct discovery

Different service discovery strategies are described in [138]. In service discovery process, UEs are allowed to advertise and monitor the services. Initial devices are required to register to the ProSe function. After the registration, the application layer permits the UEs to start or monitor the ProSe. A discovery signal is transmitted in discovery resources by advertising UEs. There are two types of service discovery approaches, uncoordinated service discovery and coordinated service discovery. An uncoordinated service discovery approach is not assisted by the BS for monitoring the services. The monitor UE starts RF discovery by blind decoding on all RF discovery resources. This approach requires significant undesirable processing and power consumption. In a coordinated service discovery approach, a monitoring UE is assisted by ProSe function indicating either if a service is offered or not in the specific area. For the advertised service, the network gives the information about the RF discovery resources to monitor the respective service. This approach is efficient but can only be used for the in-coverage scenario.

An enhanced algorithm is proposed in [139] to improve the discovery performance by detecting the presence and removal of UEs by using dynamic configuration instead of static configuration. In a static configuration, each UE will keep the same record of other discovered UEs at the time they were discovered. Furthermore, all the UEs use the initial transmission probability, and it will be not updated according to the current situation during the whole discovery process. The proposed algorithm uses a dynamic configuration where each UE processes the received announcements to check different transmission probabilities and computes its own transmission probability, after the addition or removal of UEs in the discovery group. The approach is known as dynamic configuration due to the continuous upgrading of transmission probabilities. Presented results show that the proposed algorithm can improve the accuracy and required time for the discovery up to 15%.

In [140], D2D discovery mechanisms for 3GPP are investigated, in particular, w.r.t. energy consumption; in addition it is proposed a D2D discovery mechanism based on the concept of proximity area, i.e., a dynamic region wherein UEs activate their D2D capabilities, enabling UEs to perform D2D discovery only when there is a high probability to find other UEs for the same service.

Furthermore, the authors in [141] discuss some key requirements and solutions, including those regarding discovery, for enabling D2D communications in LTE in order to meet public protection, disaster relief, national security, and public safety services-related requirements. The contribution of the paper is based on a clustering approach integrating cellular and ad hoc operation modes depending on the availability of infrastructure nodes.

Table 6
Summary of D2D communication in decentralized mode.

Proposed scheme	KPI	D2D scenario	Achieved performance	Drawback
Uncoordinated service discovery [138]	Direct discovery	Out-of-coverage Partial coverage	Able to discovered the services	Undesired processing Power consumption
Enhanced discovery algorithm [139]	Direct discovery	Out-of-coverage Partial coverage	Detected the withdrawal of the UEs. Accuracy of the discovery, and the time required for discovery is improved up to 15%	It is not autonomous to tune the parameters depending on the group size
PSCCH resource pool arrangement [142]	Direct communication Synchronization	Out-of-coverage	Same throughput as compared to conventional method	Throughput could be Reduced
PSSCH resource pool arrangemen [143]	Direct communication	Out-of-coverage	Increased the transmission probability up to 11%	Throughput could be Reduced
Frequency hopping resource scheduling [144]	Direct communication Synchronization	Out-of-coverage Partial coverage	Improved the reliability up to 20%	Performance could be decreased by increasing the number of UEs
Enhanced HARQ process [145]	Direct communication	Out-of-coverage	Improved the reliability and latency up to 9%	Able to increase the Interference

3.3.2. Direct communication

LTE sidelink communication has two physical channels [139]. The physical sidelink shared channel (PSSCH), which carries the transmission data of UE and the physical sidelink control channel (PSCCH), which carries the sidelink control information (SCI) message to detect and decode the PSSCH of a receiving UE. A UE uses the PSSCH to send data to other UEs. First, a UE should advertise the transmission using the PSCCH channel to send a SCI message that informs the remaining UEs about the transmission occupying by the PSSCH resources [146].

- **PSCCH:** All control messages are sent twice in PSCCH in the same period with two different PRBs. The out-of-coverage UEs randomly choose PRB pairs from the PSCCH resource pool defined by the following pair of parameters: the number of subframes from the time domain, and that of PRBs from the frequency domain [144]. As two PRBs are used for each transmission, the number of accessible resources in the pool can be found as: number of subframes * [number of PRBs /2]. If the same PSCCH resource index is selected by two or more UEs, then their SCI messages will interfere with each other. If the SINR at the receiver UE is high enough, then it could be possible to decode one of the interfering messages. The message could also be lost because of the half-duplex nature of UE transmissions. SCI message could be missed by a UE from another UE if it utilizes its own SCI in the same pair of subframes. So, SCIs can be missed because of collisions or the half-duplex effect; UEs that lose the advertisements could not get the real sent data during the following occurrence of the PSSCH. However, the problem could be overcome if the PSCCH resource pool is appropriately dimensioned. In [142], the authors propose a scheme for out-of-coverage scenarios where the PSCCH resources can be selected by UEs autonomously. They did the distribution of UEs in the D2D category that could get a transmitted control message as a function of the PSCCH and the number of UEs in the group. This distribution is used to make performance metrics as the maximum number of UEs that could be supported above a preferred threshold for a given resource pool arrangement. The results show that arrangement of the resource pools has a vital impact on the performance. PSCCH performance could be enhanced by increasing the number of subframes. The transmission period is a ratio of the PSCCH to the PSSCH, so by decreasing the duration of the PSSCH will increase the length of PSCCH that will reduce the throughput.
- **PSSCH:** PRBs of PSSCH are periodically repeated after the PSCCH in the time domain. In PSSCH, the band of PRBs is distributed into Nsb sub-bands in the frequency domain, whereas the set of subframes is divided into multiple time resource patterns (TRPs) on the time domain and each TRPs has NTRP subframes. OOC UEs randomly select the resources in PSSCH, so there could be interference between them. The collision impact could be resolved by the hybrid automatic repeat request (HARQ) process. UEs do not give feedback for each HARQ transmission over the sidelink even not for the successful transmission. A transmitting UE over the PSSCH sends four redundant versions (RVs) of data; each RV has the information and error correction bits [144]. However, the HARQ mechanism will increase the time response and also decrease throughput. It is observed in [143] that increasing the number of sub-bands in the PSSCH enhances the probability of decoding the transmitted message of a UE up to 7%, but this decreases the throughput. It is also seen that the value of kTRP (number of subframes for each TRP utilized by UEs to send data) has a crucial influence on performance. The probability of decoding the message of a receiving UE increases with the lower values of kTRP, but also the throughput is reduced.

The D2D frequency hopping resource scheduling on PSSCH is extended over the LTE Uplink as described in [144]. Frequency hopping is divided into two types. The first type is constant frequency hopping and the second type is pseudo-random frequency hopping. Constant frequency hopping determines the starting resource block for the transmission occurring in odd or even subframe indexes using two predefined formulas from the standard. Pseudo-random frequency hopping for the resource schedule assignment is performed with a predefined pattern calculated by a pseudo-random generated binary sequence, a set of equations defined by 3GPP standard in [147]. It is shown in [144] that frequency hopping improves the LTE D2D communications by about 20% with a single link, while the results obtained from sidelink group communication reveal a limited performance enhancement when enabling the frequency hopping over the standard no-hopping sidelink schedule assignment. This is due to lack of resource scheduling coordination in out-of-coverage scenario and the interference between UEs. Overall constant hopping slightly outperforms pseudo-random hopping.

In [145], the authors analyzed the effect of various configuration settings of unsupervised D2D communication on system performance. The impact on different parameters, such as reliability and latency, is observed using a simulation approach by varying the PSCCH to PSSCH ratio. As HARQ process transmits the same data four times even packets are transmitted successfully because there is no feedback system. Thus, the re-transmission process is improved by adding the transmission probability to the HARQ process. Every re-transmission X is achieved with a probability P(X). It is shown that the reliability is increased with increasing HARQ probability and it is maximum for 100% HARQ probability (conventional HARQ process). But it can also be seen that the reliability is improved with more number of nodes even with lower HARQ probability. It is also analyzed that latency is reduced by decreasing the HARQ probability which is desirable for he highly loaded network. While reliability decreases with smaller PSCCH to PSSCH ratio because smaller PSCCH periods enhance communication overhead but increase the interference between the UEs.

3.3.3. Synchronization

Synchronization helps to establish effective sidelink communication and discovery. UEs are required to coordinate in frequency and time domain, and they must settle on the same system information utilized in the communication procedures such as subframe indication, bandwidth, etc. Therefore, the same synchronization reference (SyncRef) must be followed by two UEs. The BS is responsible for providing the SyncRef for in-coverage UEs. While for out-of-coverage UEs, predefined parameters are utilized for the synchronization process between UEs to settle down on shared SyncRef. A transmitting UE in the Sidelink communication becomes a SyncRef in an out-of-coverage scenario. After becoming a SyncRef, it sends sidelink synchronization signals (SLSS) periodically for sharing its synchronization info. SLSS use one time domain subframe and the six central RBs from the frequency domain. The periodic length of SLSS is 40ms [99].

An SLSS signal is further categorized into four elements as the primary sidelink synchronization signal (PSSS), the secondary sidelink synchronization signal (SSSS), the demodulation reference signals (DMRS), and the physical sidelink broadcast channel (PSBCH). The PSSS and SSSS are operated for frequency and time reference; together they identify the SyncRef by encoding the SLSS identifier (SLSSID). SLSSID has two subsets: the first is dedicated to the identification of the SyncRefs for in-coverage situations and the second is reserved for the out-of-coverage scenario. The PSBCH has the master information block-SL (MIB-SL), which carries the systematic information required for the arrangement of the synchronizing UE. The DMRSs have the information of the receiving UE for channel approximation, demodulation of the PSBCH, and measurement of sidelink reference signal received power (S-RSRP). The S-RSRP has the strength information of the SyncRef signal [99].

3.4. Network layer

Historically, at the network level routing was realized by conventional technologies such as mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). Emergency MANETs (eMANETs) are deployed in emergency cases to provide communication for emergency workers with intelligent devices such as smartphones and personal digital assistants (PDAs) [148]. Recently, integration of UAVs in D2D/MANETs for efficient routing named as UAV-NETs is proposed [149]. The authors in [150] provided a comprehensive survey of multi-hop routing protocols for different classes of MANETs and the integration of networking technologies for disaster response scenarios. Similarly, [151] highlighted the merits and demerits of MANETs and delay tolerant networks (DTNs) and further presented the case of integrated MANET and DTN for improving the performance in dynamic environments. This survey also highlights the lack of realistic simulations models for disaster environments. Kawamoto et al. present the case of hybrid MANET and DTN implementation [152]. However, a single technology is not able to provide a complete solution. Therefore, a fusion of MANET based technologies such as MANETs, vehicular ad hoc networks (VANETs), flying ad hoc networks (FANETs), WSNs, and DTNs are the suitable choices. The authors in [153] reiterate the fact that most of the research work is simulation-based. However, they have tried to present details of the real experimental work in this domain and concluded that it is feasible provided the interoperability issues are resolved. In [154], a survey of routing algorithms and mobility models proposed for MANETs, DTNs, VANETs, WSNs for communication under disaster scenarios is presented. It also highlighted the challenges, gaps between applications, protocols evaluations and mobility models. In another effort, dynamic routing in FANETs is discussed in detail for the case of self-organizing wireless networks [155]. The success of any networking technology is also dependent on the underlying access technology. These days, user devices are equipped with multiple access and network technologies that allow these to communicate on multiple interfaces. This makes it more feasible to enable and facilitate D2D communication. D2D communication allows (I) Single hop communication, (II) Two hop communication, and (III) Multi-hop communication. Single hop communication is the basic mode of communication and D2D standards support for two and multi-hop communications through relays. There are multiple uses of relays in multi-hop communications such as range extension, connectivity with infrastructure, and other devices. Multi-hop D2D communication is an important feature and requires coordination between multiple nodes. The coordination between nodes can be achieved through routing protocols and gives rise to a new routing paradigm called multi-hop D2D routing.

3.4.1. Multi-hop D2D routing for PSN

The authors of [156] gave a very comprehensive survey on multi-hop D2D routing. They have presented a taxonomy of the D2D communications systems, classification of routing protocols, application areas, comparative analysis, and future directions. The survey classified multi-hop routing into three main categories (I) multi-hop device to infrastructure (D2I) and infrastructure to device (I2D) communication, (II) Multi-hop D2D communication and (III) Ad hoc routing for D2D networks. Multi-hop D2D devices operate in two modes. In the first one, a BS, or another central entity, controls the routing decision, while, in the second one devices operate in a distributed manner. The broad categories identified by the authors for base station dependent multi-hop D2D routing protocols are incentive-based, security-based, content-based, location-based, and topology-based. Similarly, the broad categories for D2D ad hoc routing are incentive-based, topology-based, QoS-based, security-based, device-aware, and multipath coding based. In addition to the above classification, routing protocols can be further classified as reactive, proactive, hybrid, and adaptive. Based on more recent trends in multi-hop D2D routing a few new classifications are possible: mm-wave D2D multi-hop routing (for spectrum efficiency), cluster based multi-hop routing (for load balancing and energy efficiency) and social aware multi-hop routing (for reducing the overhead and improve energy efficiency). The important factors affecting multihop D2D routing are node mobility, dynamic network, and network fragmentation. Multi-hop D2D routing can further benefit from advanced techniques such as software-defined networking (SDN) and network function virtualization (NFV).

3.4.2. Software-defined networking for PSN

The Table 7, presents a summary of main SDN architectures and frameworks. In SDN, the control plane is decoupled from the data plane. The control plane is responsible for monitoring

Table 7
Summary of SDN Frameworks.

SDN architecture framework	Features	Achievement	SDN controller
D2D-SDN [157]	Data packets sent in more flexible and efficient way	Hierarchical control plane for scalability and reduce communication overhead	Centralized global controller and multiple local controllers
VARP [158]	Better security, lower routing overheads, and higher scalability	Centralized and distributed	Main SDN controller to manage sub SDN controllers
HSAW [159]	Splitting of network control and data forwarding by two separate frequency bands	Demonstrates the advantage of hybrid architecture, offers better scalbility and reliability	Centralized SDN controller
EHSD [160]	QoS parameters, handover mechanism, security and coverage area	Results in better QoS compared to legacy LTE, improved security	SDN controller, L7 switch, open flow controller and security is provided in user side
SEANET [161]	Energy harvesting, separate energy plane	Improves data traffic by reducing packet loss, energy saving by optimizing energy utilization	SD data and energy controller
Softnet [162]	Coverage and low decentralized mobility management	Low signaling overhead compared to LTE NA	Network controller consisting of SDN controller and Virtual Network Function (VNF) orchestrator
CROWD [163]	MAC layer reconfiguration, dynamic backhaul reconfiguration	Reduced signaling overhead	Regional controller and Local controller
SoftPSN [164]	Resource slicing, reliability and low latency	Priority based resource slicing to accommodate first responders	Virtual resource controller

flows and managing the resources of the network. The control plane has a broad view of the network topology and can be used for the dynamic allocation of resources [165]. Initially, SDNs were widely used for wired networks. However, recently, an increasing interest in deployment of SDNs for distributed and wireless networks has been observed [166,167]. This is mainly due to the flexibility of deployment offered by SDNs. Most of the current SDN based research is mainly limited to proposals, architectures, and frameworks. A survey of recent SDN related efforts in wireless networks such as cellular, sensor, mesh, and home networks is presented in [167]. It highlights the advantages of using SDNs and discusses further opportunities to improve the performance of wireless networks. The report [168] proposes the integration of modern technologies such as LTE with networking technologies like SDN and NFV for the PSNs. As per the studies conducted on earthquakes, the features of these networking technologies are suitable because of rapid deployment, reliability, security and resilience. It further summarizes the features of the frameworks published in the literature.

SDNs play an important role in providing central management to the D2D clouds. They make use of the global information such as link quality, battery life, routing, etc. of all the devices available. They also control device registration, authentication and provide information about reliable connections. This hierarchical architecture is well suited for public safety applications where infrastructure is partially or totally damaged [68]. A wireless network architecture that exploits multi-hop D2D controlled through SDN controller to provide effective and efficient communication between devices is presented in [169]. Usman et al. [170] proposed a hierarchical architecture composed of several domain controllers being monitored by a central controller. The central controller dynamically allocates resources and thus reduces the energy consumption and signaling.

D2D-SDN is a hierarchical SDN based architecture [157]. It uses two tier centralized controller to derive the network topology with the help of connectivity and conflict graphs. MAC performance of the architecture against time division multiple access (TDMA) and carrier sense multiple access (CSMA) is also demonstrated through a prototype. Virtual ad hoc routing protocol (VARP) [158] framework provides multi-hop D2D routing as an extended service to the cellular networks through routing virtualization and SDN. VARP has the main SDN controller and sub-controllers for each cell to allow scalability, independence and intelligent decision forwarding. Each UE can use both LTE and Wifi bands and acts as an end-user of the main network and a forwarding node for the controller. VARP-based source (VARP-S) performs topology discovery, route discovery and route maintenance using modified control packets. For performance comparison, a modified version of Hybrid SDN Architecture for WDNs (HSAW) [159] proposed earlier is used. This protocol has shown the advantage of using a hybrid architecture over centralized and distributed architectures. An architecture based on the integration of SDN and short-range UEs to achieve reliability and low latency is presented in [164]. This creates a virtual network of available resources and applies a resource slicing algorithm. There is a provision to use priority-based resource slicing for the cases when the traffic load is too high. An architecture using the SDN controller nearby base stations to extend coverage to dead nodes is proposed in [172]. This is possible as the SDN controller is at the core and can better monitor network issues. This also proposes a flow based routing using relays to extend coverage in the dead spots. The UEs acts as relay nodes, therefore, it is important to take into account their limited energy and computational resources. Software-defined energy harvesting IoT (SEANET) is a proposed architecture that takes into account energy issues of the network [161]. In addition to data and control plane, it introduces an energy plane for efficient energy utilization. This uses a central controller which also considers energy situation of the nodes. CROWD [163] presents a flexible architecture for dense networks that facilitates reconfiguration of wireless devices and links. This uses two-tier hierarchical SDN controller named local controller (for fast and short time decisions) and regional controller (for slower and long time decisions).

The authors in [173] proposed an SDN based routing protocol for wireless multi-hop networks. The centralized controller has a broad view of the whole network and can make better routing decisions compared to AODV and OLSR when realized in simulations. The OpenFlow controller is located outside the core wireless network and connected to UEs via OpenFlow switch component. A low-overhead D2D routing (LODR) is proposed and compared with other protocols in terms of convergence time and overhead. In [171] the authors have presented a centralized

Table 8
Summary of SDN based D2D Multi-hop Routing Protocols.

Proposed scheme	KPI	D2D scenario	SDN controller	Achieved performance	Drawback
SD-MANET [171]	Overhead, throughput, delay, packet delivery ratio	Ad Hoc	SDN controller on one of the nodes, local controllers on other nodes	Low routing and communication overhead, low average end to end delay, proactive routing	Not suitable for large networks
VARP-S [158]	Overhead,energy consumption	Multi-hop D2D	Main SDN controller responsible for sub controllers in BS in each cell	Source based scalable routing	Optimization of power control, traffic classification strategy, metric measurements
HSAW routing [158]	Overhead,energy consumption	Hybrid(multi-hop D2D and cellular)	Sub controller need to exchange information	N/A	Higher overhead due to sub controller information exchange
LODR [169]	Convergence time, Overhead	5G, data plane multi-hop D2D	Central OpenFlow controller supported by OpenFlow switch function at UEs	Low routing overhead, hybrid reactive and proactive approach	Single central controller
FINDER routing [172]	Overhead ratio, delivery probability, average residual energy	D2D coverage extension	SDN controller at core network	Reduced energy consumption in routing and increased network lifetime, hybrid ant colony optimization	Single SDN controller
SDN routing [173]	Hop count, residual energy	Ad hoc	Central controller	Better performance in terms of hop count and end to end delay	Single controller is not suitable for high node density

SDN based proactive routing protocol SD-MANET for MANETs. The SDN controller learns the network topology without location services and the performance is much better compared to OLSR for a network of 50 nodes. Clustering is a suitable option for large networks.

Software-defined decentralized mobile network (SoftNet) is an architecture that proposes a natural alliance of SDN and 5G. SofNet shows better performance compared to legacy LTE. 5G networks allow the use of different devices and protocols, therefore, mobility of these devices in different segments of the network is unavoidable. SoftNet mainly suffers from coverage and device handover issues. Exemplary handover scheme during (EHSD) D2D communication based on decentralization of SDN is a framework that combines D2D communication and 5G vertical handover. Handovers can introduce delays and security issues. EHSD uses OpenFlow controller to reduce delay, L7 switch to support load balancing and has a provision for security. The cost of enabling handover is extra signaling overhead. A summary of SDN based routing protocols is presented in Table 8. This section has provided a detailed description of the communication technologies supporting D2D communication. In the next section, we introduce various channels models in the context of D2D communication including UAVs.

3.5. Jamming in mobile networks

With the term jamming, it is denoted any transmission activity that is intended to have explicitly a negative impact on the communication between one or more legitimate transmitters and one or more legitimate receivers. It is also clear that the wireless propagation environment is inherently more vulnerable to malicious attacks, as intentional or unintentional jamming signals or also passive eaves-dropping for data interception. In the reference scenario of this survey, the systems involved in the scenario are (i) the base stations still active in the network, (ii) the terminals on the ground and (iii) the UAVs acting as temporary base stations or relays towards and from the network as described in our reference scenario; the technology is again LTE and Sidelink, with a particular emphasis on PSNs.

In the context of terrorist attacks, jamming techniques can be part of the terrorists' strategy and/or of the public authorities in order to disturb the terrorists' communications and/or take control or limit the access to the network infrastructure. From these two perspectives, we can state that jamming is one of the technical challenges to be faced in the context of PSNs in presence of terrorist activity.

1. Terrorist strategy:
    - causing the network failure for preventing persons involved in the area from calling and communicating in order to increase the advantage in terms of time and effectiveness w.r.t. public authorities;
    - decreasing the communication capability of the public authorities and first responders;
    - preventing the use of machines, including UAVs, controlled by remote devices.
2. Public authorities strategy:
    - decreasing or nullifying the communication capability of the terrorists in order to decrease their effectiveness;
    - preventing the use of controlled devices, including UAVs, and possibly containing explosives or dangerous items.

Jamming can operate thanks to techniques applied to different physical and transport channels of the attacked network; for a general introduction to this area, the reader can refer to [174, 175] for an introduction and classification of jamming and anti-jamming techniques in wireless networks. Concerning the terminology useful for the sequel of this section, we can distinguish among (i) *elementary jammers*, which are blind interfering signals transmitted without considering the nature of the network and its possible defenses, and (ii) *advanced jammers*, capable of more sophisticated strategies; elementary jammers can be further classified as *proactive*, operating independently from the network activity, or *reactive*, which transmit only after detecting a radio communication on the channels to be attacked. On the other hand, advanced jammers are typically capable of adapting to the behavior of the attacked network, with enhanced functions designed according to specific protocols and system specifications and possibly more sophisticated capabilities of intercepting the control channels of the network in order to increase the probability of causing a service outage.

In terms of general articles, moving closer to the LTE interface, we mention the tutorial in [176], which analyzes the physical layer resilience of orthogonal frequency division multiplexing (OFDM) communications, considering elementary noise-like forms of jamming, energy-efficient jamming attacks, and possible countermeasures. Then, in the context of the evolution towards the fifth generation, in [177] it is possible to find a methodology for classifying the attacks to security in mobile phone networks with its application to the digital network generations; in particular, the analysis is exploited for proposing defenses and suggestions for the 5G specifications, with the final aim of increasing the protection of users' privacy and network resistance even in multi-operator scenarios. In [178], after an overview of the security vulnerabilities and threats in wireless systems as Bluetooth, WiFi, WiMAX, and LTE, it is presented the state of the art of physical-layer security, which is a set of techniques for protecting wireless communications at the physical layer: several techniques are reviewed and compared w.r.t. the presence of different jamming attacks and it is also discussed the integration of physical-layer security into the current authentication and cryptography mechanisms. Finally, in the same context of physical layer security, in [179] it is observed that the cooperation among the legitimate devices in a network can significantly enhance the security w.r.t. an uncoordinated scenario; so the paper provides a survey of works on cooperative relaying and jamming techniques for securing wireless transmissions against eavesdropping nodes, which attempt to intercept the transmissions. Then, the challenges of cooperative security are discussed, including their application to device-to-device communication.

In the sequel, we divide the review of the recent literature (mainly since 2016) into three parts, (i) jamming techniques against LTE and PSN, (ii) techniques for contrasting jamming in LTE and PSN and (iii) jamming techniques against UAVs operations. These topics have been knowing a growing interest also due to the development of the 5th generation mobile network.

3.5.1. Jamming techniques in LTE and PS networks

The studies in this field can be divided primarily into contributions on the analysis of LTE vulnerability to jamming signals and the proposal of anti-jamming techniques. In this section, we are interested in the former group, with an emphasis on the contributions of PSNs. In general, LTE appears vulnerable both in uplink and downlink, especially in the synchronization and reference signals.

Vulnerability of LTE Physical Layer: in [180], it is investigated the vulnerability of all the physical layer channels to RF jamming, spoofing and sniffing, with an assessment of different threats; LTE appears highly vulnerable to jamming and, in particular, the weakest links are identified as the PSS (primary synchronization signal), PUCCH (physical uplink control channel), PCFICH (physical control format indicator channel), and PBCH (physical broadcast channel). In [181], it is possible to find results from practical laboratory tests, performed for measuring the jamming margins of LTE physical layer w.r.t. several jamming techniques. Then, in [182], the LTE downlink is analyzed w.r.t. each subsystem in order to identify the weakest parts of the system: the experimental results, obtained with an open-source system and a synchronized protocol-aware jammer, show that the synchronization signals (PSS/SSS) are robust while the weakest ones are the cell specific reference signals (CRS), at least under these test conditions. On the other hand, also [183] confirms that the impact of pseudo-CRS signals can be really severe on the performance of channel estimation and consequently on data demodulation. Then, also in, it is provided a set of measurements obtained with a software downlink LTE implementation, showing the high vulnerability of the system, especially for protocol-aware attacks, like those designed for RS (reference signals or pilots) and PCFICH signals. In the uplink (in particular the physical uplink control channel or PUCCH, the physical uplink shared channel or PUSCH and the access channel or PRACH), [184] and [185] provide useful results for understanding the critical points of the system, which appears fragile especially w.r.t. requirements of critical missions and infrastructures. The weakness of the uplink is confirmed also in [186], where the single carrier-frequency domain multiple access, used in the LTE uplink, is tested w.r.t. advanced jamming techniques towards the synchronization and channel estimation processes, so by means of attacks on the cyclic prefix and pilots in the signal slots.

Mission-Critical Communication: in [187], several test cases are defined and performed on the LTE subsystems involved in the mission-critical communications; the experiments confirm that one of the weakest points of the system is constituted by the synchronization signals. It is also discussed a method for detecting the specific radio frequency attack in order to be able to mitigate its impact.

Evolution to the 5th Generation: In [188], it is presented a study on the impact of jamming when the interference is localized on non-pilot blocks, which cause the pilot-aided channel estimates to be inaccurate; in addition, the results also show that this kind of attack can severely compromise low-latency applications, which are crucial in vehicle-to-vehicle (V2V) communications and other ultra-reliable low-latency applications. Then, in [189], it is analyzed the vulnerability of 5G to jamming and spoofing and some mitigation strategies are proposed; the weakest links appear to be the PSS and PBCH channels even if, compared to LTE, 5G NR seems definitively less vulnerable to jamming, also because of the removal of sparse control channels like the PCFICH.

3.5.2. Anti-jamming techniques for LTE and PS networks

In this section, we are reporting the contributions that are more focused on the techniques for contrasting jamming attacks in LTE networks, including PSNs.

Protection of LTE Physical Layer: in [190] it is considered the deployment of LTE in both licensed and unlicensed bands; the paper analyzes the effect of RF spoofing affecting devices during the initial cell selection process, a serious threat for uncoordinated unlicensed bands and licensed bands interfered by intentional jammers, and it proposes some mitigation techniques compatible with LTE networks. In [191], the authors propose some mitigation techniques for addressing the LTE weakness related to the jamming of control channels during the cell selection process. Moving to LTE for PSNs, in [192], it is presented an algorithm for timing synchronization, cell identity detection, and carrier frequency offset estimation that is robust against partial-band interference and/or jamming, thanks to a proposed, appropriate adaptive filtering of the jamming signal from the PSS. Then, in [193], it is observed how LTE networks resilience decreases under wideband multipath conditions; in this scenario, it is proposed an algorithm based on game theory for combating smart jamming attacks.

Jammer-Type Estimation: part of the techniques for mitigating the impact of jamming involves the necessity of detecting the attack and its type. In [194], a mechanism is proposed and validated for helping the network to estimate the type of jammer and computing a repeated-game strategy conditioned on this estimate; interestingly, the mechanism is autonomous since it does not require explicit feedback from the network users.

Physical Layer Security: in [195], in order to respond to the weakness of D2D communications to jamming, data modification and privacy violation, solutions based on the application-layer and physical-layer security are proposed and validated.

3.5.3. Jamming in UAV communications

In the recent literature, there is a wide selection of papers concerning the impact of jamming signals on the control of UAVs and several proposed countermeasures.

Jamming Impact: in [196], there is a study on the impact of jamming signals in the spectrum used for piloting signals, in particular for evaluating the efficiency of commercial LTE signal jammers as a countermeasure against the LTE UAVs. On the contrary, in [197], it is considered a scenario where the link between a legitimate ground user and a UAV is subject to several eavesdroppers UAVs; the proposed model and analysis provides an insight on the secure connection probability w.r.t. several parameters and propagation conditions.

Anti-jamming Techniques: among the countermeasures against jamming and eavesdropping, in [198] it is studied a secure millimeter wave (mmWave) communication assisted by multiple UAV-enabled relays and jammers; one peculiarity of the study is that a cooperative jamming scheme, generated by a part of the UAV relays, is designed to degrade the eavesdropping channels and enhance physical layer security. Then, in [199], the physical layer security mechanisms for the two case studies of a UAV as a flying base station and a UAV as an aerial node are investigated. In [200], it is proposed and studied a power allocation strategy for UAV transmission based on reinforcement-learning, in order to resist smart jamming attacks without knowing their type and the channel model in the dynamic game. The numerical results show that the proposed strategy can suppress the attack motivation of subjective smart attackers and increase the secrecy of the UAV communication. In [201] it is considered a scenario where ground devices can learn how to contrast intelligent jamming attacks coming from UAVs using the application of deep Q-networks; the problem is formulated as a dynamic game, which is analyzed and simulated. In [202], the work is devoted to a novel detection and response scheme, which operates at the UAV and ground station for detecting malicious anomalies in the network. The numerical results show that the proposed scheme has remarkable attack detection probabilities for the most known cyber-attacks for UAV networks, including jamming.

Beamforming: in [203], it is considered the problem of fast-moving jamming, which constitutes a real challenge for UAVs. Therefore, it is developed a robust adaptive beamforming technique capable of enhancing the navigation signal and suppressing the jamming efficiently.

Trajectory Design: an interesting research line has been considering the design of optimal trajectory and other parameters for contrasting efficiently jamming. In [204], it is proposed a maximization function for the average secrecy rate by jointly optimizing the UAV trajectory, transmit power in the presence of an eavesdropper, and avoiding specific no-fly zones. The sub-optimal solution allows an efficient computational implementation despite the general high complexity of this kind of problem. In [205], the scenario is constituted by an UAV under the threat of a malicious jammer; it is proposed a joint power and trajectory optimization method based on a game theory approach. Then, in [206], a tracking algorithm for a legitimate UAV is proposed to track the trajectories of some suspicious UAVs, by using eavesdropped packets, angle-of-arrival and received signal strength. Finally, in [207], the optimization of a UAV flight trajectory for a relay communication system in presence of a jammer is investigated; a performance gain is achieved by optimizing the UAV path for maximizing the signal-to-interference-plus-noise ratio of the link.

GNSS Jamming: also the global navigation satellite systems (GNSS) can be subject to jamming, causing problems to the UAVs flight under control during GPS jamming. In [208], it is analyzed the impact of off-the-shelf GPS jammers to UAVs and a countermeasure is described, implemented and tested in realistic conditions.

4. Channel models proposed for D2D communication

The architecture proposed for the COUNTER TERROR project, depicted in Fig. 4 shows the three different channel models that are required to obtain realistic performance: (i) the channel between two D2D users, given in [74]; (ii) the air-to-ground (A2G) channel between UAV and ground user, defined in [209]; and (iii) the UAV-to-UAV or air-to-air (A2A) channel, studied in [210]. The channel model characterization is done by defining large scale parameters (LSP) and small scale parameters (SSP). While the LSP include path-loss and shadowing effects, the SSPs take into account angular spread, delay spreads, and the Rician factor. To model these parameters, three different channel approaches can be adopted: stochastic, map-based, and hybrid. In the stochastic-based approach, the parameters are characterized by the data obtained using channel measurement campaigns. In the map-based (or deterministic) approach, environments are simulated using a radio propagation or ray-tracing software to obtain the channel parameters. The Hybrid-based approach is a mixture of the two, where LSPs are calculated using the map-based approach and the SSPs using the stochastic ones [211].

There exist surveys pertaining to channel characterizations for A2G, A2A, and D2D. In [212], the results of measurement campaigns are described for narrow and wide-band channel sounders, IEEE 802.11 transceivers and cellular-connected UAVs operating at either unlicensed frequency bands or respective bands according to the considered technology. Further, measurement results were shown for A2G and A2A characterization with LSP and SSP. In this area, reference [213] describes the difference and analysis of A2A and A2G aeronautical and UAV channel fading statistics, where aeronautical channels are clearly characterized by a flight altitude that is much higher than the UAV one, especially when UAV is used as a low altitude aerial platform (LAP). Then, a list of civil aircraft and UAV channel modeling campaigns is provided along with the link budget, channel impulse response metric, antenna diversity, spatial multiplexing and MIMO characteristics over rural, urban, and sea environments. Another relevant survey [214] describes in detail the impact of multipath channel propagation effects, including scattering and Doppler effects, in different types of environments. Furthermore, antenna configurations, channel sounding waveforms, effects of elevation angles are extensively elaborated. These surveys on A2G and A2A channels also provide open challenges in channel modeling for UAV aided wireless networks.

About D2D channel models, in [215], a comprehensive overview of the state-of-the-art D2D channel research is provided for different scenarios with a discussion on the associated parameters.

In the sequel, we present the details of the models elaborated and adopted in the COUNTER TERROR project.

4.1. D2D-to-D2D Channel model

The channel models defined by 3GPP for the link between D2D users were obtained from the stochastic approach and are classified for three different scenarios [74]. **Outdoor-to-Outdoor:** for this scenario the path-loss is modeled as

$$\mathrm{PL}_{tot}(d) = \max\{\mathrm{FSPL}(d), \mathrm{PL}_{B1}(d)\}, \quad (1)$$

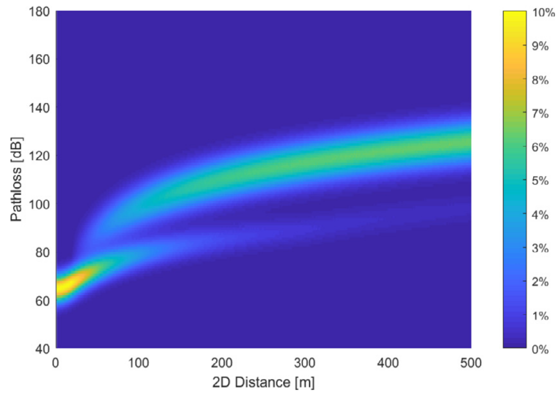

Fig. 10. Path-loss statistical modeling for the case of BS height equal to 25 m and UE height set to 1.5 m, operating frequency 1.9 GHz. A clear separation between LOS and NLOS conditions can be seen.

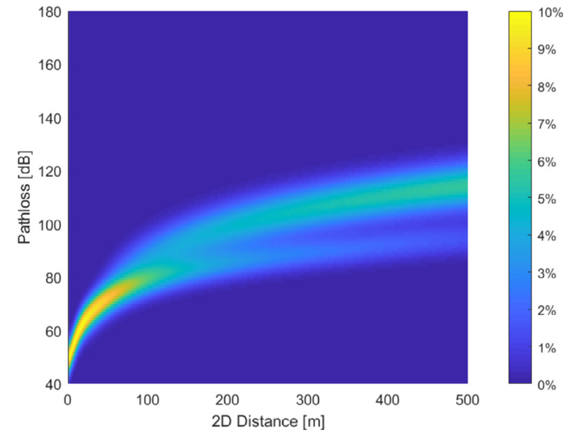

Fig. 11. Path-loss statistical modeling for the case of BS height equal to 25 m and UE height set to 20 m, operating frequency 1.9 GHz.

where $\max(\cdot,\cdot)$ chooses the maximum of its two arguments, d is the distance, in meters, between the UEs establishing D2D communication, which is used to calculate both FSPL(d), the free space path-loss, and $\mathrm{PL}_{B1}(d)$, the path-loss in dB for Winner and channel model [216] in the urban microcell layout. The FSPL is computed as [217]

$$\mathrm{FSPL}(d) = 20\log_{10}(d) + 46.4 + 20\log_{10}\left(\frac{f_c}{5}\right), \tag{2}$$

where f_c is the system frequency in GHz. Similarly, PL_{B1} is modeled as follows:

- $$\mathrm{PL}_{B1}(d) = (44.9 - 6.55\log_{10}(h_{UE}))\log_{10}(d) + 5.83\log_{10}(h_{UE}) + 16.33 + 26.16\log_{10}(f_c), \tag{3}$$
  for f_c in the range $0.45 - 1.5$ GHz;
- $$\mathrm{PL}_{B1}(d) = (44.9 - 6.55\log_{10}(h_{UE}))\log_{10}(d) + 5.83\log_{10}(h_{UE}) + 14.78 + 34.97\log_{10}(f_c), \tag{4}$$
  for f_c in the range $1.5 - 2$ GHz;
- $$\mathrm{PL}_{B1}(d) = (44.9 - 6.55\log_{10}(h_{UE}))\log_{10}(d) + 5.83\log_{10}(h_{UE}) + 18.38 + 23\log_{10}(f_c), \tag{5}$$
  for f_c in the range $2 - 6$ GHz.

In the equations h_{UE} is the height of the UE above the ground, usually taken as 1.5 m.

Indoor-to-Indoor: the path-loss modeled for this scenario is taken from [218],

$$\mathrm{PL}(d_{OI}) = 38.46 + 20\log_{10}(d) + 0.7d_{OI} + 18.3n^{((n+2)/(n+1)-0.46)} + q\,L_{iw}, \tag{6}$$

where d_{OI} is the distance inside the house, n is the number of penetrated floors, q is the number of walls separating apartments between the two UEs and L_{iw} is the penetration loss of the wall, which is 5 dB.

Outdoor-to-Indoor: in this scenario, the model for path-loss is obtained from [218] as

$$\mathrm{PL}(d) = \max\left\{15.3 + 37.6\log_{10} d,\ 38.46 + 20\log_{10}(d) + 0.7\,d_{OI} + 18.3\,n^{((n+2)/(n+1)-0.46)}x + qL_{iw} + L_{ow}\right\}, \tag{7}$$

where L_{ow} is the penetration loss of an outdoor wall, which is 20 dB.

Furthermore, other channel parameters such as LoS probability and coefficient generation for fast fading effects are reported in [219]. The shadowing correlation is assumed to be independent and identically distributed, with a standard deviation of log-normal shadowing as 7 dB for outdoor-to-outdoor and outdoor-to-indoor scenario. For indoor-to-indoor scenario, 3 dB standard deviation is taken for LoS, 4 dB for NLoS and 10 dB if UEs are in different buildings, as reported in [74].

4.2. Air-to-ground channel model

The A2G channel model between UAVs and UEs, where UAVs act as low-altitude aerial platforms, can be inferred from [220, 221]. This channel is different from terrestrial and satellite links. The authors here have used the map-based approach and used the close-in reference path-loss model to characterize the path-loss effect. This model is given by

$$\mathrm{PL}_{LOS}(d) = 20\log_{10}\left(\frac{4\pi d_0}{\lambda}\right) + 10\eta_{LOS}\log_{10}(d) + X_{\sigma,LOS} \tag{8}$$

and

$$\mathrm{PL}_{NLOS}(d) = 20\log_{10}\left(\frac{4\pi d_0}{\lambda}\right) + 10\eta_{NLOS}\log_{10}(d) + X_{\sigma,NLOS}, \tag{9}$$

for LoS and NLoS, respectively. Here, η is the path-loss exponent, d is the distance between UAV and UE in meters, d_0 is the reference distance, taken as 1 m here. X_σ is the log-normal random variable with standard deviation σ that models the large scale shadowing. The average path loss is given by

$$PL(d) = P_{LOS}\cdot PL_{LOS}(d) + (1 - P_{LOS})\cdot PL_{NLOS}(d), \tag{10}$$

where P_{LOS} is the probability of having a LoS condition. The LoS probability is modeled as

$$P(LoS,\theta) = \frac{1}{1 + a\exp(-b[\theta - a])}, \tag{11}$$

where θ is an elevation angle between UAV and UE, a and b are parameters that depend on the type of environment, as indicated in ITU-R regulations.

The channel characterization for these models using a map-based approach is given in [221] at 2.4 GHz for environments defined according to ITU-R environment description. A comprehensive survey is also provided in [214] with several measurements and simulation campaigns to describe LSP, SSP, and MIMO channel characteristics.

A guide for channel modeling can be found also in the 3GPP specifications from 0.5 to 100 GHz in TR38.901 [222]. Of particular interest in our scenario is the modeling of urban macro-areas, defined for BS height of 25 m and variable user height. While this model is of limited applicability to the scenario that includes UAVs, it is nonetheless an important reference. Figures 10 and 11 show the probability distribution of the path-loss values depending on the 2D distance for different cases of UE height assuming that a UAV flies at 25 m of altitude. 3GPP has also provided a technical report for enhancing LTE support for aerial BSs [209], where channel characterizations are provided for uplink and downlink over different cell areas.

4.3. UAV-To-UAV channel model

The LSP and SSP for the UAV-to-UAV channel can be found in [210]. The approach is based on a ray-tracing or map-based approach in order to identify the channel parameters over a certain specific city environment and the sea at 2.4 GHz. A simple path-loss model was addressed, with attenuation and path-loss exponent measurements. Also, delay and Doppler dispersion were characterized.

5. Open challenges and discussions

5.1. Challenges faced by D2D in decentralized mode

D2D communication has attracted both academia and industry. The literature mostly focuses on D2D communication in a centralized mode. In emergency scenarios, the BS would be only partially available or completely damaged; however, only few works in the literature exist on D2D communication in a decentralized mode. Here, we describe some of the main challenges faced by D2D in decentralized mode.

- **Blind Discovery:** After advertising, the monitoring UE starts to discover the associated service/device by blind decoding on all RF resources in decentralized mode, which is undesirable for battery life of cellular phones because higher power consumption and computations are required.
- **Adaptive Resource Scheduling:** Various configurations are possible for sidelink communication by varying the PSCCH to PSSCH ratio and PSCCH period length according to D2D UEs. However, according to the best of our knowledge, there is no adaptive resource scheduling technique which could vary the configuration according to the required situation that would improve the reliability and throughput.
- **HARQ Process:** HARQ process, in sidelink communication, retransmits the data four times. Even if the data is sent successfully in the first attempt, the HARQ process will retransmit the same data although this is not required and desired because there is no technique to get feedback. So, the HARQ process could be improved having feedback to improve the latency and reliability.
- **Energy Consumption vs ProSe Performance:** Battery life of the UE is one of the most significant challenges in critical situations. This highly depends on the designed protocol for direct discovery and communication, for example, if the UE is forced to wake up by the protocol or to advertise the discovery frequently or to retransmit the data repeatedly. The trade-off between the energy consumption of UE and the performance of ProSe should be better analyzed.
- **Adaptive Tuning:** In emergency and critical scenarios it is likely that the BS is either partially available or completely damaged. To handle such situations, 3GPP defines pre-configured parameters [223]. Those are provisioned on ProSe enabled UE by the network operator before the deployment. To have efficient performance, it is required to develop an adaptive tuning at run time according to the specific and possibly dynamic situation.
- **Limited Resources:** There is no literature using experimental evaluation because chip-sets supporting LTE sidelink are not available on the market for the practical implementation; moreover, experimental equipment and test-beds are extremely expensive.

5.2. Challenges in beamforming for UAVs

When a beamforming system is installed on the UAV, the main issue is the relation between the array, with its steering properties, and the position and orientation of the UAV, which is a mobile system. In other words, the array is mounted on an object whose position and orientation in space is not fixed but, changes either as a result of a controlled flight or atmospheric/non-atmospheric disturbance factors like wind or the automatic corrections of the UAV flight control system. This dynamic behavior clearly increases the difficulty of controlling the beamforming, affecting and reducing the final accuracy of the system. Therefore, the main challenges can be summarized as:

- **Beamforming Management in a Dynamic Reference System:** This is the main issue, in which the dynamics of the UAV affects the position and orientation of the array, causing the necessity of managing beam steering, coordinates, and antenna mechanical tilt accordingly. The time constants associated with the UAV dynamics and electronic steering are different, and this could allow the decoupling of the two processes, flight control and beamforming control. However, in a real system, this remains one of the main issues to be addressed.
- **Impact of Flight Turbulence:** In the context of the flight dynamics, some disturbances can condition the stability of the UAV, also when it is supposed to transmit and receive in a fixed position. It is important to study the impact on the communication and localization performance of phenomena like wind, flight turbulence, transitory periods between flight commands and their actuation.
- **Energy Budget in Presence of Beamforming:** The energy budget could be affected by the presence of a beamforming system aboard since the electronic beam steering could be used for changing the flight trajectories and plans. Trade-off studies with given coverage and/or transmission quality requirements and experimental validation are surely another challenging point of research interest.

5.3. Challenges in UAV based localization

Many works have focused on utilizing the versatility of UAV anchors for performing localization. In most of them, the main challenges are represented by the energy and weight constraints the hardware and, while prominent, they are not the only challenges faced in the case of terrorist attacks.

- **Hardware Weight and Aerodynamic Constraints:** Some works in the literature focus on the introduction of massive MIMO into AoA localization [119]. These approaches are suitable for ground based BS that are already equipped with such hardware but they are unpractical for UAV based relays due to clear constraints on the size and weight of the antenna array, which calls for alternatives approaches.

- **Energy Budget Constraints:** Drones are battery-powered and low energy consumption is a fundamental requirement. Therefore, an emerging trend is to select RSS or hybrid RSS/AoA solutions due to their simplicity, reduced cost and energy consumption w.r.t. pure AoA or ToA/TDoA approaches, which would provide better accuracy but at the expense of higher energy costs.
- **Adversarial Activity:** On the one hand, moving the UAVs closer to, and, in LoS condition, the target certainly improves localization accuracy. On the other hand, in the case of terrorist attacks, it gives the terrorists the capability of damaging the drones by shooting them down. To the best of our knowledge, no study has attempted to address this problem, which remains an open issue.

5.4. Challenges in multi-hop routing

Many earlier works have focused on multi-hop D2D routing. However, due to the topology and application dependent nature of the networks, there is a lot of room to develop new routing protocols which can achieve spectral and energy efficiency.

- **DTN Based Routing:** Node mobility is one of the important factors affecting the performance of D2D routing. DTNs use the principal of store carry and forward to allow nodes to carry data and forward when a possible connection is available. For content distribution in disaster and post-disaster scenarios, inspiration from store carry forward can be derived to devise routing protocols for multi-hop D2D routing.
- **Security Based Routing:** As mentioned earlier security becomes a significant concern in multi-hop D2D. The interactions between different devices need some secure routing protocols to avoid malicious activities, which remains an open issue.
- **Energy Harvesting Based Routing:** Network lifetime is dependent on efficient utilization of energy resources. However, in public safety scenarios, energy is very critical in order to keep devices alive for tracking and content distribution. Devices provisioned with energy harvesting capability can further enhance their life. Devices can harvest energy from solar, radio frequency and other sources, which should be considered in routing algorithms.
- **Interference Aware Routing:** Interference is the main reason for performance degradation in multi-hop D2D networks. Interference aware routing strategies can improve performance and save energy.

5.5. Challenges in SDN

As discussed earlier in the paper, SDNs have a great potential to improve multi-hop D2D routing. Some of the open challenges in this domain are listed below:

- **Security:** Security is a major concern and is not catered in the majority of the architectures. It is important to have security provisions in D2D communications. However, central controllers result in delays and some security related tasks could be delegated to local controllers.
- **Wireless Channels:** Wireless channels are dynamic and require continuous monitoring of change in channel conditions. Having centralized controllers can result in delays. Therefore, it is desirable to design hierarchical (main centralized + multiple distributed) or distributed controllers to cater for dynamic nature of the channel and timely update to central controller.
- **Scalable Architectures:** Most of the existing architectures report scalability issues. Considering the increasing number of devices, it is desirable to target architectures which are scalable and support routing protocols which can accommodate a wide variety of devices.

5.6. Challenges in jamming techniques

The analysis of the recent literature has emphasized some clear weaknesses in LTE and potentially in the 5G against jamming attacks. We think that there is still a need for further research in this context.

- **PSNs Resilient to Jamming Attacks:** the context of terrorist attacks requires a specific resilience of the PSN to jamming in order to reach the devices in the area with a secure and reliable connectivity.
- **Jamming in D2D Communications:** this aspect seems not sufficiently addressed by the literature even if, in the scenario considered by this survey, D2D communication is one of the key technologies for overcoming the difficulties in an area without the full infrastructure support.

6. Conclusion

This article has provided a comprehensive survey for pervasive public safety communication technologies in public safety scenarios, especially in terrorist attacks. We have discussed different disaster scenarios, difference between natural and human-made disasters, technical challenges faced by PS services, existing architectures for PSNs along with the enhancements from 3GPP standardization on D2D, and importance to have reliable PSN to deal such disasters. Furthermore, various ongoing research projects have been summarized in the context of pervasive public safety communication. One of the important issues in such scenarios is how to reduce the response time. In order to reduce the time response, we briefly describe an architecture for disseminating the critical information. With this motivation, we have discussed the emerging technologies for PSN that could be critical in the context of emergency management, i.e. UAVs, localization techniques, weak signal detection methods, reliable routing, and jamming and anti-jamming in mobile networks. Finally, the article concluded with open challenges in each layer to highlight the possible future directions of the research in PSC.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This project has received funding from the NATO-SPS funding grant agreement No. G5482 and the European Union's Horizon 2020 research and innovation program under grant agreement No. 668995 and is also partly supported by European Union Regional Development Fund in the framework of the Tallinn University of Technology Development Program 2016–2022, code 2014-2020.4.01.16-0032. This material reflects only the authors view and the EC Research Executive Agency is not responsible for any use that may be made of the information it contains.

References

[1] E. Miller, G. LaFree, L. Dugan, Global terrorism database [online]. (Accessed 27-04-2020), 2020, URL https://www.start.umd.edu/gtd/.

[2] 211 terrorist attacks Carried out in EU member states in 2015, EUROPOL [online]. (Accessed 27-04-2020), 2020, https://www.europol.europa.eu/newsroom/news/211-terrorist-attacks-carried-out-in-eu-member-states-in-2015/new-europol-report-reveals.

[3] Terrorism in the EU: Terror attacks, deaths and arrests, European parliament news [online]. [Accessed 27-04-2020], 2020, URL http://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests.

[4] European union terrorism situation and trend report (TE-SAT 2019), EUROPOL [online]. (Accessed 22-10-2019), 2019, URL https://www.europol.europa.eu/tesat-report.

[5] Belgium's Economic Losses Over Terror Attacks Amount to $1Bln, Sputnik News (2016) [Online]. (Accessed 27-04-2020), 2020, URL https://sputniknews.com/europe/20160726/1043618264/belgium-economic-losses-terror-attacks.html.

[6] Terror attacks cost Paris region 750m in lost tourism, guardian news, 2016, [Online]. (Accessed 27-04-2020) URL https://www.theguardian.com/world/2016/aug/23/terror-attacks-cost-paris-region-750m-in-lost-tourism-officials/says.

[7] L. Alderman, Terrorism scares away the tourists europe was counting on, NY times (2016) [online]. (Accessed 27-04-2020), 2020, URL http://www.nytimes.com/2016/07/30/business/international/europe-economy-gdp-terrorism.html?.

[8] Pakistan Lost over 50,000 civilians in war on terror, the express tribune (2018) [online]. (Accessed 27-04-2020]), 2020, URL https://tribune.com.pk/story/1599831/1-pakistan-lost-50000-civilians-war-terror/.

[9] A. Gul, US War on terror kills nearly 500,000 in Afghanistan, Iraq, Pakistan, Voice of America (VOA) news, 2018, [Online]. (Accessed 22-10-2019) URL https://www.voanews.com/middle-east/us-war-terror-kills-nearly-500000-afghanistan-iraq-pakistan.

[10] A. Paulson, T. Schwengler, A review of public safety communications, from LMR to voice over LTE (VoLT E), in: IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2013, pp. 3513–3517, http://dx.doi.org/10.1109/PIMRC.2013.6666757.

[11] G. Baldini, S. Karanasios, D. Allen, F. Vergari, Survey of wireless communication technologies for public safety, IEEE Commun. Surv. Tutor. 16 (2) (2014) 619–641, http://dx.doi.org/10.1109/SURV.2013.082713.00034.

[12] A. Kumbhar, F. Koohifar, I. Güvenç, B. Mueller, A survey on legacy and emerging technologies for public safety communications, IEEE Commun. Surv. Tutor. 19 (1) (2017) 97–124, http://dx.doi.org/10.1109/COMST.2016.2612223.

[13] W. Yu, H. Xu, J. Nguyen, E. Blasch, A. Hematian, W. Gao, Survey of public safety communications: User-side and network-side solutions and future directions, IEEE Access 6 (2018) 70397–70425, http://dx.doi.org/10.1109/ACCESS.2018.2879760.

[14] A.U. Chaudhry, R.H. Hafez, LMR And LTE for public safety in 700 MHz spectrum, Wirel. Commun. Mob. Comput. (2019) 1–37.

[15] A. Jarwan, A. Sabbah, M. Ibnkahla, O. Issa, LTE-Based public safety networks: A survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1165–1187.

[16] K. Gaibulloev, T. Sandler, Hostage taking: Determinants of terrorist logistical and negotiation success, J. Peace Res. 46 (6) (2009) 739–756.

[17] B. Ganor, Israel's policy in extortionist terror attacks (abduction and hostage barricade situations), Perspect. Terror. 11 (4) (2017) 631–645.

[18] K.C.B.K. Balachandran, J.H. Kang, Push-to-talk group Call system using CDMA 1x-EVDO cellular network, 2011, US Patent No. 7, 970, 425.

[19] P. Rawat, M. Haddad, E. Altman, Towards efficient disaster management: 5G and device to device communication, in: 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 2015, pp. 79–87, http://dx.doi.org/10.1109/ICT-DM.2015.7402056.

[20] S. Krishnamoorthy, A. Agrawala, M-urgency: A next generation, context-aware public safety application, in: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, ACM, 2011, pp. 647–652.

[21] M. Conti, F. Delmastro, G. Minutiello, R. Paris, Experimenting opportunistic networks with wifi direct, in: IFIP Wireless Days (WD), 2013, pp. 1–6, http://dx.doi.org/10.1109/WD.2013.6686501.

[22] F. Chiti, R. Fantacci, L. Pierucci, Social-aware relay selection for cooperative multicast device-to-device communications, Future Internet 9 (2017) pp. 92–105, http://dx.doi.org/10.3390/fi9040092.

[23] L. Babun, A.I. Yurekli, I. Güvenç, 2015. Multi-hop and D2D communications for extending coverage in public safety scenarios, in: IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), pp. 912–919.

[24] L. Babun, Extended coverage for public safety and critical communications using multi-hop and D2D communications, in FIU digital, [online]. (Accessed 22-10-2019), FIU digital, 2015, https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=2927&context=etd.

[25] K. Ali, H. Nguyen, Q.-T. Vien, P. Shah, Z. Chu, Disaster management using D2D communication with power transfer and clustering techniques, IEEE Access PP (2018) 1–12, http://dx.doi.org/10.1109/ACCESS.2018.2793532.

[26] X. Lin, J.G. Andrews, A. Ghosh, R. Ratasuk, An overview of 3GPP device-to-device proximity services, IEEE Commun. Mag. 52 (2014) 40–48.

[27] ETSI, Proximity-based services (ProSe), Technical Specification (TS), (123.303) European Telecommunications Standards Institute (ETSI), 2016, https://www.etsi.org/deliver/etsi_ts/123300_123399/123303/13.04.00_60/ts_123303v130400p.pdf, Version 13.4.0 Release 13.

[28] X. Li, D. Guo, H. Yin, G. Wei, Drone-assisted public safety wireless broadband network, in: Wireless Communications and Networking Conference Workshops (WCNCW), IEEE, 2015, pp. 323–328.

[29] J. Chen, D. Gesbert, Local map-assisted positioning for flying wireless relays, 2018, pp. 113–118, arXiv preprint arXiv:1801.03595.

[30] A. Wirtz, R. Below, D. Guha-Sapir, Working paper disaster Category classification and peril terminology for operational purposes, Context (October) (2009) 1–20.

[31] D. Guha-Sapir, R. Below, The quality and accuracy of disaster data: A comparative analyses of three global data sets, 2002, URL https://www.researchgate.net/publication/209804039_The_Quality_and_Accuracy_of_Disaster_Data_A_Comparative_Analyses_of_Three_Global_Data_Sets.

[32] P. Peduzzi, H.D.C. Herold, Mapping disastrous natural hazards using global datasets, Nat. Hazards 35 (2) (2005) 265–289.

[33] D. Guha-Sapir, P. Hoyois, R. Below, A. Vanderveken, Annual Disaster Statistical Review 2015: The Numbers and Trends, Centre for Research on the Epidemiology of Disasters, Tech. Rep., 2016, pp. 1–59, http://dx.doi.org/10.13140/RG.2.2.10378.88001.

[34] I.R.M. Association, Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018, https://books.google.ee/books?id=X3j1tAEACAAJ.

[35] C.-N. Huang, J.J. Liou, Y.-C. Chuang, A method for exploring the interdependencies and importance of critical infrastructures, Knowl.-Based Syst. 55 (2014) 66–74.

[36] C. TaylorTaylor, E. Vanmarcke, Infrastructure Risk Management Processes: Natural, Accidental, and Deliberate hazards, Vol. 1, ASCE Publications, 2006.

[37] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Syst. Mag. 21 (6) (2001) 11–25.

[38] W.-C. Wang, M.-C. Hsieh, C.-H. Huang, et al., Applying Prim's Algorithm to identify isolated areas for natural disaster prevention and protection, Engineering 10 (07) (2018) 417.

[39] D. Eckstein, V. Künzel, L. Schäfer, Global climate risk index 2018, 2017, Germanwatch, Bonn, [Online]. (Accessed 22-10-2019). URL https://germanwatch.org/en/node/14987.

[40] W.W. Botzen, L.M. Bouwer, P. Scussolini, O. Kuik, M. Haasnoot, J. Lawrence, J.C. Aerts, Integrated disaster risk management and adaptation, in: Loss and Damage from Climate Change, Springer, 2019, pp. 287–315.

[41] M.G. Kocher, J. Pahlke, S.T. Trautmann, Tempus fugit: Time pressure in risky decisions, Manage. Sci. 59 (10) (2013) 2380–2391.

[42] C. Short, L. Clarke, F. Carnelli, C. Uttley, B. Smith, Capturing the multiple benefits associated with nature-based solutions: Lessons from a natural flood management project in the Cotswolds, UK, Land Degrad. Develop. 30 (3) (2019) 241–252.

[43] D. Murthy, A.J. Gross, Social media processes in disasters: Implications of emergent technology use, Soc. Sci. Res. 63 (2017) 356–370.

[44] A. Elbanna, D. Bunker, L. Levine, A. Sleigh, Emergency management in the changing world of social media: Framing the research agenda with the stakeholders through engaged scholarship, Int. J. Inf. Manage. 47 (2019) 112–120.

[45] D. Murthy, A. Gross, M. McGarry, Visual social media and big data. interpreting instagram images posted on twitter, Digit. Cult. Soc. 2 (2) (2016) 113–134.

[46] B.W. Robertson, M. Johnson, D. Murthy, W.R. Smith, K.K. Stephens, Using a combination of human insights and 'deep learning'for real-time disaster communication, Progress Disaster Sci. 2 (2019) 100–130.

[47] M. Imran, C. Castillo, J. Lucas, P. Meier, S. Vieweg, AIDR: Artificial intelligence for disaster response, in: Proceedings of the 23rd International Conference on World Wide Web, ACM, 2014, pp. 159–162.

[48] Z. Ashktorab, C. Brown, M. Nandi, A. Culotta, Tweedr: Mining twitter to inform disaster response., in: ISCRAM, 2014, pp. 269–272.

[49] A. O'Neal, B. Rodgers, J. Segler, D. Murthy, N. Lakuduva, M. Johnson, K. Stephens, Training an emergency-response image classifier on signal data, in: 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, 2018, pp. 751–756.

[50] X.-q. Chen, J.-g. Chen, P. Cui, Y. You, K.-h. Hu, Z.-j. Yang, W.-f. Zhang, X.-p. Li, Y. Wu, Assessment of prospective hazards resulting from the 2017 earthquake at the World Heritage Site Jiuzhaigou Valley, Sichuan, China, J. Mt. Sci. 15 (4) (2018) 779–792.

[51] A. Novellino, C. Jordan, G. Ager, L. Bateson, C. Fleming, P. Confuorto, Remote sensing for natural or man-made disasters and environmental changes, in: Geological Disaster Monitoring Based on Sensor Networks, Springer, 2019, pp. 23–31.

[52] R. Miceli, I. Sotgiu, M. Settanni, Disaster preparedness and perception of flood risk: A study in an Alpine Valley in Italy, J. Environ. Psychol. 28 (2) (2008) 164–173.

[53] L.K. Comfort, W.L. Waugh, B.A. Cigler, Emergency management research and practice in public administration: Emergence, evolution, expansion, and future directions, Public Adm. Rev. 72 (4) (2012) 539–547.

[54] L. Schipper, M. Pelling, Disaster risk, climate change and international development: Scope for, and challenges to, integration, Disasters 30 (1) (2006) 19–38.

[55] C.D. Reese, Occupational Health and Safety Management: A Practical Approach, CRC press, 2015, pp. 1–513.

[56] J. Yeung, H. Regan, A. Renton, E. Reynolds, M. Hayes, M. Wagner, March 24 coronavirus news, CNN [online]. (Accessed 27-04-2020), 2020, URL https://edition.cnn.com/world/live-news/coronavirus-outbreak-03-24-20-intl-hnk/h_b5c13ce244635a6e5b945f6462b4a374.

[57] K.T.O. Coimbra, E. Alcântara, C.R. de Souza Filho, An assessment of natural and manmade hazard effects on the underwater light field of the Doce River Continental Shelf, Sci. Total Environ. 685 (2019) 1087–1096.

[58] L. Coleman, Frequency of man-made disasters in the 20th century, J. Conting. Crisis Manag. 14 (1) (2006) 3–11.

[59] N. Pidgeon, M. O'Leary, Man-made disasters: Why technology and organizations (sometimes) fail, Saf. Sci. 34 (1) (2000) 15–30, http://dx.doi.org/10.1016/S0925-7535(00)00004-7, URL http://www.sciencedirect.com/science/article/pii/S0925753500000047.

[60] T. Sandler, The analytical study of terrorism: Taking stock, J. Peace Res. 51 (2013) 257–271, http://dx.doi.org/10.1177/0022343313491277.

[61] E.H. Kaplan, A. Mintz, S. Mishal, Tactical prevention of suicide bombings in Israel, Interfaces 36 (6) (2006) 553–561.

[62] A. Kaplan, The Counter-terrorism Puzzle: A Guide for Decision Makers, Routledge, 2017.

[63] X. Hu, F. Lai, G. Chen, R. Zou, Q. Feng, Quantitative research on global terrorist attacks and terrorist attack classification, Sustainability 11 (5) (2019) 1487–1500.

[64] W.V. Pelfrey Jr., Local law enforcement terrorism prevention efforts: A state level Case study, J. Crim. Justice 35 (3) (2007) 313–321.

[65] R.W. Taylor, E.J. Fritsch, J. Liederbach, Digital Crime and Digital Terrorism, Prentice Hall Press, 2014.

[66] W. Enders, T. Sandler, Distribution of transnational terrorism among countries by income class and geography after 9/11, Int. Stud. Q. 50 (2) (2006) 367–393.

[67] B. Hoffman, P. St John, Inside terrorism, Int. J. 55 (1) (2000) 1–159.

[68] A. Alnoman, A. Anpalagan, On D2D communications for public safety applications, in: Humanitarian Technology Conference (IHTC), 2017 IEEE Canada International, pp. 120–127.

[69] T. Ohtsuji, K. Muraoka, H. Aminaka, D. Kanetomo, Y. Matsunaga, Device-to-device relay selection based on effective path throughput to fill coverage hole in public safety LTE, in: Information and Communication Technology Convergence (ICTC), International Conference on, IEEE, 2016, pp. 613–618.

[70] D.G. Cileo, N. Sharma, M. Magarini, Coverage, Capacity and interference analysis for an aerial base station in different environments, in: International Symposium on Wireless Communication Systems (ISWCS), 2017, pp. 281–286, http://dx.doi.org/10.1109/ISWCS.2017.8108125.

[71] CAREER, CAREER: Towards broadband and UAV-assisted heterogeneous networks for public safety communication, (NSF,USARef. Nr: CNS-1453678), 2015, [Online]. Available: https://sites.google.com/site/uav4psc/home (Accessed 22-10-2019).

[72] C. TERROR, Public Safety COmmUNication in ConTExt Related to Terror Attacks, (NATO SPS), 2019, [Online]. Available: https://www.counterterror.eu/ (Accessed 22-10-2019).

[73] X. Lin, J.G. Andrews, A. Ghosh, R. Ratasuk, An overview of 3GPP device-to-device proximity services, IEEE Commun. Mag. 52 (4) (2014) 40–48, http://dx.doi.org/10.1109/MCOM.2014.6807945.

[74] 3GPP TR 36.843 V12.0.1, Technical specification group radio access network; Study on lte device to device proximity services; radio aspects (release 12), 2014.

[75] 3GPP TS 23.002 V12.6.0, Technical specification services and system aspects; Network architecture; (release 12), 2014.

[76] 3GPP TR 23.703 V12.0.0, Technical specification group services and system aspects; study on architecture enhancements to support proximity-based services (release 12), 2014.

[77] 3GPP TS 23.303 V15.1.0, Technical specification group services and system aspects; Proximity Based services (ProSe); stage 2 (release 15), 2018.

[78] 3GPP TS 23.343 V0.1.0, Technical specification group core network and terminals; Proximity-services (ProSe) function to prose application server aspects (PC2); stage 3; (release 12), 2014.

[79] 3GPP TS 23.334 V1.1.0, Technical specification group core network and terminals; Proximity services (ProSe) user equipment (UE) to proximity-services (ProSe) function protocol aspects; stage 3 (release 12), 2014.

[80] 3GPP TS 29.334 V12.3.0, Technical specification group core network and terminals; IMS application level gateway (IMS-ALG) IMS access gateway (IMSAGW); iq interface; stage 3 (release 12), 2014.

[81] M. Alam, D. Yang, J. Rodriguez, R.A. Abd-alhameed, Secure device-to-device communication in LTE-A, IEEE Commun. Mag. 52 (4) (2014) 66–73, http://dx.doi.org/10.1109/MCOM.2014.6807948.

[82] 3GPP TSG RAN Meeting 75, RP-170295, Study on further enhancements to LTE device to device, UE to network relays for IoT and wearables, 2017.

[83] M.M. Alam, D.B. Arbia, E.B. Hamida, Research trends in multi-standard device-to-device communication in wearable wireless networks, in: Cognitive Radio Oriented Wireless Networks, Springer International Publishing, 2015, pp. 735–746.

[84] M.M. Alam, D.B. Arbia, E.B. Hamida, Wireless Public Safety Networks - Series II, Wiley-Springer, 2016, pp. 63–94.

[85] 3GPP TS 22.186 V16.0.0, Technical Specification Group Services and System Aspects; Enhancement of 3GPP support for V2X scenarios; Stage 1 (Release 16), 2018.

[86] BSA-D2D, Base station (bs) aided D2D (device to device) communication in cellular networks, (fp7 project reference number: 274523), 2019, [Online]. (Accessed 22-10-2019) http://cordis.europa.eu/project/rcn/98651_en.html.

[87] F. Adachi, Y.K. Kddi, S. Ohmori, K. Takeuchi, M. Hamaguchi, R. Kajiwara, R&D project of Multilayered Communications Network - For Disaster-Resilient Communications, in: the 15th International Symposium on Wireless Personal Multimedia Communications, 2012, pp. 350–351.

[88] ABSOULTE, Aerial base stations with opportunistic links for unexpected & temporary events - ABSOLUTE" (FP7 Ref. Nr.ICT-318632), 2012, [Online].(Accessed 22-10-2019). https://www.hhi.fraunhofer.de/en/departments/wn/projects/archive/absolute.html.

[89] CODEC, Cellular network based device-to-device wireless communications, (FP7 MC project, reference number: 630058), 2014.

[90] Texas, Device-to-device (D2D) communication: Fundamentals with applications to LTE, 2014, [Online]. (Accessed 22-10-2019) URL https://wncg.org/research/briefs/device-device-d2d-communication-fundamentals-applications-lte.

[91] PSS, Pervasive spectrum sharing for public safety communications, (NSF Ref. Nr: NSFEARS-2014-1443946), 2014.

[92] COHERENT, Coordinated control and spectrum management for 5G heterogeneous radio access networks, (EU Grant, H2020-ICT-14-2014), 2015, http://www.ict-coherent.eu/.

[93] METIS-II, Mobile and wireless communications enablers for twenty-twenty (2020) information society-II, (H2020-ICT-2014-2), 2015, [Online]. Available: https://metis-ii.5g-ppp.eu (Accessed 22-10-2019).

[94] NICER, Networked infrastructureless cooperation for emergency response , (LOEWE- excellent research for Hesse's future), 2015, [Online]. (Accessed 22-10-2019) https://www.nicer.tu-darmstadt.de/en/nicer/overview/.

[95] BROADMAP, Mapping interoperable eu ppdr broadband communication applications and technology - BROADMAP, (H2020 Ref. Nr.700380), 2016, [Online]. Available: http://www.broadmap.eu/ (Accessed 22-10-2019).

[96] LCMSSER, Location-based control and management system for safety and emergency rescuing services using LTE D2D technology, (Newton Fund, British Council), 2016, [Online]. Available: http://5g-iot.mdx.ac.uk/?page-id=201 (Accessed 22-10-2019).

[97] DDPS, Device-to-device system for public safety, (NIST), 2017, [Online]. Available: https://www.nist.gov/ctl/pscr/device-device-system-public-safety (Accessed 22-10-2019).

[98] BROADWAY, Innovation activity to develop technologies to enable a pan-european interoperable broadband mobile system for PPDR, validated by sustainable testing facilities, (H2020 Ref. Nr.786912), 2018, [Online]. Available: https://www.broadway-info.eu/ (Accessed 22-10-2019).

[99] 3GPP TS 36.300 V15.4.0, Technical specification group radio access network; evolved universal terrestrial radio access (e-UTRA) and evolved universal terrestrial radio access network (E-UTRAN); overall description; stage 2 (release 15), 2018.

[100] ETSITS 124 334 V13.2.0, Proximity-services (ProSe) user equipment (UE) to ProSe functions protocol aspects; stage 3 (release 13), 2018.

[101] B. Zhang, Y. Li, D. Jin, Z. Han, Network science approach for device discovery in mobile device-to-device communications, IEEE Trans. Veh. Technol. 65 (7) (2016) 5665–5679, http://dx.doi.org/10.1109/TVT.2015.2453234.

[102] D. Camps-Mur, A. Garcia-Saavedra, P. Serrano, Device-to-device communications with Wi-Fi Direct: Overview and experimentation, IEEE Wirel. Commun. 20 (3) (2013) 96–104, http://dx.doi.org/10.1109/MWC.2013.6549288.

[103] B. Han, J. Li, A. Srinivasan, On the energy efficiency of device discovery in mobile opportunistic networks: A systematic approach, IEEE Trans. Mob. Comput. 14 (4) (2015) 786–799, http://dx.doi.org/10.1109/TMC.2014.2333749.

[104] D. Camps-Mur, E. Garcia-Villegas, E. Lopez-Aguilera, P. Loureiro, P. Lambert, A. Raissinia, Enabling always on service discovery: Wi-fi neighbor awareness networking, IEEE Wirel. Commun. 22 (2) (2015) 118–125, http://dx.doi.org/10.1109/MWC.2015.7096294.

[105] K. Cho, G. Park, W. Cho, J. Seo, K. Han, Performance analysis of device discovery of bluetooth low energy (BLE) networks, Comput. Commun. 81 (2016) 72–85.

[106] Z. Yuan, J. Jin, J. Chen, L. Sun, G. Muntean, Comprose: Shaping future public safety communities with ProSe-based UAVs, IEEE Commun. Mag. 55 (12) (2017) 165–171, http://dx.doi.org/10.1109/MCOM.2017.1600869.

[107] F. Jiang, A.L. Swindlehurst, Dynamic UAV relay positioning for the ground-to-air uplink, in: IEEE Globecom Workshops, 2010, pp. 1766–1770, http://dx.doi.org/10.1109/GLOCOMW.2010.5700245.

[108] J. Ouyang, Y. Zhuang, M. Lin, J. Liu, Optimization of beamforming and path planning for UAV-assisted wireless relay networks, Chin. J. Aeronaut. 27 (2) (2014) 313–320, http://dx.doi.org/10.1016/j.cja.2014.02.011, http://www.sciencedirect.com/science/article/pii/S100093611400020X.

[109] N. Rupasinghe, A.S. Ibrahim, I. Guvenc, Optimum hovering locations with angular domain user separation for cooperative UAV networks, in: IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2016.7842113.

[110] Z. Xiao, P. Xia, X. Xia, Enabling UAV cellular with millimeter-wave communication: Potentials and approaches, IEEE Commun. Mag. 54 (5) (2016) 66–73, http://dx.doi.org/10.1109/MCOM.2016.7470937.

[111] Y. Shi, R. Enami, J. Wensowitch, J. Camp, UABeam: UAV-based beamforming system analysis with in-field air-to-ground channels, in: 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2018, pp. 1–9, http://dx.doi.org/10.1109/SAHCN.2018.8397110.

[112] B. Li, C. Chen, R. Zhang, H. Jiang, X. Guo, The energy-efficient UAV-based BS coverage in air-to-ground communications, in: IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2018, pp. 578–581, http://dx.doi.org/10.1109/SAM.2018.8448770.

[113] S. Fan, J. Liu, M. Tian, H. Huang, F. Dai, L. Yang, G. Gui, Robust adaptive beamforming signal techniques for drone surveillance, in: IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2018, pp. 582–586, http://dx.doi.org/10.1109/SAM.2018.8448700.

[114] L.K. Dressel, M.J. Kochenderfer, Efficient and low-cost localization of radio signals with a multirotor UAV, in: AIAA Guidance, Navigation, and Control Conference, 2018, p. 1845.

[115] M. Petitjean, S. Mezhoud, F. Quitin, Fast localization of ground-based mobile terminals with a transceiver-equipped UAV, in: 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2018, pp. 323–327.

[116] F. Koohifar, I. Guvenc, M.L. Sichitiu, Autonomous tracking of intermittent RF source using a UAV swarm, IEEE Access 6 (2018) 15884–15897.

[117] S. Tang, X. Shu, J. Hu, R. Zhou, S. Shen, S. Cao, Study on RSS/AOA hybrid localization in life detection in huge disaster situation, Nat. Hazards (2018) 1–15.

[118] M. Hasanzade, O. Herekoglu, N.K. Ure, E. Koyuncu, R. Yeniceri, G. Inalhan, Localization and tracking of RF emitting targets with multiple unmanned aerial vehicles in large scale environments with uncertain transmitter power, in: Unmanned Aircraft Systems (ICUAS), International Conference on, IEEE, 2017, pp. 1058–1065.

[119] N. Garcia, H. Wymeersch, E.G. Larsson, A.M. Haimovich, M. Coulon, Direct localization for mssive MIMO, IEEE Trans. Signal Process. 65 (10) (2017) 2475–2487.

[120] R.P. Fernandes, J.A. Apolinário, A.L. Ramos, Bearings-only aerial shooter localization using a microphone array mounted on a drone, in: Circuits & Systems (LASCAS), in 8th Latin American Symposium on, IEEE, 2017, pp. 1–4.

[121] K. Doppler, M. Rinne, C. Wijting, C.B. Ribeiro, K. Hugl, Device-to-device communication as an underlay to LTE-advanced networks, IEEE Commun. Mag. 47 (12) (2009) 42–49, http://dx.doi.org/10.1109/MCOM.2009.5350367.

[122] U. Saleem, S. Jangsher, H.K. Qureshi, S.A. Hassan, Joint subcarrier and power allocation in the energy-harvesting-aided D2D communication, IEEE Trans. Ind. Inf. 14 (6) (2018) 2608–2617.

[123] D. Feng, L. Lu, Y. Yuan-Wu, G.Y. Li, G. Feng, S. Li, Device-to-device communications underlaying cellular networks, IEEE Trans. Commun. 61 (8) (2013) 3541–3551, http://dx.doi.org/10.1109/TCOMM.2013.071013.120787.

[124] Y. Yuan, T. Yang, Y. Hu, H. Feng, B. Hu, Matching based two-timescale resource allocation for cooperative D2D communication (technical report), 2018, pp. 208–219, arXiv preprint arXiv:1810.13116.

[125] M. Zulhasnine, C. Huang, A. Srinivasan, Efficient resource allocation for device-to-device communication underlaying LTE network, in: IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, 2010, pp. 368–375, http://dx.doi.org/10.1109/WIMOB.2010.5645039.

[126] R. An, J. Sun, S. Zhao, S. Shao, Resource allocation scheme for device-to-device communication underlying LTE downlink network, in: International Conference on Wireless Communications and Signal Processing (WCSP), 2012, pp. 1–5, http://dx.doi.org/10.1109/WCSP.2012.6542986.

[127] F. Wang, L. Song, Z. Han, Q. Zhao, X. Wang, Joint scheduling and resource allocation for device-to-device underlay communication, in: IEEE Wireless Communications and Networking Conference (WCNC), 2013, pp. 134–139, http://dx.doi.org/10.1109/WCNC.2013.6554552.

[128] H.H. Esmat, M.M. Elmesalawy, I.I. Ibrahim, Adaptive resource sharing algorithm for device-to-device communications underlaying cellular networks, IEEE Commun. Lett. 20 (3) (2016) 530–533, http://dx.doi.org/10.1109/LCOMM.2016.2517012.

[129] Y. Kai, H. Zhu, Resource allocation for multiple-pair d2d communications in cellular networks, in: IEEE International Conference on Communications (ICC), 2015, pp. 2955–2960, http://dx.doi.org/10.1109/ICC.2015.7248776.

[130] C. Kai, L. Xu, J. Zhang, M. Peng, Joint uplink and downlink resource allocation for d2d communication underlying cellular networks, in: 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 2018, pp. 1–6.

[131] Y. Luo, Z. Feng, H. Jiang, Y. Yang, Y. Huang, J. Yao, Game-theoretic learning approaches for secure d2d communications against full-duplex active eavesdropper, IEEE Access 7 (2019) 41324–41335.

[132] H. Malik, M. Ghoraishi, R. Tafazolli, Suboptimal radio resource management for full-duplex enabled small cells, in: IEEE International Conference on Communications Workshops (ICC Workshops), 2017, pp. 942–947.

[133] M.I. Khan, M.M. Alam, Y.L. Moullec, E. Yaacoub, Throughput-aware cooperative reinforcement learning for adaptive resource allocation in device-to-device communication, Future Internet 9 (4) (2017) http://dx.doi.org/10.3390/fi9040072, URL http://www.mdpi.com/1999-5903/9/4/72.

[134] S. Nie, Z. Fan, M. Zhao, X. Gu, L. Zhang, Q-learning based power control algorithm for D2D communication, in: IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016, pp. 1–6, http://dx.doi.org/10.1109/PIMRC.2016.7794793.

[135] Y. Luo, Z. Shi, X. Zhou, Q. Liu, Q. Yi, Dynamic resource allocations based on Q-learning for D2D communication in cellular networks, in: 11th International Computer Conference on Wavelet Actiev Media Technology and Information Processing(ICCWAMTIP), 2014, pp. 385–388, http://dx.doi.org/10.1109/ICCWAMTIP.2014.7073432.

[136] J. Kim, J. Park, J. Noh, S. Cho, Completely distributed power allocation using deep neural network for device to device communication underlaying LTE, 2018, pp. 20–32, arXiv preprint arXiv:1802.02736.

[137] R. Rouil, F.J. Cintrón, A. Ben Mosbah, S. Gamboa, Implementation and validation of an LTE d2d model for NS-3, in: Proceedings of the Workshop on Ns-3, ACM, 2017, pp. 55–62.

[138] G. Poitau, B. Pelletier, G. Pelletier, D. Pani, A combined PUSH/pull service discovery model for LTE direct, in: IEEE 80th Vehicular Technology Conference (VTC2014-Fall), 2014, pp. 1–5, http://dx.doi.org/10.1109/VTCFall.2014.6965805.

[139] A.B. Mosbah, D. Griffith, R. Rouil, Enhanced transmission algorithm for dynamic device-to-device direct discovery, in: 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–8, http://dx.doi.org/10.1109/CCNC.2018.8319178.

[140] A. Prasad, A. Kunz, G. Velev, K. Samdanis, J. Song, Energy-efficient D2D discovery for proximity services in 3GPP LTE-advanced networks: ProSe discovery mechanisms, IEEE Veh. Technol. Mag. 9 (4) (2014) 40–50, http://dx.doi.org/10.1109/MVT.2014.2360652.

[141] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, N. Brahmi, Device-to-device communications for national security and public safety, IEEE Access 2 (2014) 1510–1520, http://dx.doi.org/10.1109/ACCESS.2014.2379938.

[142] D.W. Griffith, F.J. Cintrón, R.A. Rouil, Physical sidelink control channel (PSCCH) in mode 2: Performance analysis, in: IEEE International Conference on Communications (ICC), 2017, pp. 1–7, http://dx.doi.org/10.1109/ICC.2017.7997074.

[143] D. Griffith, F. Cintron, A. Galazka, T. Hall, R. Rouil, Modeling and simulation analysis of the physical sidelink shared channel (PSSCH), in: IEEE International Conference on Communications (ICC), 2018, pp. 1–7, http://dx.doi.org/10.1109/ICC.2018.8422164.

[144] 3GPP TS 36.213 V15.3.0, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures; TS 36.213,, 2016.

[145] F. Eckermann, J. Freudenthal, C. Wietfeld, Performance analysis of unsupervised LTE device-to-device (D2D) communication, in: IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1–5.

[146] 3GPP TS 36.321 V15.3.0, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification; TS 36.321, 2018.

[147] 3GPP TS 36.211 V15.3.0, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation; TS 36.211,, 2018.

[148] H. Nishiyama, T. Ngo, S. Oiyama, N. Kato, Relay by smart device: Innovative communications for efficient information sharing among vehicles and pedestrians, IEEE Veh. Technol. Mag. 10 (4) (2015) 54–62.

[149] S. Sabino, N. Horta, A. Grilo, Centralized unmanned aerial vehicle mesh network placement scheme: A multi-objective evolutionary algorithm approach, Sensors 18 (12) (2018) 1–16, http://dx.doi.org/10.3390/s18124387, URL http://www.mdpi.com/1424-8220/18/12/4387.

[150] D.G. Reina, M. Askalani, S.L. Toral, F. Barrero, E. Asimakopoulou, N. Bessis, A survey on multihop ad hoc networks for disaster response scenarios, Int. J. Distrib. Sen. Netw. (2015) 1–33, http://dx.doi.org/10.1155/2015/647037.

[151] M. del Pilar Salamanca, J. Camargo, A survey on IEEE 802.11-based MANETs and DTNs for survivor communication in disaster scenarios, in: IEEE Global Humanitarian Technology Conference (GHTC), 2016, pp. 197–204, http://dx.doi.org/10.1109/GHTC.2016.7857280.

[152] Y. Kawamoto, H. Nishiyama, N. Kato, Toward terminal-to-terminal communication networks: A hybrid MANET and DTN approach, in: IEEE 18th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2013, pp. 228–232, http://dx.doi.org/10.1109/CAMAD.2013.6708122.

[153] D.G. Reina, J.M.L. Coca, M. Askalani, S.L. Toral, F. Barrero, E. Asimakopoulou, S. Sotiriadis, N. Bessis, A survey on ad hoc networks for disaster scenarios, in: International Conference on Intelligent Networking and Collaborative Systems, 2014, pp. 433–438, http://dx.doi.org/10.1109/INCoS.2014.28.

[154] E. Rosas, N. Hidalgo, V. Gil-Costa, C. Bonacic, M. Marin, H. Senger, L. Arantes, C. Marcondes, O. Marin, Survey on simulation for mobile ad-hoc communication for disaster scenarios, J. Comput. Sci. Technol. 31 (2) (2016) 326–349, http://dx.doi.org/10.1007/s11390-016-1630-x.

[155] S. Rosati, K. Krużelecki, G. Heitz, D. Floreano, B. Rimoldi, Dynamic routing for flying ad hoc networks, IEEE Trans. Veh. Technol. 65 (3) (2016) 1690–1700, http://dx.doi.org/10.1109/TVT.2015.2414819.

[156] F.S. Shaikh, R. Wismüller, Routing in multi-hop cellular device-to-device (D2D) networks: A survey, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2622–2657, http://dx.doi.org/10.1109/COMST.2018.2848108.

[157] M. Zhou, H. Zhang, S. Zhang, L. Song, Y. Li, Z. Han, Design and implementation of device-to-device software-defined networks, in: IEEE International Conference on Communications (ICC), 2016, pp. 1–6, http://dx.doi.org/10.1109/ICC.2016.7511134.

[158] M. Abolhasan, M. Abdollahi, W. Ni, A. Jamalipour, N. Shariati, J. Lipman, A routing framework for offloading traffic from cellular networks to SDN-based multi-hop device-to-device networks, IEEE Trans. Netw. Serv. Manag. 15 (4) (2018) 1516–1531, http://dx.doi.org/10.1109/TNSM.2018.2875696.

[159] M. Abolhasan, J. Lipman, W. Ni, B. Hagelstein, Software-defined wireless networking: Centralized, distributed, or hybrid?, IEEE Netw. 29 (4) (2015) 32–38, http://dx.doi.org/10.1109/MNET.2015.7166188.

[160] H.B. Valiveti, P.T. Rao, EHSD: An exemplary handover scheme during D2D communication based on decentralization of SDN, Wirel. Personal Commun. 94 (4) (2017) 2393–2416, http://dx.doi.org/10.1007/s11277-016-3490-7.

[161] X. Huang, R. Yu, J. Kang, Z. Xia, Y. Zhang, Software defined networking for energy harvesting Internet of Things, IEEE Internet of Things J. 5 (3) (2018) 1389–1399, http://dx.doi.org/10.1109/JIOT.2018.2799936.

[162] H. Wang, S. Chen, H. Xu, M. Ai, Y. Shi, SoftNet: A software defined decentralized mobile network architecture toward 5G, IEEE Netw. 29 (2) (2015) 16–22, http://dx.doi.org/10.1109/MNET.2015.7064898.

[163] H. Ali-Ahmad, C. Cicconetti, A. de la Oliva, M. Dräxler, R. Gupta, V. Mancuso, L. Roullet, V. Sciancalepore, CROWD: An SDN approach for densenets, in: Second European Workshop on Software Defined Networks, 2013, pp. 25–31, http://dx.doi.org/10.1109/EWSDN.2013.11.

[164] A.A. Gebremariam, M. Usman, R. Bassoli, F. Granelli, SoftPSN: Software-defined resource slicing for low-latency reliable public safety networks, Wirel. Commun. Mob. Comput. (4) (2018) 39–47.

[165] M. Chen, Y. Zhang, L. Hu, T. Taleb, Z. Sheng, Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5G technologies, Mob. Netw. Appl. 20 (6) (2015) 704–712, http://dx.doi.org/10.1007/s11036-015-0590-7.

[166] W. Xia, Y. Wen, C.H. Foh, D. Niyato, H. Xie, A survey on software-defined networking, IEEE Commun. Surv. Tutor. 17 (1) (2015) 27–51.

[167] I.T. Haque, N. Abu-Ghazaleh, Wireless software defined networking: A survey and taxonomy, IEEE Commun. Surv. Tutor. 18 (4) (2016) 2713–2737, http://dx.doi.org/10.1109/COMST.2016.2571118.

[168] M. Wetterwald, X.-N. D. Saucez, T. TurlettiJ, SDN for Public Safety Networks, Research Report hal-01400746, Inria Sophia Antipolis, 2016, pp. 1–32.

[169] R. Jayadi, Y. Lai, Low-overhead multihop device-to-device communications in software defined wireless networks, in: International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT), 2017, pp. 144–149, http://dx.doi.org/10.1109/ICSIIT.2017.30.

[170] M. Usman, A.A. Gebremariam, U. Raza, F. Granelli, A software-defined device-to-device communication architecture for public safety applications in 5G networks, IEEE Access 3 (2015) 1649–1654, http://dx.doi.org/10.1109/ACCESS.2015.2479855.

[171] V.K. Mishra, A. Dusia, A. Sethi, Routing in Software-Defined Mobile Ad hoc Networks (SD-MANET), Technical Report ARL-TR-8469, in US Army Research Laboratory, Aug 2018, pp. 1–34.

[172] A. Thomas, G. Raja, FINDER: A D2D based critical communications framework for disaster management in 5G, Peer-to-Peer Netw. Appl. (2018) 1–27, http://dx.doi.org/10.1007/s12083-018-0689-2, https://doi.org/10.1007/s12083-018-0689-2.

[173] J. Wang, Y. Miao, P. Zhou, M.S. Hossain, S.M.M. Rahman, A software defined network routing in wireless multihop network, J. Netw. Comput. Appl. 85 (2017) 76–83, Intelligent Systems for Heterogeneous Networks. http://dx.doi.org/10.1016/j.jnca.2016.12.007. URL http://www.sciencedirect.com/science/article/pii/S1084804516303058.

[174] K. Grover, A. Lim, Q. Yang, Jamming and anti-jamming techniques in wireless networks: A survey, Int. J. Ad Hoc Ubiquitous Comput. 17 (4) (2014) 197–215, http://dx.doi.org/10.1504/IJAHUC.2014.066419.

[175] S.R. Ratna, R. Ravi, Survey on jamming wireless networks: Attacks and prevention strategies, Int. J. Comput. Electr. Autom. Control Inf. Eng. 9 (2) (2015) 110–117.

[176] C. Shahriar, M. La Pan, M. Lichtman, T.C. Clancy, R. McGwier, R. Tandon, S. Sodagari, J.H. Reed, PHY-Layer resiliency in OFDM communications: A tutorial, IEEE Commun. Surv. Tutor. 17 (1) (2015) 292–314, http://dx.doi.org/10.1109/COMST.2014.2349883.

[177] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, C. Pöpper, On security research towards future mobile network generations, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2518–2542, http://dx.doi.org/10.1109/COMST.2018.2820728.

[178] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765, http://dx.doi.org/10.1109/JPROC.2016.2558521.

[179] F. Jameel, S. Wyne, G. Kaddoum, T.Q. Duong, A comprehensive survey on cooperative relaying and jamming strategies for physical layer security, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2734–2771, http://dx.doi.org/10.1109/COMST.2018.2865607.

[180] M. Lichtman, R.P. Jover, M. Labib, R. Rao, V. Marojevic, J.H. Reed, LTE/LTE-A Jamming, spoofing, and sniffing: Threat assessment and mitigation, IEEE Commun. Mag. 54 (4) (2016) 54–61, http://dx.doi.org/10.1109/MCOM.2016.7452266.

[181] T. Pushpalata, S.Y. Chaudhari, Need of physical layer security in LTE: Analysis of vulnerabilities in LTE physical layer, in: 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 1722–1727, http://dx.doi.org/10.1109/WiSPNET.2017.8300057.

[182] R.M. Rao, S. Ha, V. Marojevic, J.H. Reed, LTE Phy layer vulnerability analysis and testing using open-source sdr tools, in: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 744–749, http://dx.doi.org/10.1109/MILCOM.2017.8170787.

[183] X. Li, Z. Wang, A study on pseudo CRS signal jamming attacks in LTE network, in: 2018 IEEE Symposium on Computers and Communications (ISCC), 2018, pp. 1–4, http://dx.doi.org/10.1109/ISCC.2018.8538662.

[184] G. Romero, V. Deniau, O. Stienne, LTE Physical layer vulnerability test to different types of jamming signals, in: 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, 2019, pp. 1138–1143, http://dx.doi.org/10.1109/EMCEurope.2019.8872052.

[185] F. Girke, F. Kurtz, N. Dorsch, C. Wietfeld, Towards resilient 5G: Lessons learned from experimental evaluations of LTE uplink jamming, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–6, http://dx.doi.org/10.1109/ICCW.2019.8756977.

[186] H. Alakoca, H.B. Tugrel, G.K. Kurt, C. Ayyildiz, CP And pilot jamming attacks on SC-FDMA: Performance tests with software defined radios, in: 2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS), 2016, pp. 1–6, http://dx.doi.org/10.1109/ICSPCS.2016.7843341.

[187] V. Marojevic, R.M. Rao, S. Ha, J.H. Reed, Performance analysis of a mission-critical portable LTE system in targeted RF interference, in: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 2017, pp. 1–6, http://dx.doi.org/10.1109/VTCFall.2017.8288187.

[188] R.M. Rao, V. Marojevic, J.H. Reed, Analysis of non-pilot interference on link adaptation and latency in cellular networks, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1–5, http://dx.doi.org/10.1109/VTCSpring.2019.8746307.

[189] M. Lichtman, R. Rao, V. Marojevic, J. Reed, R.P. Jover, 5g NR jamming, spoofing, and sniffing: Threat assessment and mitigation, in: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018, pp. 1–6, http://dx.doi.org/10.1109/ICCW.2018.8403769.

[190] M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, Enhancing the robustness of LTE systems: Analysis and evolution of the cell selection process, IEEE Commun. Mag. 55 (2) (2017) 208–215, http://dx.doi.org/10.1109/MCOM.2017.1500706CM.

[191] M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, How to enhance the immunity of LTE systems against RF spoofing, in: 2016 International Conference on Computing, Networking and Communications (ICNC), 2016, pp. 1–5, http://dx.doi.org/10.1109/ICCNC.2016.7440650.

[192] A. El-Keyi, O. Üreten, H. Yanikomeroglu, T. Yensen, LTE For public safety networks: Synchronization in the presence of jamming, IEEE Access 5 (2017) 20800–20813, http://dx.doi.org/10.1109/ACCESS.2017.2751964.

[193] F.M. Aziz, J.S. Shamma, G.L. Stüber, Resilience of LTE networks against smart jamming attacks: Wideband model, in: 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015, pp. 1344–1348, http://dx.doi.org/10.1109/PIMRC.2015.7343507.

[194] F.M. Aziz, J.S. Shamma, G.L. Stüber, Jammer-type estimation in LTE with a smart jammer repeated game, IEEE Trans. Veh. Technol. 66 (8) (2017) 7422–7431, http://dx.doi.org/10.1109/TVT.2017.2672682.

[195] A. Zhang, X. Lin, Security-aware and privacy-preserving D2D communications in 5G, IEEE Netw. 31 (4) (2017) 70–77, http://dx.doi.org/10.1109/MNET.2017.1600290.

[196] R. Curpen, T. Bălan, I.A. Micloş, I. Comănici, Assessment of signal jamming efficiency against LTE UAVs, in: 2018 International Conference on Communications (COMM), 2018, pp. 367–370, http://dx.doi.org/10.1109/ICComm.2018.8484746.

[197] J. Tang, G. Chen, J.P. Coon, Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers, IEEE Trans. Inf. Forensics Secur. 14 (11) (2019) 3026–3041, http://dx.doi.org/10.1109/TIFS.2019.2912074.

[198] R. Ma, W. Yang, Y. Zhang, J. Liu, H. Shi, Secure mmwave communication using UAV-enabled relay and cooperative jammer, IEEE Access 7 (2019) 119729–119741, http://dx.doi.org/10.1109/ACCESS.2019.2933231.

[199] B. Li, Z. Fei, Y. Zhang, M. Guizani, Secure UAV communication networks over 5G, IEEE Wirel. Commun. 26 (5) (2019) 114–120, http://dx.doi.org/10.1109/MWC.2019.1800458.

[200] L. Xiao, C. Xie, M. Min, W. Zhuang, User-centric view of unmanned aerial vehicle transmission against smart attacks, IEEE Trans. Veh. Technol. 67 (4) (2018) 3420–3430, http://dx.doi.org/10.1109/TVT.2017.2785414.

[201] N. Gao, Z. Qin, X. Jing, Q. Ni, S. Jin, Anti-intelligent UAV jamming strategy via deep Q-networks, IEEE Trans. Commun. (2019) 1–6, http://dx.doi.org/10.1109/TCOMM.2019.2947918.

[202] H. Sedjelmaci, S.M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks, IEEE Trans. Syst. Man Cybern. 48 (9) (2018) 1594–1606, http://dx.doi.org/10.1109/TSMC.2017.2681698.

[203] L. Zhang, L. Huang, B. Li, M. Huang, J. Yin, W. Bao, Fast-moving jamming suppression for UAV navigation: A minimum dispersion distortionless response beamforming approach, IEEE Trans. Veh. Technol. 68 (8) (2019) 7815–7827, http://dx.doi.org/10.1109/TVT.2019.2924951.

[204] Y. Gao, H. Tang, B. Li, X. Yuan, Joint trajectory and power design for UAV-enabled secure communications with no-fly zone constraints, IEEE Access 7 (2019) 44459–44470, http://dx.doi.org/10.1109/ACCESS.2019.2908407.

[205] Y. Xu, G. Ren, J. Chen, X. Zhang, L. Jia, Z. Feng, Y. Xu, Joint power and trajectory optimization in UAV anti-jamming communication networks, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–5, http://dx.doi.org/10.1109/ICC.2019.8761467.

[206] K. Li, S.S. Kanhere, W. Ni, E. Tovar, M. Guizani, Proactive eavesdropping via jamming for trajectory tracking of UAVs, in: 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), 2019, pp. 477–482, http://dx.doi.org/10.1109/IWCMC.2019.8766696.

[207] M. Mah, H. Lim, A.W. Tan, UAV Relay flight path planning in the presence of jamming signal, IEEE Access 7 (2019) 40913–40924, http://dx.doi.org/10.1109/ACCESS.2019.2907962.

[208] B. Van den Bergh, S. Pollin, Keeping UAVs under control during GPS jamming, IEEE Syst. J. 13 (2) (2019) 2010–2021, http://dx.doi.org/10.1109/JSYST.2018.2882769.

[209] 3GPP TR 36.777 V15.0.0, Technical Specification Group Radio Access Network; Study on Enhanced LTE Support for Aerial Vehicles (Release 15), 2017.

[210] S.N. Venkatasubramanian, Propagation Channel Model Between Unmanned aerial Vehicles for Emergency Communications, G2 Pro gradu, diplomityö, 2013, pp. 63–87, URL http://urn.fi/URN:NBN:fi:aalto-201303201831.

[211] V. Nurmela, A. Karttunen, A. Roivainen, L. Raschkowski, V. Hovinen, J.Y. EB, N. Omaki, K. Kusume, A. Hekkala, R. Weiler, et al., Deliverable D1. 4 METIS channel models, in: Proc. Mobile Wireless Commun. Enablers Inf. Soc.(METIS), 2015, pp. 1–223.

[212] A.A. Khuwaja, Y. Chen, N. Zhao, M. Alouini, P. Dobbins, A survey of channel modeling for UAV communications, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2804–2821, http://dx.doi.org/10.1109/COMST.2018.2856587.

[213] C. Yan, L. Fu, J. Zhang, J. Wang, A comprehensive survey on UAV communication channel modeling, IEEE Access 7 (2019) 107769–107792, http://dx.doi.org/10.1109/ACCESS.2019.2933173.

[214] W. Khawaja, I. Guvenc, D.W. Matolak, U. Fiebig, N. Schneckenburger, A survey of air-to-ground propagation channel modeling for unmanned aerial vehicles, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2361–2391, http://dx.doi.org/10.1109/COMST.2019.2915069.

[215] X. Cheng, Y. Li, B. Ai, X. Yin, Q. Wang, Device-to-device channel measurements and models: A survey, IET Commun. 9 (3) (2015) 312–325, http://dx.doi.org/10.1049/iet-com.2014.0442.

[216] J. Meinilä, P. Kyösti, L. Hentilä, T. Jämsä, E. Suikkanen, E. Kunnari, M. Narandzic, D5. 3: WINNER+ Final Channel models, in: Wireless World Initiative New Radio WINNER, 2010, pp. 119–172.

[217] J. Meinilä, P. Kyösti, T. Jämsä, L. Hentilä, WINNER II Channel models, in: Radio Technologies and Concepts for IMT-Advanced, Wiley Online Library, 2009, pp. 39–92.

[218] G. T. 36.814, Evolved universal terrestrial radio access (e-UTRA); further advancements for e-UTRA physical layer aspects, 2010.

[219] M. Series, Guidelines for evaluation of radio interface technologies for IMT-advanced, Report ITU 638 (2009) 1–72.

[220] A. Al-Hourani, S. Kandeepan, S. Lardner, Optimal LAP altitude for maximum coverage, IEEE Wirel. Commun. Lett. 3 (6) (2014) 569–572, http://dx.doi.org/10.1109/LWC.2014.2342736.

[221] N. Sharma, M. Magarini, L. Dossi, L. Reggiani, R. Nebuloni, A study of channel model parameters for aerial base stations at 2.4 GHz in different environments, in: 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018, pp. 1–6, http://dx.doi.org/10.1109/CCNC.2018.8319165.

[222] 3GPP TR 38.901 V14.0.0, Study on channel model for frequencies from 0.5 to 100 GHz, 2017.

[223] 3GPP TS 36.331, Evolved universal terrestrial radio access (e-UTRA); resource control (RRC); protocol specification; version 13.0.0 release 13, 2016.

Ali Masood received his M.Sc. degree in Advanced Electronic Systems Engineering from University of Burgundy, France, in 2017. He was a Research Engineer at Inserm U1253 (Imaging and Brain), INSA Centre Val de Loire, France from March 2017 to October 2017. Currently, he is working towards his Ph.D. at Thomas Johann Seebeck Department of Electronics, School of Information Technology, Tallinn University of Technology. His domain of research is Cooperative Device to Device Communication for Emergency and Critical Wireless Communication System.

Davide Scazzoli was born in Italy, in 1989. He received a M.Sc. degree in Telecommunications Engineering in the year 2016 from Politecnico di Milano defending a thesis on the implementation of Wireless Sensor Networks for avionic applications. He is currently a Ph.D. student in the field of Telecommunications Engineering at the Politecnico di Milano. His research interests are Wireless Sensor Networks, redundancy management and localization.

Navuday Sharma received his M-Tech in avionics engineering from Institute of Space Science and Technology, Amity University, Uttar Pradesh, India, in 2015 and Ph.D. degree in telecommunication engineering from the Department of Electronics, Information and Bioengineering (DEIB), Politecnico di Milano, Italy, in 2018. He was also a Research Engineer at Infocomm Lab, School of Computer Science and Robotics, Tomsk Polytechnic University, Russia, from Oct 2017 to June 2018. Currently, he is working as a Post-Doctoral Researcher at Thomas Johann Seebeck Department of Electronics, Tallinn University of Technology, Estonia. He has worked on wireless communication with aerial base stations for 5G systems and currently working towards ultra-reliable low latency communication. His other research interests are channel modeling, multi-carrier communication, digital signal processing and internet of things.

Yannick Le Moullec received the M.Sc. (EE) degree from Université de Rennes I (France) in 1999 and the Ph.D. (EE) degree from Université de Bretagne Sud (France) in 2003. From 2003 to 2013 he successively held postdoc, assistant, and associate professor positions at Aalborg University (Denmark). He then joined Tallinn University of Technology (Estonia) as a senior researcher, where he now holds a professorship in electronics. He has supervised 11 PhD theses and 50+ M.Sc. theses. He is Co-PI for the H2020 COEL ERA-Chair project. He is a member of the IEEE Sustainable ICT Community. His research interests span HW/SW co-design, embedded systems, reconfigurable systems, and IoT.

Rizwan Ahmad received M.Sc. degree in Communication Engineering and Media Technology from the University of Stuttgart, Stuttgart, Germany in 2004 and Ph.D. degree in Electrical Engineering from Victoria University, Melbourne, Australia in 2010. From 2010 to 2012, he was a Postdoctoral Research Fellow with Qatar University on a QNRF grant. He is currently working as Assistant Professor at School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Pakistan. His research interests include medium access control protocols, spectrum and energy efficiency, energy harvesting and performance analysis for wireless communication and networks. He has published and served as a reviewer for IEEE journals and conferences. He also serves on the TPC of leading conferences in the communication and networking field, including, e.g. IEEE VTC, IEEE ICC, IEEE Globecom. He is a member of IEEE. He was the recipient of the prestigious International Postgraduate Research Scholarship from the Australian Government.

Luca Reggiani received the Ph.D. in Electronics and Communications Engineering in 2001 from Politecnico di Milano (Italy). He has collaborated with several industries and Universities in the field of wireless communications and magnetic recording, as a consultant or within Italian and European research programs. His research interests include cellular systems, wireless sensor networks, high capacity point-to-point links, information theory.

Maurizio Magarini received the M.Sc. and Ph.D. degrees in electronic engineering from the Politecnico di Milano, Milan, Italy, in 1994 and 1999, respectively. In 1994, he was granted the TELECOM Italia scholarship award for his M.Sc. Thesis. He worked as a Research Associate in the Dipartimento di Elettronica, Informazione e Bioingegneria at the Politecnico di Milano from 1999 to 2001. From 2001 to 2018, he was an Assistant Professor in Politecnico di Milano where, since June 2018, he has been an Associate Professor. From August 2008 to January 2009 he spent a sabbatical leave at Bell Labs, Alcatel-Lucent, Holmdel, NJ. His research interests are in the broad area of communication and information theory. Topics include synchronization, channel estimation, equalization and coding applied to wireless and optical communication systems. His most recent research activities have focused on molecular communications, massive MIMO, study of waveforms for 5G cellular systems, wireless sensor networks for mission critical applications, and wireless networks using UAVs and high-altitude platforms. He has authored and coauthored more than 100 journal and conference papers. He was the co-recipient of four best-paper awards. Since 2017 he has been an Associate Editor of IEEE Access and a member of the Editorial Board of Nano Communication Networks (Elsevier). In 2017 he also served as Guest Editor for IEEE Access Special Section on "Networks of Unmanned Aerial Vehicles: Wireless Communications, Applications, Control and Modelling". He has been involved in several European and National research projects.

Muhammad Mahtab Alam (M'07, SM'19) received M.Sc. degree in electrical engineering from Aalborg University, Denmark, in 2007, and Ph.D. degree in signal processing and telecommunication from the University of Rennes1 France (INRIA Research Center) in 2013. He joined Swedish College of Engineering and Technology, Pakistan, in 2013 as assistant professor. He did his postdoc research from 2014-2016 at Qatar Mobility Innovation Center, Qatar. In 2016, he joined as European Research Area Chair and Associate Professor at Thomas Johann Seebeck Department of Electronics at Tallinn University of Technology, where later in 2018 he was elected as Professor. From 2019, he is the communication systems research group leader. His research focusses on the fields of wireless communications - connectivity, NB-IoT 5G/B5G services and applications, low-power wearable networks for SmartHealth. He has15+ years of combined academic and industrial multinational experiences while working in Denmark, Belgium, France, Qatar and Estonia. He has several leading roles as PI in multimillion Euros international projects funded by European Commission (H2020-ICT-2019-3, "951867", NATO-SPS (G5482), Estonian Research Council (PRG424), Telia industrial grant. He is author and co-author of more than 80 research publications. He is actively supervising a number of PhD and postdoc researchers. He is also a contributor in two standardization bodies (ETSI SmartBAN, IEEE-GeeenICT-EECH), including "Rapporteur" of work item: DTR/SmartBAN-0014, "Applying SmartBAN MAC (TS 103 325) for various use cases". He is associate editor of the IEEE Access journal.