This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges

Mahmoud Elsaadany, *Student Member, IEEE*, Abdelmohsen Ali, *Student Member, IEEE* and Walaa Hamouda, *Senior Member, IEEE*

***Abstract*—Human-generated information has been the main interest of the wireless communication technologies designs for decades. However, we are currently witnessing the emerge of an entirely different paradigm of communication introduced by machines, and hence the name Machine Type Communication (MTC). Such paradigm arises as a result of the new applications included in the Interne-of-Things (IoT) framework. Among the enabling technologies of the IoT, Cellular-based communication is the most promising and more efficient. This is justified by the currently well-developed and mature radio access networks, along with the large capacities and flexibility of the offered data rates to support a large variety of applications. On the other hand, several radio-access-network groups put efforts to optimize the 3GPP LTE standard to accommodate for the new challenges by introducing new communication categories paving the way to support the machine-to-machine communication within the IoT framework. In this paper, we provide a step-by-step tutorial discussing the development of MTC design across different releases of LTE and the newly introduced user equipment categories namely: MTC Category (CAT-M) and Narrowband IoT Category (CAT-N). We start by briefly discussing the different physical channels of the legacy LTE. Then we provide a comprehensive and up-to-date background for the most recent standard activities to specify CAT-M and CAT-N technologies. We also emphasize on some of necessary concepts used in the new specifications, such as the narrowband concept used in CAT-M and the frequency hopping. Finally, we identify and discuss some of the open research challenges related to the implementation of the new technologies in real life scenarios.**

***Index Terms*—IoT, M2M, MTC, Legacy LTE, CAT-M, CAT-N, LTE-A specifications, Narrowband concept, Frequency re-tuning, Repetitions transmission, Enhanced coverage, Low cost, Low power.**

I. Introduction

The Internet technology has undergone enormous changes since its early stages and it has become an important communication infrastructure targeting anywhere, anytime connectivity. Historically, human-to-human (H2H) communication, mainly voice communication, has been the center of importance. Therefore, the current network protocols and infrastructure are optimized for human-oriented traffic characteristics. Lately, an entirely different paradigm of communication has emerged with the inclusion of "machines" in the communications landscape. The exchange of any machine-generated traffic is known as Machine-to-Machine (M2M) communication [1]. As a result, the speculations about the number of devices expected to access the Internet in the near future is increasing every day. This is indeed supported by the Internet-of-Things (IoT) framework being promoted to allow a tremendous number of "Things" to generate and communicate information among each other without the need of human interaction [2]. The term "Things" can be used to refer to human services, machineries (or parts of machines), sensors in smart grids, monitoring devices in e-Health applications, smart motors/cars or any house hold device in a smart home or a smart city [3][4].

In terms of M2M communications and IoT features, a new paradigm of networks has to respect the requirements of machines, such as power and cost [5]. For instance, a set-and-forget type of application in M2M devices, such as smart meters, require very long battery life where the device has to operate in an ultra low-power mode [6]. Moreover, the future network should allow for low complex and low data rate communication technologies which provide low cost devices that encourages the large scale of the IoT. The network architecture, therefore, needs to be flexible enough to provide these requirements and more.

In this regard, a considerable amount of research has been directed towards available network technologies such as ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), or WiFi (IEEE 802.11b) by interconnecting devices in a form of large heterogeneous network [7][8]. Furthermore, solutions for the heterogeneous network architecture (connections, routing, congestion control, energy-efficient transmission, etc.) have been presented to suit the new requirements of M2M communications. However, it is still not clear whether these sophisticated solutions can be applied to M2M communications due to constraints on the hardware complexity, coverage, and coordination. Indeed, while WiFi, Bluetooth and ZigBee are widely used nowadays for -more or less- similar applications as M2M communication, the coverage range of these technologies is very short [9][10]. Also, operation on unlicensed spectrum forces such technologies to adopt spectrum sensing techniques (listen-before-talk) and may force a restriction on the transmission duty cycle. Although these reasons do not kill the chances of local area network (LAN) technologies to enable the IoT and MTC frameworks, it would urge the need for a unified standard (or at least coordination and organization mechanisms) to serve the needs of M2M and IoT [11]. On the other hand, Low Power Wide Area (LPWA) networks present a good candidate to support the aforementioned diverse require-

The authors are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, H3G 1M8, Canada (e-mail:(m_elsaad, ali_abde, hamouda)@ece.concordia.ca).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

ments of the IoT framework [12][13][14]. A variety of LPWA technology candidates can overcome the short range constraint of the LAN and still satisfy the power and latency constraints using either proprietor or cellular technologies (using licensed or unlicensed spectrum). It seems more efficient to take advantage of the currently well developed and mature radio access networks. With the large coverage and flexible data rates offered by cellular systems, research efforts from industry have recently been focused on optimizing the existing cellular networks considering M2M specifications [15]. Among the possible solutions, the famous proprietary technologies: Sigfox [16] and LoRa [17], along with the new developments of the current cellular technologies such as the new categories of LTE-A user equipments are considered.

A. Unlicensed Technologies

1) Sigfox: Sigfox is a French company works with network operators to offer an end-to-end LPWA connectivity solution based on its patented technologies. Sigfox Network Operators deploy the proprietary base stations equipped with cognitive software defined radios to operate as a secondary system (unlicensed), and connect them to the back-end servers using an IP-based network. The connectivity to the base station is simplified and uses only Binary Phase Shift Keying (BPSK) modulation in an ultra narrow bandwidth (100Hz) in the 868 MHz or 915 MHz ISM band. This way, Sigfox utilizes bandwidth efficiently and promises ultra-low power consumption, and inexpensive RF chain designs. However, Sigfox offers a throughput of only 100bps rendering it a candidate for low traffic applications. Further, a Sigfox downlink communication can only precede uplink communication after which the end device should wait to listen for a response from the base station. The number and size of messages over the uplink are limited to 140 12-byte messages per day to conform to the regional regulations on use of license-free spectrum.

2) LoRa/LORAWAN: A special interest group constituted from several commercial and industrial partners known as LoRa™ Alliance proposed LoRaWAN, as an open standard defining the network architecture and layers above the LoRa physical layer. LoRa (short for Long Range), originally developed and commercialized by Semtech Corporation [18], is a physical layer technology that modulates the signals in SUB-GHz ISM band. Using chirp spread spectrum (CSS) technique, a narrow band input signal spread over a wider channel bandwidth. The resulting signal has noise like properties, making it harder to detect or jam and hence, at the receiver, the signal enjoys an increased resilience to interference and noise. LoRa supports multiple spreading factors (between 7-12) to decide the tradeoff between range and data rate. Higher spreading factors deliver long range at an expense of lower data rates. Also the combination of Forward Error Correction (FEC) with the spread spectrum technique to further increase the receiver sensitivity. The data rate ranges from 300bps to 37.5kbps depending on spreading factor and channel bandwidth. Further, multiple transmissions using different spreading factors can be received simultaneously by a LoRa base station. The messages transmitted from end devices are received by multiple base stations, giving rise to “star-of-stars" topology, and hence improves the probability of successfully received messages. However, this increases the overhead of the network side as the resulting duplicate receptions are filtered out in the back-end. Some studies reported the performance of LoRa for outdoor [19][20][21] and [22] for indoor settings.

3) INGENU RPMA: Unlike LoRa and Sigfox, INGENU (also known as On-Ramp Wireless) is a proprietary LPWA technology that operates in 2.4 GHz ISM band and takes advantage of more relaxed regulations on the unlicensed spectrum use across different regions [23]. INGENU leads efforts to standardize the physical layer specifications under IEEE 802.15.4k standard [24]. INGENU uses a patented physical access scheme named as Random Phase Multiple Access (RPMA) [25] Direct Sequence Spread Spectrum, which it employs for uplink communication only. Using CDMA, RPMA enables multiple transmitters to share a single time slot. However, RPMA increases the duration of time slot of traditional CDMA and then distributes the channel access within this slot by adding a random offset delay for each transmitter. By asynchronous access grants, RPMA reduces overlapping between transmitted signals and thus increases signal to interference ratio for each individual link [26]. INGENU provides bidirectional communication, although with a slight link asymmetry. For downlink communication, base stations spread the signals for individual end devices and then broadcast them using CDMA. Further, the end devices can adjust their transmit power for reaching closest base station and limiting interference to nearby devices.

B. Licensed Technologies

Among other solutions, scenarios defined by the 3rd Generation Partnership Project (3GPP) standardization body emerge as the most promising solutions to enable wireless infrastructure of M2M communications [27]. Due to the M2M communication challenges and the wide range of supported device specifications, developing the features for M2M communication, also refers to machine-type-communication (MTC) in the context of Long Term Evolution (LTE), started as early as release 10 (R10) for the advanced LTE standard [28]. From the history of M2M communication (in the LTE convention) development, the first generation of a complete feature MTC device has emerged in R12. In this release, R12, the 3GPP committee has defined a new profile referred to as category 0 or CAT-0 for low-cost MTC operation [29]. Also a full coverage improvement is guaranteed for all LTE duplex modes. Indeed, the effort continued to future releases including release 13 (R13) that was released late in 2016. In this front, two special categories, namely CAT-M for MTC and CAT-N for Narrowband-IoT (NB-IoT), have been incorporated by the 3GPP to LTE specifications to support complete M2M and IoT features, respectively. The new categories satisfy the general requirements of MTC and can support the wide range of IoT applications. For example, the capabilities of the new categories can support applications in the domain of fleet management and logistics, which require secured, wide range, real time and accurate information with typical data rate of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

hundreds of Kbps at speeds ranging from 10 to 150 Km/h. On the other hand, they can also support applications with very low moving speeds (or stationary) and moderate data rates with hours of latency , such as, automation and monitoring applications.

Several working groups in radio-access-networks (RAN) contribute very actively to the work on MTC and IoT-related optimization for 3GPP LTE networks. From day one, the support for MTC was one of the major concerns for the 3GPP and the development for a robust MTC design was divided across different releases [30]. Since LTE has the ability to support high performance, high throughput devices, the objective was to develop high volume, low cost, low complexity, and low throughput User Equipment (UE) LTE-based MTC devices. This rapid change in the standard spirit causes considerable amount of updates to all protocol stack layers including Radio Resource Control (RRC) layer, Medium Access Control (MAC) layer, and physical layer [31]. However, the updates to RRC are quite thin when compared to the significant amount of changes required for the physical layer [15]. The reason is that MTC/IoT features are more related to the implementation side of the device rather than the procedures for communications. For example, one of the mandatory features for CAT-N is to be flexible in deployment such that it can be deployed in-band or in the guard band of an LTE carrier, or in the extreme case to be stand-alone system. These requirements put restrictions on the physical layer design so that the final NB-IoT system looks like a new system independent of the legacy LTE system. As a matter of fact, the legacy LTE system provides definition to Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. However, based on the current network deployments, it is a fact that a large scale of the deployments employ FDD rather than TDD. Indeed, it is China which launches TDD networking early in 2009 [32]. For this reason, CAT-N has been defined only for FDD as long as R13 is concerned. Motivated by this discussion, in this tutorial, we present a comprehensive background about the legacy LTE and the introduced updates to support CAT-M and CAT-N technologies [33]. Due to its importance, the standard view will be mainly from the physical layer perspective focusing on FDD mode.

C. Motivation

LTE-MTC standards-based family of technologies supports several technology categories, such as CAT-0 and CAT-M [34]. CAT-0 category is now fully commercial and it is already used in many M2M/IoT deployments. The new CAT-M category is a low power wide area technology, which supports IoT through lower device complexity and provides extended coverage, while allowing the reuse of the LTE installed base [6]. CAT-M allows an extended battery lifetime for a wide range of use cases, with the modem costs reduced to 20-25% of the current Enhanced General Packet Radio Service (EGPRS) modems [28]. Supported by all major mobile equipment, chip set and module manufacturers, LTE-MTC networks will co-exist with 2G, 3G, and 4G mobile networks and benefit from all the security and privacy mobile network features, such as support for user identity confidentiality, entity authentication, confidentiality, data integrity, and mobile equipment identification. Commercial launches of LTE-MTC networks is expected to take place in 2017. Unlike LTE-MTC, NB-IoT systems can be deployed as stand-alone systems or can be adopted to the LTE guard band. With its reduced bandwidth of only 180KHz, low data rate devices can leverage the extended coverage, reduced complexity, and reduced power consumption by employing NB-IoT systems [33]. Indeed, NB-IoT is assumed to be the gate for the future cellular IoT devices that has out-of-reach issues, while seldom exchanging data with the network.

Since the introduction of LTE-A, researchers invested their effort in addressing various challenges to realize these systems and studying the issues that may appear from implementation perspectives. In fact, a countable number of survey papers exist in the literature in the context of legacy LTE covering a wide range of areas such as physical layer resiliency for LTE as an OFDM-based system [35], resource allocation [36], emerging applications for LTE in vehicular networks [37], uplink random access techniques [38], scheduling techniques for uplink and downlink streams [39][40], control channel evolution in LTE systems [34], and M2M based on LTE systems [15][38][41]. However, with the introduction of CAT-M and CAT-N LTE technologies, it is important to provide a detailed background about the new features and solutions. Investigation of realistic solutions towards combating various practical system implementations has become critical towards the actual system deployment. Hence to the best of our knowledge, a comprehensive tutorial on MTC and NB-IoT communications with its focus on LTE systems is not available in the literature. Therefore, the main purpose of this paper is to provide a review on the studies appeared in the standard agreements, helping the readers to understand what has been investigated (architecture, technologies, requirements, challenges, and proposed solutions) and what still remains to be addressed as implementation challenges. In addition, this paper will reveal an evolutionary path of the LTE-MTC and NB-IoT systems for futuristic research. For instance, open research topics, targeting the efficient algorithmic solutions for initial synchronization, cell search, frequency tracking, and channel estimation, have been considered. Furthermore, highlighting the potential implementation aspects for reduced cost and power consumption requirements are assumed.

D. Contributions

In this paper, in addition to the brief introduction to the legacy LTE, we provide a comprehensive and up-to-date background for the most recent standard activities to specify CAT-M and CAT-N technologies. We also identify and discuss some of the key open research challenges related to the implementation side of such technologies. Our main contributions can be summarized as follow:

- The development cycle of the LTE standard is discussed to show the motivation for the new categories based on the growing features. The target requirements for MTC and IoT categories are presented, compared, and analysed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

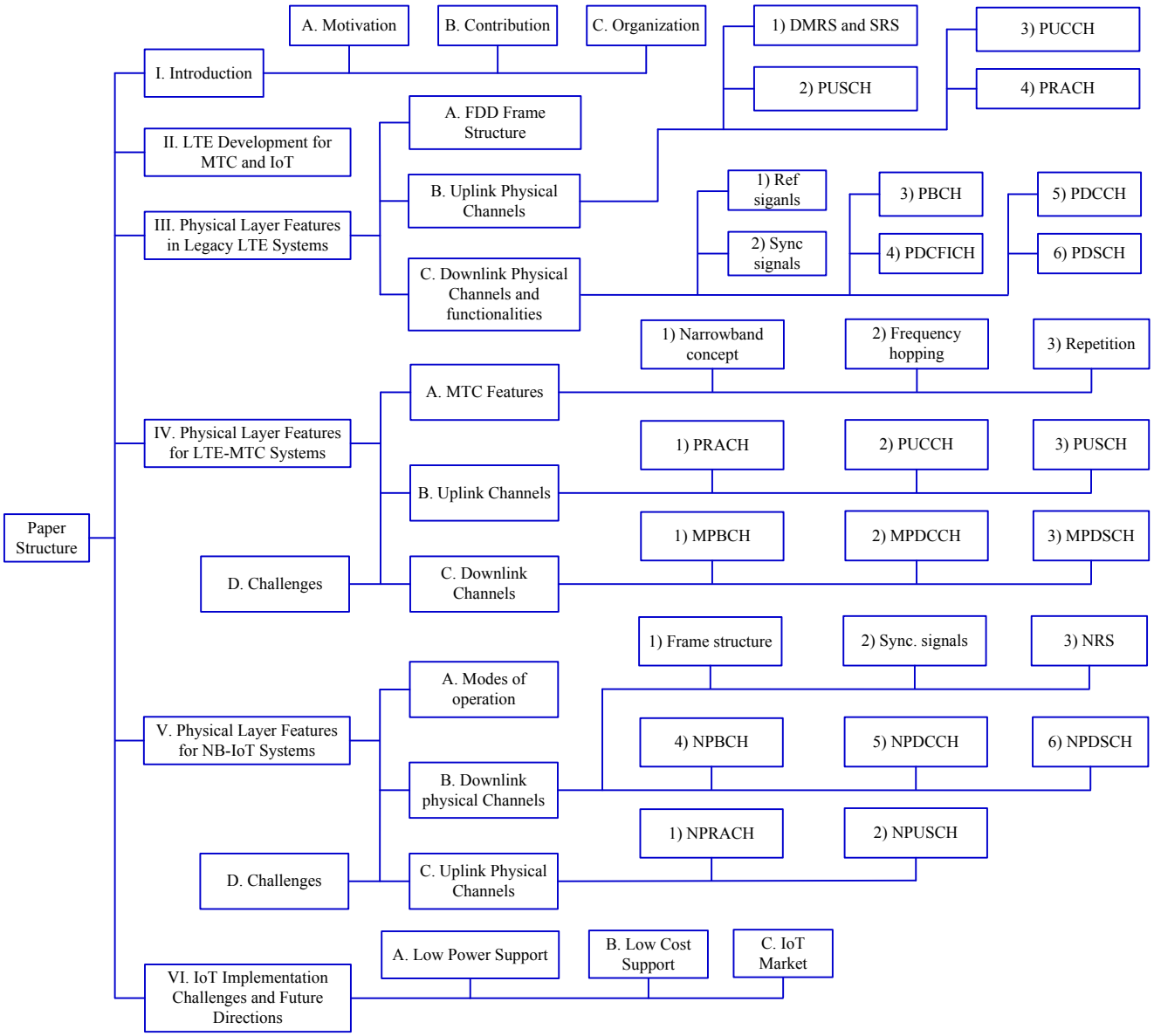

Fig. 1. Chart for the paper structure.

- An introduction to the conventional LTE system is presented. The objective of this overview is to familiarize the reader with the basic features and concepts for the legacy LTE-A. The system structure is discussed with the definition of various physical channels for both uplink an downlink sides in FDD mode. In this regard, the frame structure, uplink physical channels, and downlink physical channels are reviewed. The functionalities and brief description about the operation are assumed for each physical channel.
- The specifications for the LTE-MTC system are considered with reasonable explanations for the decisions and alternatives. The potential updates including the narrowband concept, the new introduced downlink control channel, repetitions, and frequency hopping are discussed in details. Also, the implementation challenges brought by these specification are classified and discussed.
- Since NB-IoT system is the most recent technology adopted to LTE, the system is described from scratch. The modes of operation are classified and studied. The most recent agreements about CAT-N according to R13 are considered. In the downlink side, the new synchronization signals and reference signals are discussed in addition to the conventional data and control channels. In the uplink direction, the full system is presented with enough details for fair comparison with other systems. Logical reasoning is followed to criticize the decisions for various channel designs. The implementation challenges are then discussed so that researchers are encouraged to address these potential issues.
- IoT general challenges and future directions are captured. Low power consumption and reduced complexity are highlighted in regards to the LTE-MTC and NB-IoT systems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Table I
DEFINITIONS OF ACRONYMS AND NOTATIONS

Acronym	Definition	Acronym	Definition
3GPP	Third Generation Partnership Project	NCCE	Narrowband Control Channel Elements
ADC	Analog-to-digital conversion	NPRACH	Narrowband Physical Random Access Channel
AWGN	Additive White Gaussian Noise	NPSS	Narrowband Primary Synchronization Signal
BLER	Block Error Rate	NPUSCH	Narrowband Physical Uplink Shared Channel
CCE	Control channel elements	NSSS	Narrowband Secondary Synchronization Signal
CFO	Carrier frequency offset	PAPR	Peak to Average Power Ratio
CQI	Channel Quality Indicator	PBCH	Physical Downlink Broadcast Channel
CRC	Cyclic Redundancy Check	PDCCH	Physical Downlink Control Channel
CRS	Cell-Specific Reference Signals	PDCFICH	Physical Downlink Control Format Indicator Channel
CSI	Channel State Information	PDSCH	Physical Downlink Shared Channel
CSS	Common Search Space	PHY	Physical Layer
DAC	Digital-to-analog conversion	PMI	Precoding Matrix Information
DCI	Downlink Control Information	PRACH	Physical Random Access Channel
DCI	Downlink Control Information	PRB	physical resource block
DMRS	Demodulation Reference Signals	PSS	Primary Synchronization Signal
DRX	Discontinuous reception	PUCCH	Physical Uplink Control Channel
ECCE	Enhanced control channel elements	PUSCH	Physical Uplink Shared Channel
EGPRS	Enhanced General Packet Radio Service	RAN	Radio-access-networks
EPDCCH	Enhanced physical downlink control channel	RAR	Random access response
FDD	Frequency Division Duplex	RE	Resource elements
H2H	Human-to-human	REG	Resource element group
HARQ	Hybrid Automatic Repeat Request	RI	Rank Indication
IEEE	Institute of Electrical and Electronics Engineers	RLC	Radio link control
LAN	Local Area Network	RNTI	Radio Network Temporary Identifier
IoT	Internet-of-Things	RRC	Radio Resource Control
LTE	Long Term Evolution	RSRP	Reference Signal Received Power
LPWA	Low Power Wide Area	SFBC	Space Frequency Block Coding
M2M	Machine-to-Machine	SRS	Sounding Reference Signal
MAC	Medium Access Control	SSS	Secondary Synchronization Signal
MCL	Mutual Coupling Loss	TDD	Time Division Duplex
MIMO	Multiple-Input Multiple-Output	ToA	Time of Arrival
MPDCCH	MTC Physical Downlink Control Channel	UCI	Uplink control information
MTC	Machine Type Communication	UE	User Equipment
NB	Narrowband	USS	User Specific Search Space

E. Organization

The paper is organized as follows. Section II introduces the development cycle of the LTE standard to provide the fundamental targets for both LTE-MTC and NB-IoT categories. A summary of the main physical layer features of various MTC/IoT categories is introduced to highlight the main differences. Based on the presented category classification, the legacy LTE fundamentals are presented in Section III. In addition to the general features, both uplink and downlink physical channels are discussed in Sections III-B and III-C, respectively. The second item in this classification is the LTE-MTC development which is considered in Section IV. The most important features for LTE-MTC are presented in Sections IV-A. Again, the uplink and downlink physical channels are investigated and the main differences are highlighted when compared to the legacy LTE system.

The up-to-date agreements about the NB-IoT system including the modes of operations, the uplink physical channels, and downlink physical channels are considered in Section V. The definitions of the main concepts for this category are not only presented but the main differences among various categories are assumed as well. In Sections VI-C, the implementation challenges are demonstrated for the NB-IoT system. It is of great interest that low power and low complexity requirements are potential aspects for the cellular based IoT network. The advances to these requirements in the scope of LTE-MTC and NB-IoT systems are also provided in Section VI-C. Finally, conclusions are drawn in Section VIII. The overall structure of the paper is shown in Fig. 1, and Table I lists the acronyms and notations used in the paper.

II. LTE DEVELOPMENT FOR MTC AND IOT

Although data transmission has been on the rise in the cellular networks for human-involved applications in the last decade, cellular networks are mainly optimized for H2H communication. However, characteristics of M2M traffic are different from the human-generated traffic in the cellular

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

networks. The main differences between H2H and M2M traffic can be expressed as [42][43]:

- In contrast to human-traffic, in M2M devices, the uplink traffic is higher than downlink.
- While human-traffic is mostly concentrated during daylight and evening, M2M traffic is more uniformly generated by the M2M devices throughout the day.
- In some applications (e.g., involving metering devices), M2M traffic is periodic.
- In some monitoring applications, the volume of traffic increases sharply after the detection of events (burst traffic).
- For many classes of M2M devices, M2M devices have a much lower mobility than human devices. However, for the health care devices, and for accessories such as Google glass and Apple watch, the mobility is the same as the human devices.
- The quality-of-service requirements of M2M and human devices may be vastly different.

While an M2M device typically sends/receives a small packet of data at each transmission, the extremely large number of M2M devices may cause severe problems in both access channel and traffic channel of a radio access network and congestion in the core network [44][45]. For these reasons, from the network access perspective, M2M access requests are classified by 3GPP into two groups of uncoordinated/non-synchronized and coordinated/synchronized traffic [46]. Coordinated/synchronized traffic is a type of traffic generated by many similar M2M devices in reaction to an event, whereas uncoordinated/non-synchronized traffic is a result of independent reporting of data. Accordingly, the medium access for M2M devices would require a special attention and hence the medium access techniques have to be revised to address such challenges . For instance, the access channel overhead has been carefully investigated where many approaches, including the classical Back-off techniques, the access class barring scheme, slotted access, and others, are assumed [47]. The reader is encouraged to refer to [48][49][50] [51] for more details about the higher layer challenges and solution for M2M devices from 3GPP perspective.

From the physical layer perspective, the 3GPP standardization community has provisioned suitability of LTE to allow MTC communication and connectivity over LTE network. A lot of studies have been conducted to optimize the radio access related technologies and mechanisms. The main task of this effort was to:

- Improve the support of low-cost and low-complexity device types to match low performance requirements (low data rates and delay tolerance) of certain MTC applications.
- Provide extended coverage for MTC devices in challenging locations.
- Prolong long battery life of the UEs by enabling very low energy consumptions.
- Optimize signalling of small data transmission to increase the cell/network capacity to serve very large numbers of devices.

The 3GPP enhancement for LTE to accommodate the requirements of MTC and IoT are summarized next:

A. CAT-0 in Release-12

Although Category 1 (CAT-1) was the lowest among all LTE UE categories in R11 in terms of transmission capability (10 Mbps peak downlink transmission rate and 5 Mbps for the uplink), it was concluded that a new category will be needed to support the new requirements of MTC and IoT. Category 0 is the new standardized category for this purpose in R12. CAT-0 UEs have a reduced transmission rate of 1 Mbps peak rates for both uplink and downlink. CAT-0 UEs enjoy a reduced complexity by up to 50% compared to CAT-1. The new features of the new category include the use of only one receiver antenna with a maximum receive bandwidth of 20 MHz, which eliminates the use of dual receiver chains. Also the support of FDD half-duplex operation with relaxed switching time eliminating the need for duplex filters, which help the manufacturers to significantly reduce the modem cost compared to more advanced UE categories.

B. CAT-M or LTE-MTC in Release-13

For further complexity reduction techniques, on top of the ones introduced for CAT-0, a new category, namely Category MTC (CAT-M), is proposed in the recent work of R13 [52]. The aim of the LTE-MTC (CAT-M) Task Force was to provide a market representation to accelerate the wide-spread adoption of 3GPP-based LTE-MTC technology. LTE-MTC is addressing the low-power wide-area IoT market opportunity using licensed spectrum with the intent to launch commercial solutions 2017. The main objectives of the LTE-MTC (CAT-M) are:

- Facilitate demonstrations and proof of concept trials which strengthen the LTE-MTC solution to meet the low power requirements.
- Lead industry partners to build a strong end-to-end industry chain for LTE-MTC growth, development and deployment.
- Further reduction in complexity of LTE-MTC devices.

Recent studies indicate that CAT-M features a complexity reductions up to 75-80$\%$ compared to CAT-1. The most important additional feature is the possibility to implement the UE transmitter and receiver parts with reduced bandwidth compared to legacy LTE UEs operating with 20 MHz bandwidth. specifically, a CAT-M UE will operate with a maximum channel bandwidth limited to 1.4 MHz. Another differentiating feature in CAT-M is the coverage enhancements of more than 15 dB (i.e. the received SNR $\approx$ - 15 dB), enabling the reach the UEs behind the thickest walls or under the ground.

C. CAT-N or NB-IoT LTE in Release-13

Since the core IoT devices or massive MTC devices typically send small amounts of data and require extended coverage, a special category, namely NB-IoT, has been incorporated to LTE specifications to support IoT features [53]. The design targets for this special category require reduced

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Table II
SUMMARY OF THE BASIC REQUIREMENTS FOR CAT-0, CAT-M, AND CAT-N SYSTEMS

Specification	R12 CAT-0	R13 CAT-M	R13 CAT-N
Downlink peak rate (Mbps)	1	1	0.2
Uplink peak rate (Mbps)	1	1	0.144
Number of UE receive antennas	1	1	1
Duplex mode	Half duplex	Half duplex	Half duplex
UE receive Bandwidth (MHz)	20	1.4	0.2
Maximum UE Transmit power (dBm)	23	23	20

complexity, promote battery longevity, and enhanced coverage. Furthermore, the need to support high data rates seldom applies to massive MTC. The link budget of NB-IoT has a 20dB improvement over conventional LTE-A [54]. These requirements have been realized by utilizing a single receive antenna system, supporting only QPSK modulation in the downlink side, and employing extended discontinuous reception cycles to reduce the power consumption in deep sleep modes. Moreover, signal repetition is considered as the key factor to provide performance gain [55].

A summary of the main physical layer features of varies LTE developments is presented in Table II. Furthermore, the main features for various physical layer channels included in different technologies are summarized in Table III and Table IV. The objective of these tables is to list the main differences between different technologies which will be addressed in the rest of this manuscript.

III. PHYSICAL LAYER FEATURES IN LEGACY LTE SYSTEMS

Among the objectives of the LTE standard is to create a more efficient and streamlined protocol stack and architecture. Many dedicated channels specified in previous 3GPP standards have been replaced by shared channels and the total number of physical channels has been reduced. Logical channels represent the data transfers and connections between the radio link control (RLC) layer and the MAC layer. In LTE, two types of logical channel are defined: the traffic channels and the control channels. While the traffic logical channel is used to transfer the data of users, the control logical channels, communicate the necessary signalling to sustain the connectivity.

Transport channels connect the MAC layer to the physical layer, and the physical channels are processed by the transceiver at the physical layer. Each physical channel is mapped on the resource grid to a set of resource elements (REs) that carry information from higher layers of the protocol stack for eventual transmission on the air interface.

The most important transport channel types are the downlink shared channel and uplink shared channel, which are used for data transmission in the downlink and uplink respectively. A physical channel carries the time-frequency resources used for transmission of a particular transport channel. Each transport channel is mapped to a corresponding physical channel. In addition to the physical channels with corresponding transport channels, there are also physical channels without corresponding transport channels. These channels, known as L1/L2 control channels, are used for downlink control information (DCI), providing the terminal with the information required for proper reception and decoding of the downlink data transmission. As for uplink control information (UCI), they are used to provide the scheduler and the Hybrid Automatic Repeat Request (HARQ) protocol with information about the situation at the terminal. The relationship between the logical channels, transport channels, and physical channels in LTE differs in downlink versus uplink transmissions. Next, we will describe -in some details- various physical channels used in the uplink and downlink as well as some of the important signalling used within each of them.

A. FDD Frame Structure

For the LTE to feature a high spectrum flexibility, the frequency spectra are formed as concatenation of physical resource blocks (PRBs) each consists of 12 subcarriers. Subcarriers are separated by 15 KHz, hence, the total bandwidth of PRB is 180 KHz. This enables configurations for transmission bandwidth form 1.4 MHz with 6 PRBs to a maximum bandwidth of 20 MHz consisting of 110 PRBs. The available channel bandwidths are (1.4. 3, 5, 10, 15, 20 MHz), with transmission bandwidth occupies 90% of all channels, expect for the 1.4 MHz channel which has only 77% efficiency. The rest of the channel bandwidth is used as a guard band to reduce the unwanted emissions outside the neighbouring bands.

LTE specifies two downlink frame structures. A type 1 frame applies to an FDD deployment and a type 2 frame is used for a TDD deployment. Each frame is composed of 10 subframes and each subframe consists of two time slots. Each time slot is 0.5 msec, thus a radio frame is 10 msec. The three components of a resource grid are used for, user data, control channels, and reference and synchronization signals.

Figure 2 shows FDD downlink radio frame structure. The duration of each frame is 10ms, composed of ten 1 ms subframes denoted by indices ranging from 0 to 9. Each subframe is subdivided into two slots of 0.5ms duration. Each slot is composed of seven or six OFDM, depending on whether a normal or an extended cyclic prefix is used. The DCI is placed within the first slot of each subframe. The DCI carries the content of the PDCCH, PCFICH, and PHICH, and together they occupy up to the first three OFDM symbols in each subframe. The PBCH containing the MIB is located within subframe 0 and the PSS and SSS are located within subframes 0 and 5. The uplink subframe structure is similar to the downlink frame. It is composed of 1ms subframes divided into two 0.5 ms slots. Each slot is composed of either seven or six single carrier frequency division multiplexing (SC-FDM) symbols, depending on whether a normal or an extended cyclic prefix is used. The inner-band (towards the center) resource blocks are reserved for data resource elements (PUSCH) in order to reduce out-of-band emissions, while

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Table III
SUMMARY FOR THE SUPPORTED FEATURES AND FUNCTIONALITIES FOR VARIOUS DOWNLINK PHYSICAL CHANNELS FOR LEGACY LTE, CAT-M, AND CAT-N DEVICES.

Channel	Legacy LTE	LTE CAT-M	LTE CAT-N
Sync. Signals	- PSS and SSS signals - Used for cell differentiation and frame timing acquisition - Also, used for initial synchronization - Sent periodically every 5 msec - Span the central 72 subcarriers - PSS is Zadoff-Chu sequence - SSS is a concatenated binary m-sequence	- Same as legacy	- NPSS and NSSS signals - NPSS is used for timing acquisition and Initial synchronization - NSSS carries the cell information - Each spans a complete subframe - Each has a periodicity of 10msec - Generation for both sequences is based on Zadoff-Chu sequence
Cell-Specific Reference Signals	- A pseudo random sequence with cell specific initializations used. - The sequence is modulated through QPSK - The mapping is a function of the cell ID and the CP type - Used to assist channel estimation for coherent detection - Also, used for channel quality indication - Time-frequency orthogonal mapping is utilized for different antenna ports	- Same as legacy	Same as legacy with the exceptions: - The mapping process uses different OFDM symbols when compared to legacy - Only two antenna ports are supported
Physical Broadcast Channel	- Carries Master information block which has the essential cell parameters such as the bandwidth and frame timing. - it is always allocated in the central 72 subcarriers - Uses QPSK as the basic modulation - The message is segmented over four data chunks, each is carried in a separate radio frame. - Blind decode is essential to determine: the radio frame numbering and the number of Tx antennas.	- Same as legacy with the addition that repetition is possible to enable coverage enhancement and frequency tracking under low SNR regimes.	- A new channel is defined - The master information block contents has been updated - The message size has been reduced to 1600 bits instead of 1920 bits - The message is segmented into 8 segments where each segment is identically repeated 8 times. - Each repetition is carried over a complete subframe with a periodicity of one complete radio frame.
Physical Control Channel	- Used to carry the Downlink Control Information (DCI) - Also, used to define the paging opportunities - Different formats are defined for different DCI messages. - Mapped to the first couple of OFDM symbols in a subframe. - Aggregation is defined to reduce the coding rate - Uses QPSK modulation - Uses convolutional codes - Message is scrambled by the user identity - Blind decode is required for the UE to extract the control information, if any. - Search spaces are defined to enable UE better allocates its DCI	- A new channel, namely MPDCCH, is defined - New search spaces are defined with reduced blind decode capabilities (up to 20 candidates) - New formats are defined to carry a new set of DCIs - Repetition is supported to enhance the decoding - Frequency hopping is supported - Mapping spans the whole OFDM symbols per PRB - Aggregation levels up to 24 control elements can be used - Localized and distributed mapping are supported - Control DCI is meant for future downlink assignment	- A new channel, namely NPDCCH, is defined - Only up to four candidates are required for blind decode - New formats are defined to carry a new set of DCIs - Repetition is supported to enhance the decoding - Mapping spans the whole OFDM symbols per PRB - Aggregation levels of up to two control elements can be used
Physical Shared Channel	- Carries physical data with high data rates - Uses Turbo coding - Higher order modulation up to 256 QAM is supported - Transmit diversity and spatial multiplexing are required	Same as legacy with the following exceptions: - Modulation orders of only QPSK and 16-QAM are supported - A maximum transport block size of 1Kb is required - Repetition is supported - Frequency hopping is supported	- A new channel, namely NPDSCH, is defined - Convolutional coding is used - Only QPSK is supported - A maximum transport block size of 680bits is required. - Fragmentation is applied - Repetition is supported

edges are reserved as a control region. The reference signals necessary for data demodulation are interspersed throughout the data and control channels.

B. Uplink Physical Channels

LTE has three uplink physical channels namely, the Physical Uplink Shared Channel (PUSCH), Physical Uplink Control Channel (PUCCH), and Physical Random Access Channel (PRACH). The PUSCH carries the user data transmitted from the user terminal. while the PRACH is used for initial access

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Table IV
SUMMARY FOR THE SUPPORTED FEATURES AND FUNCTIONALITIES FOR VARIOUS UPLINK PHYSICAL CHANNELS FOR LEGACY LTE, CAT-M, AND CAT-N DEVICES.

Channel	Legacy LTE	LTE CAT-M	LTE CAT-N
Demodulation Reference Signals	- Used for channel estimation by the eNodeB- Sent over complete OFDM symbols every slot - Zadoff-Chu sequences are utilized for the generation - Applied with different density for data and control channels	- Same as legacy but only for 1.4MHz	- Definition differs from single-tone operation to multi-tone operation - Multi-tone operation utilizes the legacy Zadoff-Chu sequences with an introduced frequency shift.
Random Access Channel	- Used to send the preamble sequence during the initial call setup - Occupies only 1.4MHz - Different preamble configurations are supported - Preamble sequence is based on Zadoff-Chu generation - Different cyclic shifts are defined to reduce the collision possibilities. - Different preamble formats are supported to mitigate various channel conditions	Same as legacy with the following additions: - Repetition is allowed - Repetition is a function of the CE level - Frequency hopping is mandatory	- A new channel is defined, namely NPRACH - To increase the coverage distance, a single tone sequence is required with a new defined subcarrier spacing of 3.75KHz - Preamble is sent in a form of symbol group - Frequency hopping is mandatory within the preamble group - Repetition is supported
Physical Control Channel	- Carries the uplink control information - Different uplink formats (1 to 5) are defined to carry uplink data including CQI, PMI, RI, and uplink scheduling requests. - Uses Zadoff-Chu sequence modulation to transmit the payload - Mapped to two PRBs at the band edges	Same as legacy with the following exceptions: - Format 1/1A and 2/2A are the only supported formats - ACK/NACK and CQI are the only possible paylaods - Frequency hopping is required between the two RBs at the band edges - Repetition is supported	There is no dedicated control channel defined
Physical Shared Channel	- Carries the uplink paylaod in addition to control information in a piggyback fashion, if required. - Utilizes SC-FDMA transmission - Uses QPSK, 16-QAM, or 64QAM for modulation - Employs Turbo encoding	- Same as legacy with the following exceptions: - Only QPSK and 16-QAM are supported - Repetition is required - Frequency hopping is mandatory	- A new channel is defined, namely NPUSCH - NPUSCH has two formats: one for control and one for data transmission - Only ACK/NACK is assumed for control transmission - NPUSCH can be sent over either single tone or multi-tone - Packet segmentation is required - Turbo coding is assumed - Repetition is mandatory - Only BPSK and QPSK are supported - Rotated constellation is achieved through signal generation

of a UE to the network through transmission of random access preambles. The PUCCH carries the UCI, including scheduling requests, acknowledgments of transmission success or failure (ACKs/NACKs), and reports of downlink channel measurements including the channel quality Indicator (CQI), Precoding Matrix Information (PMI), and Rank Indication (RI). There are two types of uplink reference signals in the LTE standard: the Demodulation Reference Signals (DMRS) and the Sounding Reference Signal (SRS). Both uplink reference signals are based on Zadoff-Chu sequences [56].

Zadoff-Chu sequences are also used in generating downlink Primary Synchronization Signals (PSSs) and uplink preambles. Reference signals for different UEs are derived from different cyclic shift parameters of the base sequence.

1) Demodulation Reference Signals (DMRS): DMRSs are transmitted by UE as part of the uplink resource grid. They are used by the uplink channel estimation to equalize and demodulate the uplink control (PUCCH) and data (PUSCH) information. In the case of PUSCH, when a normal cyclic prefix is used, DMRS signals are located on the fourth OFDM symbol of each slot and extend across all the resource blocks. In the case of PUCCH, the location of DMRS will depend on the format of the control channel.

2) Sounding Reference Signals (SRS): SRSs are transmitted on the uplink in order to enable the base station to estimate the uplink channel response at different frequencies. These channel-state estimates may be used for uplink channel-dependent scheduling. This means the scheduler can allocate user data to portions of the uplink bandwidth where the channel responses are favorable. SRS transmissions are used for timing estimation and control of downlink channel conditions when downlink and uplink channels are reciprocal or identical (TDD mode).

3) Physical Uplink Control Channel (PUCCH): The PUCCH carries three types of control signaling information: ACK/NACK signals for downlink transmission, scheduling requests (SR) indicator sent by UE when it wants to transmit uplink data on PUSCH, and finally the feedback from the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

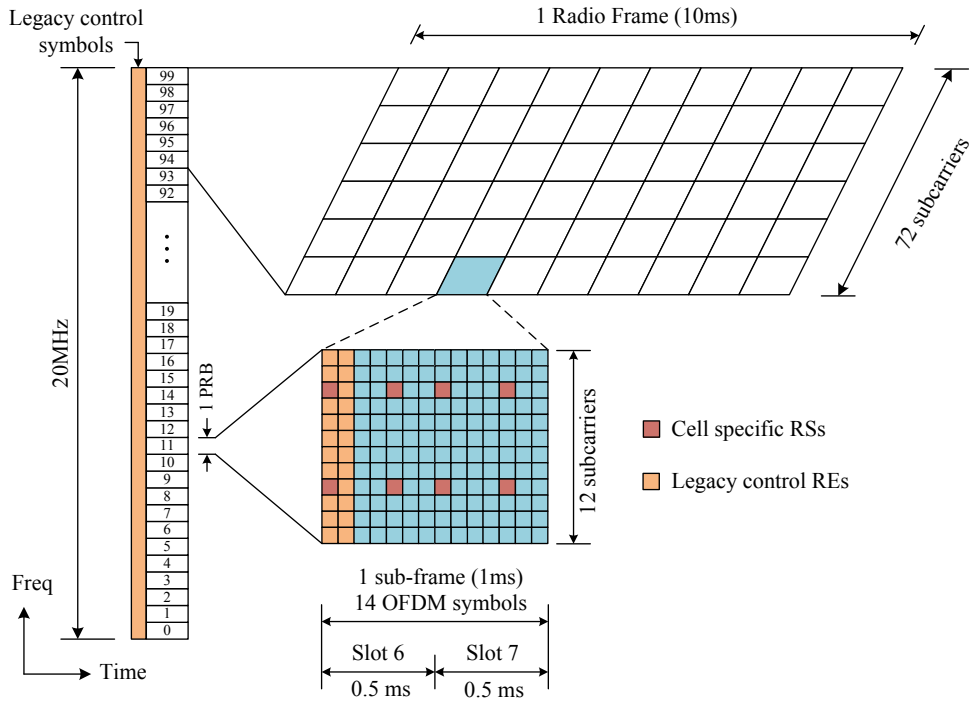

Fig. 2. Frame structure of legacy LTE systems for FDD with Normal CP type.

downlink channel information, including the Channel Quality Indicator (CQI), the Precoding Matrix Indicator (PMI), and the Rank Indicator (RI). The last three indicators are representing the channel state information (CSI). Furthermore, the feedback of the downlink channel information relates to MIMO modes in downlink. In order to ensure the correct choice of the MIMO transmission schemes in downlink, each terminal must perform measurements on the quality of the radio link and report the channel characteristic to the base station. This essentially describes the channel quality functions of the UCI as contained in the PUCCH.

4) Physical Random Access Channel (PRACH): If a UE would like to transmit on the PUSCH but does not have resource on this channel, it should send a scheduling request on the PUCCH. However, in order to initiate access to the PUCCH, the UE shall initiate the random access procedure. It uses the Physical Random Access Channel (PRACH) to transmit a preamble to begin such procedure. Since this corresponds to the first communication from the UE to the base station, the system does not know the type or specifications of the UE device. After exchanging messages with the UE, the base station sends the UE receives resource grants on the PUSCH and the required timing advance. Various transmission modes, such as Cyclic Delay Diversity (CDD) and Precoding Vector Switching (PVS), provide a transparent way of decoding the preamble information. The PRACH is transmitted on 6 RBs for the duration up to one subframe long. The exact length and the frequency offset of the PRACH is advertised by the base station using SIB2. A PRACH transmission has a cyclic prefix, a preamble, and a guard period. The preamble sequences have one or two symbols of 800 microseconds, and are generated from Zadoff-Chu sequences. The guard period is used to prevent collisions of the symbols at the base station as the PRACH is sent without timing advance. The preamble format defines the time duration of each field. There are 3 formats depending on the size of the cell and the signal strength.

5) Physical Uplink Shared Channel (PUSCH): When the UE receives an uplink scheduling grant, the PUSCH carries uplink user data and signalling transport blocks arriving from the MAC layer to the physical layer. The UE sends one transport block at a time, where CRC is attached to it to help the base station in the error detection process. The resulting block is turbo coded with rate $1/3$ and sent through rate matching. Then the UE reassembles the coded transport blocks in the form of codewords, where codewords from the data block are multiplexed with the control signals. Following this process, the transport block is passed to the physical processor where each codeword is scrambled and the modulation mapper groups the codeword bits into modulation symbols. These modulated symbols go through a forward FFT then mapped to the physical resources using the resource element mapper. Finally, time domain uplink signal is generated using the single carrier frequency division multiple access (SC-FDMA). On the resource grid, the PUSCH occupies a contiguous set of resource blocks around the center of the uplink band, and the edges of the band are reserved for the PUCCH. Each subframe contains six PUSCH symbols and one demodulation reference symbol.

C. Downlink Physical Channels and Functionalities

The Legacy LTE has a single type of traffic logical channel which is the Dedicated Traffic Channel (DTCH), and four types of control logical channel: the Broadcast Control Channel (BCCH), the Paging Control Channel (PCCH), the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Common Control Channel (CCCH), and the Dedicated Control Channel (DCCH). The dedicated logical traffic channel and all the logical control channels, except for PCCH, are multiplexed to form a transport channel known as the Downlink Shared Channel. The Paging Control Channel (PCCH) is mapped to the Paging Channel (PCH) and combined with the DL-SCH to form the Physical Downlink Shared Channel (PDSCH). The PDSCH and four other physical channels (PDCCH, Physical Downlink Control Channel; PHICH, Physical Hybrid Automatic Repeat Request Indicator Channel; PCFICH, Physical Control Format Indicator Channel; and PBCH, Physical Broadcast Channel) provide all the user data, control information, and system information needed in the unicast mode, which are delivered from higher layers.

1) Reference Signals: Downlink reference signals support the channel estimation functionality needed to equalize and demodulate the control and data information. They are used in CSI measurements (such as RI, CQI, and PMI) needed for channel quality feedback. LTE specifies five types of reference signal for downlink transmission, namely: Cell-Specific Reference Signals (CSR), UE-Specific Reference Signals, Channel-State Information Reference Signal (CSI-RS), MBMS reference signals, and Positioning reference signals. MBMS reference signals are used in the coherent demodulation employed in multicast/broadcast services, and the positioning reference signal is first introduced in R9 to provide measurements on multiple cells helping in estimating the position of a given terminal.

Cell-Specific Reference Signals

Cell-Specific Reference Signals (CSRs) are common to all users in a certain cell, and are transmitted in every downlink subframe and in every resource block in the frequency domain, thus cover the entire cell bandwidth. The CRSs can be used by the terminal for channel estimation for coherent demodulation of any downlink physical channel except PMCH and PDSCH in the case of transmission modes 7, 8, or 9, corresponding to non-codebook-based precoding. The CRSs can also be used by the UE to acquire CSI. Also the UE measurements such as CQI, RI, and PMI performed on CRSs are used as the basis for cell selection and handover decisions.

UE-Specific Reference Signals

UE-specific reference signals, also known as demodulation reference signals (DMRS), are only used in downlink transmission (modes 7, 8, or 9), where CSRs are not used for channel estimation. DMRSs first introduced in LTE R8 in order to support a single layer, and later in R9 to support up to two layers. Furthermore, an extended specification introduced in R10 aimed to support up to eight simultaneous reference signals.

When only one DMRS is used, 12 reference symbols are inserted in resource blocks pair. CSRs require spectral nulls or unused resource elements on all other antenna ports when a resource element on any given antenna is transmitting a reference signal. This is a major difference between CSR and DMRS. When two DMRSs are used on two antennas, all 12 reference symbols are transmitted on both antenna ports. The interference between the reference signals is mitigated by generating mutually orthogonal patterns for each pair of consecutive reference symbols.

CSI Reference Signals

CSI-RSs are designed for cases where we have between four and eight antennas. CSI-RSs were first introduced in LTE R10. They are designed to perform a complementary function to the DMRS in LTE transmission mode 9. While the DMRS supports channel estimation functionality, a CSI-RS acquires CSI. To reduce the overhead resulting from having two types of reference signal within the resource grid, the temporal resolution of CSI-RSs is reduced. This makes the system incapable of tracking rapid changes in the channel condition. Since CSI-RSs are only used with four to eight MIMO antenna configurations, and this configuration is only active with low mobility, the low temporal resolution of CSI-RSs does not pose a problem.

2) Synchronization Signals: In addition to reference signals, LTE also defines synchronization signals. Downlink synchronization signals are used in a variety of procedures, including the detection of frame boundaries, determination of the number of antennas, initial cell search, neighbor cell search, and handover. Two synchronization signals are available in the LTE: the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS). Synchronization signals are related to the PHY cell identity. There are 504 cell identities defined in the LTE, organized into 168 groups, each of which contains three unique identities. The PSS carries the unique identities 0, 1, or 2, whereas the SSS carries the group identity with values 0 to 167. Thus the physical layer cell identity $\mathrm{N}_{\mathrm{ID}}^{\mathrm{cell}} = 3\mathrm{N}_{\mathrm{ID}}^{1} + \mathrm{N}_{\mathrm{ID}}^{2}$ is uniquely defined by a number $\mathrm{N}_{\mathrm{ID}}^{1}$ in the range of 0 to 167, representing the cell ID group, and a number $\mathrm{N}_{\mathrm{ID}}^{2}$ in the range of 0 to 2, representing the sector ID within the group. Both the PSS and the SSS are mapped onto the central 62 subcarriers with another 10 subcarriers on the boundaries padded with zeros, forming the central 6 RBs (72 subcarriers located around the DC subcarrier). Using this structure, a UE can receive both synchronization signals without prior knowledge of the downlink bandwidth. In an FDD frame, they are positioned in subframes 0 and 5, next to each other with the PSS and the SSS placed in the last two OFDM symbols of slots 0 and 10 respectively. The PSS determines one of the three possible values of the cell identity within a group. To do so, each cell ID uses one of three Zadoff-Chu root sequences of length 63. The process of the PSS is done by 5 ms monitoring and comparing it to find the used root sequence making use of the good cross-correlation properties of the Zadoff-Chu sequences. Hence, the UE can measure the time at which the PSS arrived and extract a cell identify within a group. Then, the UE uses this timing information to receive the SSS which uses an interleaved concatenation of two binary m-sequences, each of length 31 known as Gold sequences to identify the cell group. The combination of these two sequences differs between subframes 0 and 5. The concatenated sequence is scrambled with a scrambling sequence given by the primary

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

synchronization signal. Using cross correlation, the UE will be able to identify the CP type (Normal or extended) and the duplex mode (FDD or TDD) as well as exact timing within the frame.

3) Physical Downlink Broadcast Channel (PBCH): The PBCH carries the Master Information Block (MIB), which contains the basic PHY system information and cell-specific information needed during the cell search. After the mobile terminal correctly acquires the MIB, it can then read the downlink control and data channels and perform necessary operations to access the system. The MIB contains four fields of information. The first two fields hold information regarding downlink system bandwidth and PHICH configuration. The downlink system bandwidth is communicated as one of six values for the number of resource blocks in downlink (6, 15, 25, 50, 75, or 100). Those values for the number of resource blocks map directly to bandwidths of 1.4, 3, 5, 10, 15, and 20 MHz, respectively. The PHICH configuration field of the MIB specifies the duration and amount of the PHICH. The PBCH is always confined to the first four OFDM symbols found in the first slot of the first subframe of every radio frame. The base station maps the MIB on the PBCH across 40 ms periods (four radio frames), with portions transmitted in the first subframe of every frame. When using normal CP, the PBCH occupies 72 subcarriers (6 RBs) centered on the DC subcarrier using the first four symbols of slot one.

The BCH data arrives to the coding unit in the form of a maximum of one transport block every transmission time interval of 40 ms. Generally there are 14 information bits + 10 spare bits (set to all zeroes currently), makes total 24 bits. From these information bits, 16 CRC parity bits are computed. The eNodeB can use 1, 2 or 4 antennas for transmission. The CRC bits are scrambled based on the 1, 2 or 4 antenna used in the transmitter. Hence, the total number of bits becomes 14 + 10 + 16 = 40 bits. After the convolutional encoder, the total number of bits (for normal CP) becomes = $40 \times 3 = 120$. Then, 24×3 NULLs are appended to these 120 bits to make 192 for sub-block interleaving and inter-column permutations. These bits are repeated 16 times by discarding the appended Nulls resulting in 120×16 = 1920 bits (or 1728 bits in case of Extended CP), then QPSK mapped so that the total number of QPSK symbols become = 1920/2 = 960 symbols (or 864 symbols in case of Extended CP).

These 960 symbols are segmented into 4 equal sized self-decodable units or segments. These symbols are then placed in PBCH Resource Elements in the second slot of the first subframe (slot 1). That is the first subframe's second slot contains 960/4 = 240 symbols (or 216 symbols in case of Extended CP) and then inserted in the OFDM resource elements. PBCH is restricted to the 72 subcarriers around the DC in the resource grid irrespective of the UE bandwidth. The PBCH is transmitted in the first four OFDM symbols of the second slot of the first subframe in every radio frame. For example, in a subframe which contains PBCH (e.g. first subframe of a frame) there are total $72 \times 7 \times 2$ = 1008 REs (for normal CP). Out of that, currently in that subframe, the total number of CRS (Cell Reference Signal) = $(4 \times 6) \times 6$= 144 REs (for 4 antennas system). If the system is using single antenna instead of 4 antennas, then 48 REs will be having CRSs and the remaining elements (out of 144) will be Null.

4) Physical Downlink Control Format Indicator Channel (PDCFICH): The PDCFICH is used to define the number of OFDM symbols that carry the Downlink Control Information (DCI) in a subframe. The PDCFICH information is mapped to specific resource elements belonging to the first OFDM symbol in each subframe. The possible values for PDCFICH (one, two, three, or four) depend on the bandwidth, frame structure, and subframe index. For the 1.4 MHz bandwidth, since the number of resource blocks is quite small, PDCFICH may need up to four symbols for control signaling. However, for the larger bandwidths, the number of can take up to three OFDM symbols.

5) Physical Downlink Control Channel (PDCCH): In order to start communication between the base station and the mobile terminal (UE), a PDCCH is defined for each Physical Downlink Shared Channel (PDSCH) channel. PDCCH mainly contains the scheduling decisions that each terminal requires in order to successfully receive, equalize, demodulate, and decode the data packets. Since the PDCCH information must be read and decoded before decoding of PDSCH begins, in a downlink PDCCH occupies the first few OFDM symbols of each subframe. The exact number of OFDM symbols at the beginning of each subframe occupied by the PDCCH (typically one, two, three, or four) depends on various factors, including the bandwidth, the subframe index, and the use of unicast or multicast services.

The control information carried on the PDCCH is known as Downlink Control Information (DCI). Depending on the format of the DCI, the number of resource elements (i.e., the number of OFDM symbols needed to carry them) varies. There are 10 different possible DCI formats specified by the LTE standard (known as 0,1,1A,1B,1C,1D,2,2A,2B,2C,2D,3,3A,4), with each format contains a specific set of information and certain purpose. The information carried by DCI format are: resource allocation information, such as resource block size and resource assignment duration; transport information, such as multi-antenna configuration, modulation type, coding rate, and transport block payload size; and information related to the HARQ, including its process number, the redundancy version, and the indicator signaling availability of new data. The scheduling messages transmitted over the PDCCH is addressed to a certain Radio Network Temporary Identifier (RNTI). A variety of RNTI types are used in LTE to define the identity of the intended UE which should read the scheduling messages, and the type of these messages. The type of the RNTI is used to generate the CRC code that will be used by the transport layer to encode the DCI information.

The resource element mapping of the PDCCH is done using control channel elements (CCE), each contains 9 resource element groups (REG). Each REG consists of 4 REs. Based on the length of the DCI message, the base station maps the PDCCH onto 1,2,4 or 8 consecutive CCE. This is called the *aggregation level*. In other words, based on the length of the DCI, PDCCH can be scheduled onto 36, 72, 144, or 288

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

resource elements.

Further, the CCEs are organized into *common search spaces* and *UE-specific search spaces*. The first type is available to all UE in the cell and have predefined location in the downlink region. However, the second type is assigned to groups of UEs and its location depends on the RNTI type of the UE.

As the aggregation level of a UE changes from a subframe to another, and the length of DCI changes the aggregation level, the UE locates its PDCCH and find the DCI format using blind detection. In other words, a UE attempts to decode using all DCI formats with candidate locations in the search space, and the correct combination is the one that checks the CRC. The reliability of the PDCCH is enhanced by means of transmit diversity using space-frequency block codes, and is protected against inter-cell interference using a cell-specific scrambling pattern.

Although the described PDCCH functions work fine for most of the situations, it suffers from some limitations as the requirements of the LTE network evolves. First, limiting the channel resources to the first 3-4 symbols of slot 0 has a direct limitation on the cell capacity (number of users could be scheduled). Second, PDCCH is transmitted only in a distributed manner, hence, it cannot benefit from the beamforming using MIMO while the base station enjoys multiple antennas. Third, with the PDCCH transmissions of a certain user spread over the entire frequency band, it does not benefit form frequency selective scheduling nor inter-cell interference coordination.

The aforementioned reasons urged the evolution towards the Enhanced physical downlink control channel (EPDCCH) in R11. The EPDCCH still carries the same information of PDCCH except that it shares the resources with the traffic PDSCH to increase the capacity. Within each subframe, a resource block pair is either assigned to PDSCH or EPDCCH, which makes the capacity of the new control channel adjustable and also makes use of interference coordination. EPDCCH is transmitted on newly defined four antenna ports (AP 107 - 110), which are associated with RS (occupying the same REs as AP 7-10). EPDCCH and its RS are preceded with a user-specific preceding matrix, and also supports multiuser MIMO (MU-MIMO)with up to 4 layers (i.e. supporting simultaneously 4 different users).

6) Physical Downlink Shared Channel (PDSCH): After the base station sends the UE a scheduling command, it transmits the data of the DL-SCH using the scheduling commands defined. The PDSCH carries downlink user data and signalling transport blocks arriving from the MAC layer to the PHY. Specifically, transport blocks are transmitted one at a time in each subframe. The base station adds 24-bit CRC to each DL-SCH transport block which is used by the UE for error detection. Following adaptive modulation and coding, the modulated symbols are mapped onto multiple time-frequency resource grids, which are eventually mapped to multiple transmit antennas for transmission. The type of MIMO technique used in each subframe can be adapted based on the received SNIR (which indicates the channel conditions). It should be mentioned that, the PDSCH and the PUSCH are the only physical channels that can adapt their modulation scheme according to channel quality observed at the mobile terminal. The measurements made at the terminal must be sent back to the base station in order to help the scheduling decisions. At each subframe, the mobile terminal needs to be notified about the scheduling from the base station for each transmitted resource block. Among the information that must be communicated; are the number of resource blocks allocated to a user, the transport block size, the type of modulation, the coding rate, and the type of MIMO mode used per each subframe.

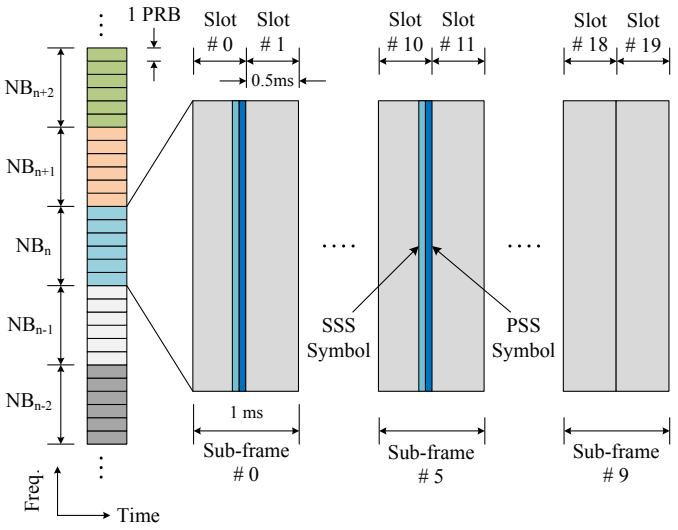

Fig. 3. Frame structure of LTE-MTC systems for FDD with Normal CP type showing the synchronization signals. The concept of narrowband is highlighted.

IV. Physical Layer Features for LTE-MTC Systems

The behaviour of the MTC terminals is different from the legacy LTE users, for which the LTE was optimized. Therefore, in order to accommodate the new requirements, the CAT-M UE category is recently added for MTC communication in R13. A lot of effort was put to specify a new UE for MTC operation in LTE which allows for enhanced coverage compared to existing LTE networks and low power consumption. In details, the LTE-MTC specifies a new R13 low complexity UE category for MTC operation in LTE half duplex FDD mode based on the R12 low complexity UE category supporting additional capabilities. Among these capabilities, is a reduced UE bandwidth of 1.4 MHz for the downlink and uplink with the ability to operate within any system bandwidth. Also, the frequency multiplexing of bandwidth reduced UEs and non-MTC UEs should be accommodated. For the new UE category to have a tangible complexity reduction, the maximum transmit power of the new UE power should be reduced such that an integrated power amplifier (PA) implementation is possible. Also, power consumption reduction is a must for the LTE-MTC UE target ultra-long battery life. The most important feature of the new category, is to improve the LTE coverage corresponding to almost 15 dB for FDD.

A variety of techniques is considered to achieve such requirements, including: subframe bundling techniques with

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

HARQ for physical data channels (PDSCH, PUSCH), repetition techniques for control channels (e.g. PBCH, PRACH, EPDCCH), uplink PSD boosting with smaller granularity than 1 PRB, resource allocation using EPDCCH with cross-subframe scheduling and repetition, new physical channel formats with repetition for SIB/RAR/Paging, new SIB for bandwidth reduced and coverage enhanced UEs, and increased reference symbol density and frequency hopping techniques.

A. MTC Features

More constrains are added on the MTC UE to reduce its cost and complexity. The features of the physical downlink control channel for MTC are summarized as:

- The design of the physical downlink control channel for MTC is based on (E)PDCCH.
- The introduction of new DCI messages to R13 for low complexity UEs.
- The use of a narrowband (within 6 PRBs) control channel.
- Its usage for other UEs in enhanced coverage.
- The demodulation of the control channel shall be based on CRS and/or DMRS.

B. Narrowband Concept

The bandwidth choice of a certain base station is configured once and remains unchanged during operation, hance, it would be a good choice to use a bandwidth unit that can be a common divisor of the available bandwidth options in the legacy LTE. Then the choices become limited to 6 RBs or one RB. However, in order for the MTC devices to capture the signature of the LTE signal, it will have to receive the synchronization signals PSS and SSS. These signals occupy the central 6 RBs of the bandwidth of the base station, which makes it desirable for the MTC devices to take 6 RBs as the basic unit of bandwidth. Not only that, but also as mentioned before, the legacy PDCCH is mapped to the full occupied bandwidth, which makes decoding PDCCH is not possible in MTC applications, since the UE is limited to bandwidth of only 1.4 MHz. However, the enhanced version EPDCCH, uses one PRB pair as the basic resource unit, which makes it a good candidate to be used to control MTC UE. Furthermore, the use of only one PRB for the MTC control channels based on EPDCCH was reported to be insufficient, as it could provide the required converge enhancement (CE) [57]. It was concluded in [58] that, increasing the bandwidth of the basic EPDCCH to 6 PRBs in the 1.4 MHz bandwidth on the MTC UE along with repetition will be sufficient to have a good coverage of -14 dB. Furthermore, coverage enhancement can be achieved by employing EPDCCH that supports beamforming which increases coverage by directing the power of the base station towards the UE. For these reasons, it is agreed on to use the 6RBs (or one narrowband (NB)) as the basic bandwidth unit for MTC. A narrowband is defined as six non-overlapping consecutive physical resource blocks in the frequency domain. The total number of downlink narrowbands in the downlink transmission bandwidth configured in the cell is given by $N_{NB}^{DL} = \lceil \frac{N_{RB}^{DL}}{6} \rfloor$ and are numbered $n_{NB} = 0, ..., N_{NB}^{DL} - 1$ in order of increasing physical resource-block number. The narrowband concept and numbering is highlighted in Fig. 3.

C. Modes Of Operation

1) Frequency Hopping: With the small bandwidth offered to MTC UE and the use of single receiver chain, the frequency and spatial diversity are taken away. To retrieve some of the lost frequency diversity, the frequency hopping concept is added to the MTC LTE system. In other words, MTC transmissions will hop from one narrowband to another to make use of transmitting over different channels, and hence, provides frequency diversity. However, frequency hopping shall introduce new challenges. One of these issues is that, the UE will have to re-tune its RF chain every time it hops. This re-tuning takes time which might affect the overall throughput. According to R13 specifications, two OFDM symbols worth of time is needed for re-tuning. Further, re-tuning will take place during the legacy control channel symbols are to be discarded anyway by the MTC UE. This choice of re-tune time and period reduces the chance of loosing a considerable amount of network throughput. Another issue with frequency hopping is that the UE and eNodeB both need to know the hopping pattern. This needs to be signalled or must be determinable from certain system parameters.

For MPDCCH, the first NB is determined without any new higher layer configuration involved (i.e. it is specified in the system information messages). The other NB are determined using a single configurable offset. The offset, signalled in the system information, is cell-specifically configured and applicable to all CE levels. In CE mode A, the hopping is turned on or off dynamically by higher-layer signalling in the DCI if the hopping is enabled. The number of NB for hopping is either 2 or 4. This parameter is signalled to the UE and it is cell-specific. In reality, one problem with frequency hopping is that channel estimation across subframes has been the main implementation scheme to enhance the estimation accuracy. However, with frequency hopping, the channel estimation will need to be restarted whenever hopping is scheduled. Based on the specifications, the MPDCCH transmission will stay on one NB for Y subframes, where Y is in the range of 2-8 subframes to allow for some benefit of cross-subframes channel estimation.

This value Y is called the frequency hopping interval and it is cell-specific. There are 4 values signalled to specify the frequency hopping interval for all channels in a specific channel direction and UE mode, namely mode A DL, mode B DL, mode A UL, mode B UL. For FDD, and mode A, the values that this parameter may take are among the set 1, 2, 4, 8. For mode B, they take values in the set 2, 4, 8, 16.

2) Repetitions: As mentioned before, the limitations forced on the MTC LTE directly affects the downlink control channel, which in turn, has a direct impact on the performance of the downlink. For the downlink to have sufficient link budget to support the prospected coverage enhancement, an enhanced version of the distributed EPDCCH is reused as the base control signal for MTC. Thus, enhancement is obtained by transiting repeated copies of the same signal over time. As

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

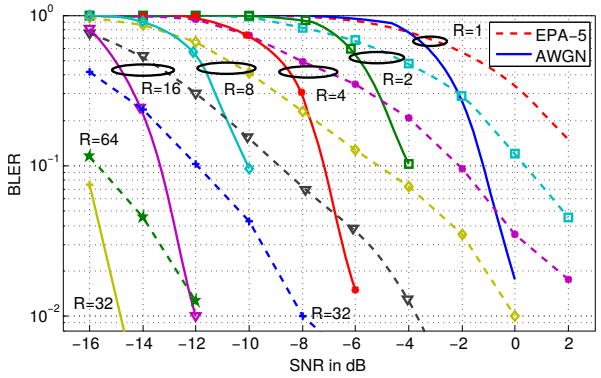

Fig. 4. Effect of repetition on the BLER versus Average SNR for aggregation level L=2 in MPDCCH decode.

a direct result of the use of such repetition code, the link performance can be enhanced through time diversity and boost the control signal energy. On the other hand, the repetition has the effect of increased decoding time (more latency), which requires more wake-up time of the MTC device.

In order to ideally show the effect of repetition, the control channel performance has been considered. For instance, Additive White Gaussian Noise (AWGN) and EPA-5 [59] were simulated. EPA-5 is a standard LTE channel with large coherence time (maximum Doppler spread is 5Hz). The performance is evaluated under perfect synchronization conditions in addition to the assumption of perfect knowledge of the channel state information. The objective is to evaluate the performance loss due to the fading channel without incorporating any implementation or complexity loss. That way, the EPA-5 effect is obvious when compared to AWGN. Fig. 4 shows the performance, represented by the Block Error Rate (BLER), for decoding a single MPDCCH candidate that corresponds to aggregation level 2. Different repetition levels are assumed for both channels. It is very clear that the gain of repetition appears significantly at very low SNR values. From Fig. 4, one can notice that enhanced coverage LTE-MTC UE operating at SNR=-15dBs requires repetitions in the order of 64 and higher for aggregation level 2 to achieve BLER of 1% and less. Indeed, the conventional EPDCCH performance is characterized by the case in which $R = 1$. It is obvious that without repetition, classical EPDCCH has no ability to decode the control channel correctly at very low SNR values for this aggregation level.

3) MTC Physical Random Access Channel (MPRACH): The legacy design of the PRACH channel is limited to 6 RBs only, which makes it suitable for the MTC use as it signifies the narrowband constraint. However, the legacy PRACH needs some modifications to support the extra path-loss due to the extended coverage. Hence, repetitions and frequency hopping is exploited to provide the necessary diversity to the MPRACH. Like the legacy PRACH, The physical layer random access preamble consists of a cyclic prefix of length T_{CP} and a sequence part of length T_{SEQ} with different 5 preamble formats (0,1,2,3,4). The values of these parameters depend on the frame structure and the random access configuration and the preamble format is controlled by higher layers. For each coverage enhancement level, UEs with different geographic locations may have different radio conditions and propagation delay. Thus, different PRACH repetition levels could apply to different preamble formats to adapt to different propagation delay and compensate for different propagation losses. For each PRACH coverage enhancement level, there is a PRACH configuration done at higher layers with a PRACH configuration index values from 0 to 63, a PRACH frequency offset, and a number of PRACH repetitions per attempt N_{rep}^{PRACH}. The UE selects the repetition level to use for the initial transmission based on DL measurements, but this is only acceptable if sufficient DL measurement accuracy can be achieved within a reasonable DL measurement time. If sufficient accuracy cannot be achieved, the UE will start at the lowest configured PRACH repetition level. The number of repetitions as well as the starting subframe are also configured by higher layer signalling. It has been proposed that, the UE should remember what PRACH repetition level is used last time and use this information when setting the starting point for the next access. PRACH frequency hopping may provide frequency diversity gain and reduce the number of repetition. From this point of view, the power consumption of enhanced PRACH transmission could be saved due to reduced active time.

4) MTC Physical Downlink Control Channel (MPDCCH): EPDCCH has been chosen to be the starting point towards designing the new MTC control channel MPDCCH. However, special requirements have been adapted to best suite the new MTC platform and to support the required coverage with reasonable complexity and power consumption. The new set of features for MPDCCH require defining new set of downlink control formats, adding a possibility for a common UE to access the control channel by introducing the new common search space, and enhancing the control channel assignment procedure to support the new MTC features such as repetition and frequency hopping. A summary of the introduced features to design the new MPDCCH is shown in Fig. 5.

5) MTC Search Spaces: In LTE systems, the downlink control region is shared by all UEs in one cell. Each UE should monitor the control region and perform blind decoding to detect whether or not there is control information for itself. In order to reduce the number of blind decoding trials per UE, each UE has a defined search space area of the control region to monitor, rather than having to monitor the whole control region. The search space is defined on the basis of enhanced control channel elements (ECCEs). Control information may occupy 1, 2, 4, or 8 CCEs aggregated together depending on the size of the control information and the channel quality of the UE.

The search space starting point for a UE is determined by a hash function and the search space size is determined by the PDCCH aggregation level. The hash function randomizes the search space locations of different UEs and effectively reduces the blocking probability. The MPDCCH has two broad classes of search spaces: UE-specific search space (USS) for messages directed specifically to the UE and Common Search Space (CSS) for messages directed to multiple users or for messages to a specific UE before the USS has been configured. It is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

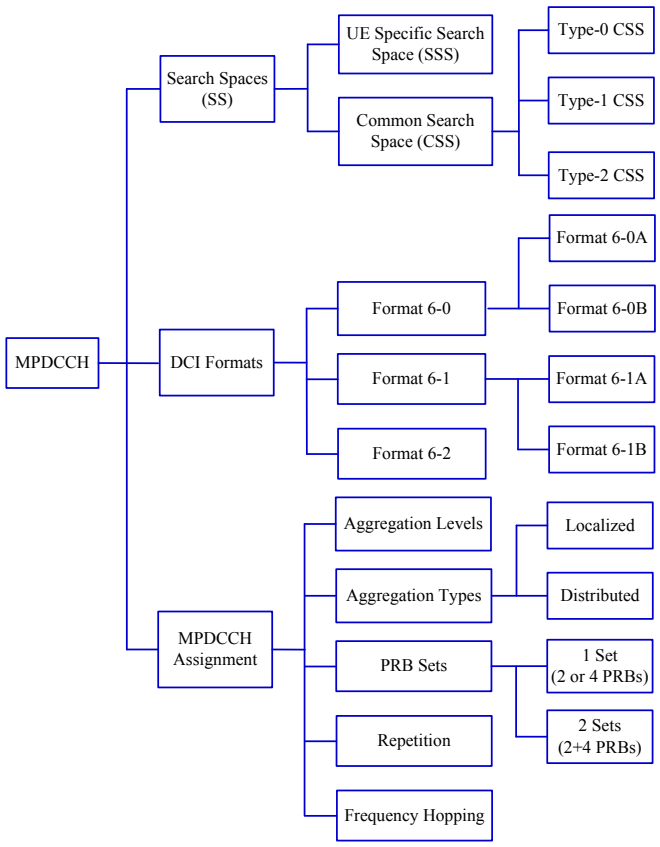

Fig. 5. Summary for the introduced features for MPDCCH.

worth to mention that the legacy EPDCCH has only USS since PDCCH is used for the CSS. In MPDCCH, the UE will have to blindly decode both USS and CSS. The search spaces will differ depending on the CE mode whether mode A or mode B.

6) MTC DCI Formats: Generally, the eNodeB employs the downlink control information messages to send downlink scheduling commands, uplink scheduling grants, and uplink power control commands to the UE. The DCI can be written using several different formats. Indeed, conventional LTE-A systems up to R12 support 14 different formats, namely format 0, 1/1A/1B/1C/1D, 2/2A/2B/2C, 3/3A, 4, and 5. Each format contains a specific set of information and has a specific purpose. However, some formats have been grouped under common name which implies that the main functionality of these downlink messages would have something in common but the details will be different. For instance, the main theme for Format 1 and its group is to mainly provide the downlink scheduling information such as the PRB allocation, modulation and coding, and single or multiple users support. The differences from one format to another in the same group are to which transmission mode and antenna system to use. Also, the basic purpose for Format 2 is to set configuration for MIMO systems. However, they differ on how the MIMO system is configured on being used for open loop, closed loop, beamforming, and multi-user MIMO configurations. Although there have been multiple formats to send various scheduling commands, in LTE-MTC systems, new formats have been introduced to the system. The motivation is to skip the unused parameters such as the number of codewords since LTE-MTC is defined for a single codeword. Also, the DCI messages for both uplink and downlink grants were designed to fit the same number of bits with some indication bits to differentiate between the formats. This is mainly to reduce the blind decoding iterations and hence, reduced UE complexity. Furthermore, with the introduction of enhanced coverage, repetition, and frequency hopping, the UE will mainly require new information to facilitate the use of repetition, narrowband resource assignment, frequency hopping flag. For example, downlink DCI assignment should indicate the MPDCCH repetition factor so that UE can expect when the message is complete. For these reasons and others, three new DCI formats, namely format 6-0, 6-1, and 6-2 have been defined for LTE-MTC system for uplink grant, downlink scheduling, and paging, respectively. To best suite the operating mode, whether being Mode A or Mode B, there are two versions for each format where the number of information bits differ.

V. Physical Layer Features for NB-IoT Systems

A. Deployment Scenarios and Modes of Operation

As a finite and scarce natural resource, spectrum needs to be used as efficiently as possible. Thus, technologies that use spectrum tend to be designed to minimize usage [60]. To achieve spectrum efficiency, NB-IoT has been designed with a number of deployment options for GSM, WCDMA, or LTE spectrum. There are three deployment scenarios.

1) **In-band Operation:** An NB-IoT carrier is a self-contained network element that uses a single PRB. For in-band deployments with no IoT traffic present, the PRB can be used by LTE for other purposes, as the infrastructure and spectrum usage of LTE and NB-IoT are fully integrated. The base station scheduler multiplexes NB-IoT and LTE traffic onto the same spectrum, which minimizes the total cost of operation for IoT services. To support full flexible design, the specifications define two modes for the in-band operation. The first mode, namely Same-PCI mode, assumes that the NB-IoT carrier has identical cell parameters (i.e., cell ID and number of Tx antennas) as the donor legacy cell. The other mode considers some flexibility of having a different cell ID and different number of Tx antennas.
2) **Stand-alone Operation:** This mode of operation is mainly intended to replace a GSM carrier with an NB-IoT carrier. By steering some GSM traffic to the WCDMA or LTE network, one or more of the GSM carriers can be used to carry IoT traffic. As GSM operates mainly in the 900 MHz and 1,800 MHz bands (spectrum that is present in all markets), this approach accelerates time to market, and maximizes the benefits of a global-scale infrastructure.
3) **Guard band Operation:** this can be applied either in WCDMA or LTE. To operate in a guard band without causing interference, NB-IoT and LTE need to coexist. The physical NB-IoT layer is designed with the requirements of LTE guard band coexistence specifically taken

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

into consideration. Again, NB-IoT uses OFDM in the downlink and SC-FDMA in the uplink. The design of NB-IoT has fully adopted LTE numerology, using 15kHz subcarriers in the uplink and downlink, with an additional option for 3.75kHz subcarriers in the uplink to provide capacity in signal-strength-limited scenarios.

It should be noted that, NB-IoT supports operation with only one or two Tx antenna ports. For operation with two Tx antenna ports, NB-IoT uses the conventional Space Frequency Block Coding (SFBC) employing the Alamouti mapping. Unlike other LTE-based systems, NB-IoT utilizes the same transmission scheme for all physical channels including Narrowband Physical Downlink Control Channel (NPDCCH), Narrowband Physical Broadcast Channel (NPBCH), and Narrowband Physical Downlink Shared Channel (NPDSCH).

B. Downlink Physical Channels

*1) **Frame Structure**:* With a carrier bandwidth of just 200KHz, an NB-IoT carrier can be deployed within an LTE carrier as one PRB. Fig. 6 shows a 3MHz LTE carrier in which a single PRB is assigned to NB-IoT. An operating NB-IoT band is defined as a contiguous set of 12 subcarriers forming one PRB. A single radio frame is 10ms which consists of 10 subframes with equal duration. Each subframe is divided into two slots with equal periods. Unlike conventional LTE which defines two CP types with different CP patterns, NB-IoT in R13 supports only the normal CP type, where a slot is composed of 7 OFDM symbols. According to the specification [54], if the signal is sampled at 1.92 MSamples/sec, similar to LTE-MTC, the CP length of the first symbol in each slot is 10 samples and those of the other symbols are 9 samples long. Also, in this case, the OFDM symbol spans $N = 128$ sub-carriers.

*2) **Synchronization Signals**:* NB-IoT intends to occupy a narrow bandwidth of only 200KHz, which is not backward compatible to the supported bandwidths by the legacy LTE. Therefore, NB-IoT redefines the cell attach procedure including cell search and initial synchronization [61][60]. During initial synchronization, CFO is estimated and compensated to enable proper signal detection. The UE acquires the physical cell identification by employing the cell search procedure. To cope with these changes, NB-IoT employs new set of synchronization signals, namely Narrowband Primary Synchronization Signal (NPSS) and Narrowband Secondary Synchronization Signal (NSSS) [54]. The new sequences have different bandwidth, mapping, periodicity, and generation when compared to the legacy LTE synchronization signals. Unlike conventional LTE, cell ID is encapsulated only in the secondary sequence without involving the primary sequence.

NPSS and NSSS sequences are constructed from a frequency domain Zadoff-Chu sequence where NPSS length is 11 samples while the NSSS consists of 132 samples. The NPSS, $P_l(n)$, is generated such that $P_l(k) = Q(l)e^{-j\pi uk(k+1)/11}$, where $0 \leq k < 11$, $3 \leq l < 14$ is the OFDM symbol index, the sequence root $u = 5$, and $Q(l)$ is a modulation sequence given by $\{1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1\}$, respectively. In NB-IoT system, there are still 504 unique physical cell IDs. However, all of them are only indicated by the NSSS. The NSSS, $S(k)$, is generated according to,

$$S(k) = \bar{C}_q(k')\, e^{-j2\pi\theta_f k}\, e^{-j\frac{\pi uk(k+1)}{131}}, \;\; 0 \leq k < 132 \qquad (1)$$

where $k' = k \bmod 128$, the root sequence, u, is related to the cell ID, N_{ID}^{Ncell}, by $u = (N_{ID}^{Ncell} \bmod 126) + 3$, and the cyclic shift, θ_f, is related to the System Frame Number (SFN), n_f, such that $\theta_f = \frac{31}{132}(n_f/2) \bmod 4$. The modulated sequence, $\bar{C}_q(k')$, is given by $\bar{C}_q(k') = 2C_q(k') - 1$, where q is a cell specific parameter that is given by $q = \lfloor N_{ID}^{Ncell}/126 \rfloor$ and C_q forms four complementary 128-bits binary sequences.

In conventional LTE, primary and secondary synchronization signals (i.e., PSS and SSS, respectively) are mapped to two consecutive OFDM symbols in the same slot with a periodicity of 5msec. However, NPSS is mapped to subframe 5 of every radio frame. NSSS is mapped to the last 11 ODFM symbols of subframe 9 in radio frames having $n_f \bmod 2 = 0$. Sequences are mapped to frequency sub-carriers in an increasing order, then applied across time as shown in Fig. 6.

*3) **Narrowband Reference Symbols (NRS)**:* Due to the lack of fully adoptable LTE signal structure in case of guard and stand-alone modes, new reference signals or pilots, namely NRS, are inserted within the transmitted signal to assist the channel estimation process which is required for coherent detection at the UE side. Similar to legacy LTE, NRS uses a cell-specific frequency shift derived as the modulo division of the NB-IoT cell ID by 6. The conventional LTE CRS sequence is reused for NRS generation where the centre of LTE CRS sequence is employed as NRS sequence for all PRBs. The NRS is mapped to the last two OFDM symbols of the slot for both antenna ports in case of transmit diversity as shown in Fig. 6. As NPSS/NSSS occupy the last 11 OFDM symbols within the subframes transmitting NPSS/NSSS for normal CP, NRS are not mapped to these subframes. To ensure the demodulation and/or measurement performance, it has been agreed to transmit NRS in all valid subframes except the NPSS/NSSS subframes regardless of whether there is downlink transmission in these valid subframes or not.

In in-band operation mode, the LTE CRS REs should be reserved from NB-IoT to avoid pollution to the LTE channel estimation and measurement. However, as a special case, NPBCH decoding shall not rely on LTE CRS due to the lack of knowledge of the legacy PRB index information. This means that the new reference signal (i.e. NRS) alone should be able to provide sufficient channel estimation performance for NPBCH decoding. The NPDCCH and NPDSCH decoding performance can be ensured also based on NRS only. In this sense, LTE CRS is not a must in-band operation mode in terms of DL channel decoding. However, the standardization is designed to provide the flexibility to UE implementation for the use of LTE CRS although the performance requirements do not rely on it. On the other hand, the extra signalling overhead to support the use of LTE CRS would be limited since the resource mapping information of the LTE CRS needs be anyhow indicated to realize the rate matching around the LTE CRS REs. LTE CRS may also benefit measurement accuracy when available. For these reasons, the agreements allow two modes for in-band operation. The first assumes that the full information

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

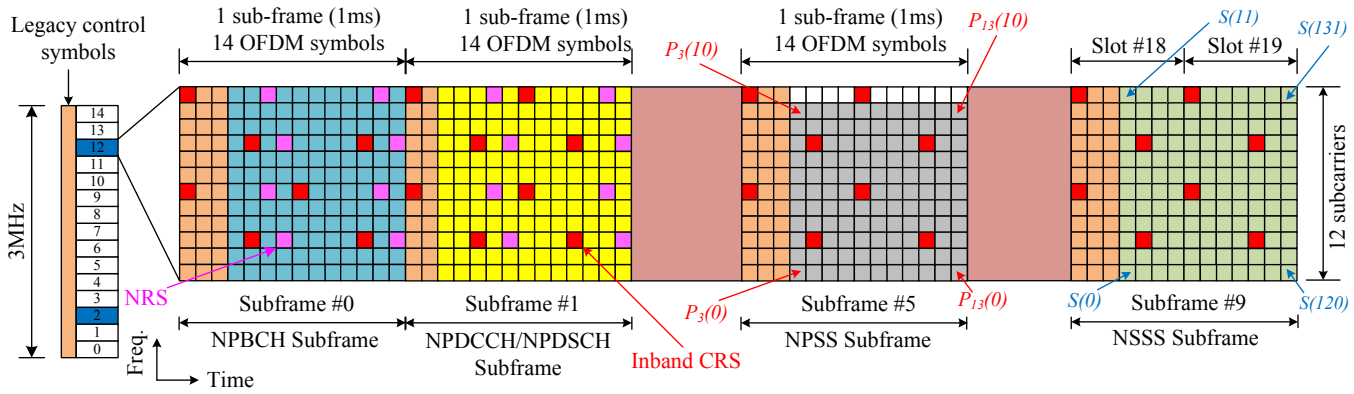

Fig. 6. Radio frame structure for NB-IoT systems. The allocated RB is expanded in time to show the NPSS/NSSS symbols mapping in addition to the broadcast channel and one data/control subframe.

of the legacy cell in terms of the cell ID and number of Tx antennas is identical to the NB-IoT carrier. In this case, the UE is free to utilize the CRS for its own demodulation and/or measurements. On the other hand, the other mode assumes that the UE is not aware of the legacy cell ID, but it has the information of the number of its Tx antennas which helps determining the rate matching around the CRS.

*4) **Narrowband Physical Downlink Broadcast Channel (NPBCH)**:* Since NB-IoT has various deployment scenarios that require different system configurations, some Narrowband Master Information Block (NB-MIB) fields are required to be operation mode dependent. For example, the UE would require to puncture the CRS in case of in-band operation. Therefore, a field representing the number of legacy Tx antennas is beneficial. In the same mode, the PRB index is needed to validate the working assumption regarding the potential usage of CRS for demodulation. In addition, there should be an indication for the raster frequency offset for the in-band operation. It is understood that, during start, the UE would scan the frequency spectrum searching for a valid NB-IoT carrier. In legacy LTE, the raster frequency is assumed to be 100KHz starting from the center of the LTE band. However, since the NB-IoT in-band deployment assumes that the NB-IoT carrier would be allocated as a single PRB with 180KHz width, the raster frequency to the NB-IoT carrier would not be multiples of 100KHz. Indeed, for odd LTE bandwidths, there is a frequency offset of $\pm$7.5KHz for the raster frequency to be multiple of 100KHz. In fact, the synchronization signal design and mapping are carefully studied so that a UE can lock to the NB-IoT carrier with an ambiguity of $\pm$7.5KHz. It is clear that a new field has to be added to the NB-MIB in order to differentiate between the various frequency offsets as the bandwidth would not be known.

In all cases, similar to LTE-MTC, NB-MIB indicates the scheduling information for the system information messages by defining the TBS size and repetition filed for the first SIB message (i.e., NB-SIB1). For these reasons, it was beneficial to design new NB-MIB fields not only to include the introduced set of fields but also to interpret the fields depending on the operation mode. The decision is to extend the NB-MIB length to 34 bits before CRC attachment. This means that the code word for the broadcast channel becomes 150 bits instead of only 120 bits. Furthermore, it was agreed that NPBCH consists of 8 independently decodable blocks. Thus, after CRC attachment and channel coding, the NB-MIB is rate matched to 1600 bits instead of 1200 bits for Normal CP type.

The rate matched bits are scrambled by the conventional LTE scrambler that is initialized with the NB-IoT Physical Cell Identifier (PCI) in each radio frame fulfilling n_f mod 64 = 0, where n_f is the SFN. This simply refers to the fact that a single NB-MIB transmission spans 64 radio frames. After the channel interleaver, the bits are QPSK modulated. The modulated bits are mapped to resource elements in a frequency then time fashion. During the mapping, the 800 QPSK modulated symbols are segmented into 8 consecutive segments such that each segment is repeated in 8 consecutive radio frames. In other words, identical symbols carrying the same segment are transmitted with 80ms duration. It is essential to enable the NPBCH decoding without any prior information about the operation mode. Indeed, only cell ID and proper frame timing are required through the conventional cell search procedure. Therefore, it has been agreed that NB-PBCH is transmitted in subframe 0 in every radio frame, where the first 3 symbols in a subframe are not utilized independent of the operational mode. In addition, for rate matching purposes, the CRS are punctured assuming 4 Tx antenna ports even for guard and stand-alone modes. Moreover, the number of NRS ports is considered based on two transmit antennas independent of the actual configuration. However, the number of NRS ports (i.e., whether 1 or 2) is indicated by NB-PBCH CRC masking similar to the conventional system.

*5) **Narrowband Physical Downlink Control Channel (NPDCCH)**:* The NB-IoT has its own control channel with customized features and definitions. Although some features have been adopted from LTE-MTC system, there are couple of restrictions that mandates redefinitions for some of the control channel concepts. First of all, the NPDCCH transmission becomes packet-based as the system only supports half-duplex mode at least for R13 version. There is no overlapping between the data channel and the control channel within the same subframe. The UE will monitor the NPDCCH when it expects a random access response (RAR), a new DL assignment, paging, or uplink grant. In case of RAR or paging, the UE has to monitor a common search space. Therefore, similar to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

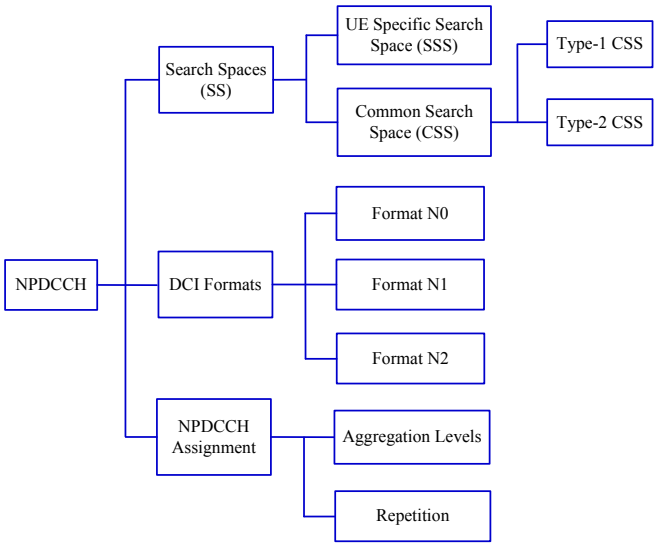

Fig. 7. Summary for the introduced features for NPDCCH.

LTE-MTC and unlike the conventional EPDCCH, two search spaces have been defined for NB-IoT. Second, due to the reduced set of information carried by the DCI messages, three new DCI formats, namely N0, N1, and N2, have been defined only for NB-IoT in R13. Third, NPDCCH assignment relies on repetition to support unconditional coverage enhancement with relatively small aggregation levels again for complexity reduction. Fig. 7 shows the essential differences between NPDCCH and other control channels in various LTE systems.

Two broad classes of search spaces have been defined for NB-IoT, namely USS for messages directed specifically to the UE and CSS for messages directed to multiple users, paging, or for messages to a specific UE before the USS has been configured (i.e., RAR message). Similar to LTE-MTC with repetitions enabled, NB-IoT provides the definition for the search space as joint combination of aggregation level and repetition factor. By varying the repetition number, a Type-1 CSS is defined for paging with more possibilities for repetitions (a maximum of 2048) and another type, namely Type-2 CSS, is specifically defined for RAR with a maximum of 8 repetitions. To avoid blocking, each UE has search space with different values for each parameter (i.e., aggregation level and number of repetitions) so that the scheduler has the ability to avoid blocking and schedule many UEs. For UEs in enhanced coverage, where it is efficient to allocate the whole bandwidth to one NPDCCH, this search space can be based on different repetition levels only, whereas for UEs in normal coverage which there may be a lesser need for repetition, it could be based on fewer repetition levels but more aggregation levels. When the number of candidates is concerned, NB-IoT is designed to monitor the minimum number of blind decodes to reduce complexity and power consumption. Indeed, a maximum of 3 candidates can be monitored every subframe in case of no repetition and only 4 candidates are targeted when repetition is employed. In addition, during the NPDCCH monitoring, the UE is not required to simultaneously process any of the UL channels and/or other DL channels.

To simplify the NPDCCH mapping, the concept of enhanced resource element group (EREG) has not been defined for NPDCCH. The control REs are directly mapped to the Narrowband Control Channel Elements (NCCEs). Only two NCCEs are available in one subframe where one NCCE consists of 6 subcarriers per OFDM symbol in a subframe. Aside from the expected performance mismatch between the two NCCEs due to the frequency selectivity of the channel, it has been agreed that NCCE mapping simply employs Frequency Division Multiplexing (FDM) structure in which the first 6 consecutive subcarriers are assigned to one NCCE and the other 6 subcarriers to the other NCCE. To support transmit diversity and gain some spatial diversity for NPDCCH, REs should be paired with shortest possible distance between REs in each pair. In this way, the instantaneous channel response for both REs within one pair are almost the same and highly correlated, which is necessary for achieving high diversity gain. However, RE-pairs are wrapped around the NRS REs when applicable. Due to the availability of two NCCEs only, two aggregation levels are only supported. In all cases except UE search space with repetition one and two, all candidates are expected to use aggregation level 2 to provide better performance under deep coverage.

An important aspect of physical layer design for NB-IoT system is to keep the UE power consumption low. Consequently, the UE should turn on its receiver for as short periods of time and in as few occasions as possible during the day. One way to keep this period short is to reduce the DCI size in order to achieve NPDCCH transmissions with small payload and short transmission time. In the DCI design for MTC, this was already considered through various simplifications to reduce the number of DCI bits. The same principles are applied to the coverage modes in NB-IoT. Furthermore to reduce the complexity, it is agreed to target the same DCI format for uplink grant and downlink assignment, as well as different coverage levels. Thus, DCI messages can be carried by NPDCCH using payload size no more than 23 bits for both UL grant/DL assignments which in turn defines a new set of DCI formats. DCI format N0 aims to scheduling of NPUSCH in one UL cell with the essential information about repetition, resource assignment, coding and modulation, and HARQ handling. Format N1, which has the same size as format N0, is used for the scheduling of one NPDSCH codeword in one cell and random access procedure initiated by a NPDCCH order. Last, Format N2 is employed for paging. Here the contents only spans 14 bits with a too short but significantly repeated messages to respect the reachability of all UEs under all coverage conditions.

Finally, DL transmissions to UEs in poor coverage may require many repetitions and thereby block the DL for other UEs. One way to mitigate the risk for blocking is to introduce intermediate transmission gaps at well-defined time instants during long DL transmissions. During these gaps the scheduler can transmit control and data information to other UEs. In our view, using a combination of transmission gaps and time division multiplexing between data and control scheduling allows NB-IoT to keep the basic DL scheduling unit in frequency as full band (i.e., 12 subcarriers).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

*6) **Narrowband Physical Downlink Shared Channel (NPDSCH)**:* To provide backward compatibility for in-band NB-IoT operation, downlink transmission with 15 kHz subcarrier spacing is required for all the modes of operation. For this reason, the NB-IoT downlink symbol duration, slot duration, and subframe duration are reused from legacy LTE. However, the NPDSCH processing has many updates to account for the reduced complexity, low power, and extended coverage targets. Fig. 8 shows the downlink transmitter processing for NB-IoT systems. There are couple of significant differences here. This includes the maximum supported TBS size, utilizing only Tail-Biting Convolutional Coding (TBCC) for channel coding, no HARQ processing, reduced modulation order, and applying repetition with the proper scrambling.

Indeed, due to the reduced bandwidth, the maximum TBS size for downlink NB-IoT is not expected to be greater than that in MTC (i.e. 1000 bits). If no fragmentation is allowed at physical layer, the stand-alone system in case of one Tx antenna with QPSK modulation can carry $2\times(12\times14-2\times4)=320$ bits in a single subframe which is too far from a realistic supported data rate when coding is considered. Also, many fragments would be required from the upper layers which introduce significantly low utilization due to the overhead. For these reason, a sensible option is to allow transmission of the data with fragmentation at physical layer. After rate matching, it was agreed that the transmitted block size is divided into N_F subframes which can be as maximum as 10. This enables the extension of the TBS size to be 680 bits as maximum for NB-IoT. Further, mapping a single transport block to multiple subframes would avoid a very high initial code rate.

Tail-Biting Convolutional Coding (TBCC) has replaced Turbo codes for simplicity. The main issue brought by this decision is the concern regarding any optimization towards the support of high code rates. The TBCC is known to provide less performance gain when compared to Turbo coding for high code rates. This is a non-essential feature whose introduction would negatively impact the reuse of existing LTE procedures thus incurring increased development cost and time-to-market. In fact, utilizing TBCC agrees with the understanding that NB-IoT payloads are generally small and in addition, for IoT applications requiring larger transport block sizes, LTE already provisions the MTC enhancements. Moreover, QPSK has been fully evaluated for coverage, capacity, latency and energy consumption, link level coexistence. It has been shown to fulfill the performance targets at low coverage modes. On the other hand, 16QAM has never been assumed for NB-IoT downlink to achieve the target SNR requirements with TBCC. For these reasons, QPSK has been selected to be the only supported modulation scheme for downlink NB-IoT and enhanced coverage MTC. However, it was agreed to leave 16QAM for further study in future releases.

To significantly reduce the complexity, only one HARQ process is supported for NB-IoT with no Redundancy Version (RV) reported. Actually, NB-IoT UEs are very likely to use low code rates in both the uplink and the downlink in order to support coverage extension, but RV is not shown to provide clear coding gains for low code rates (i.e., rate $\leq$1/3). Thus, for a single HARQ process, the benefits of RV (if any) can already be achieved by adaptive transmissions. In addition, if RV is introduced, the rate matching for TBCC for LTE will have to be changed specifically for NB-IoT, significantly reducing the synergy with LTE. This may add to the difficulty in supporting NB-IoT in some legacy LTE base stations.

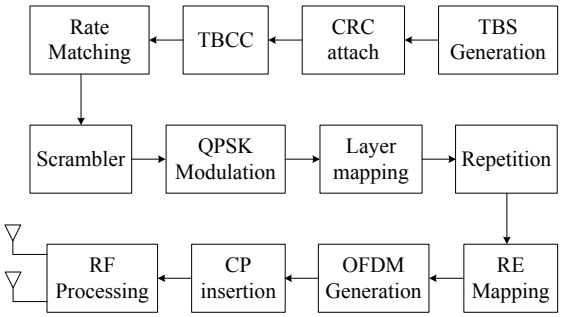

Fig. 8. Block diagram for the shared channel processing in NB-IoT systems.

Repetitions are proposed to be applied at subframe level. A maximum of 2048 repetitions are defined to support a target SNR of -12.6dB. Each repetition has a unique scrambling sequence based on the time stamp of the carrying subframe. This ensures a fully flexible support for mobility in addition to the peak to average power variations. Similar to NPDCCH, the NPDSCH is mapped to entire subframes (i.e., multiple NPDSCHs are multiplexed in a Time Division Multiplexing (TDM) manner). Contiguous and non-contiguous resource allocations can be considered to trade-off latency with inter-user blocking especially in the extreme coverage case. DL gaps are defined for NPDSCH to reduce the blocking probability for UE users in deep coverage on the account of the user in good coverage environments.

C. Uplink Physical Channels

Similar to MTC systems, in NB-IoT systems, a UE initially estimates its coverage level based on a path-loss estimate and use an NPRACH preamble according to its estimated coverage level. NPUSCH is initially set-up according to the UE's estimated coverage level. However, if the network determines that the UE's path-loss estimate is poor, the network can reconfigure a UE to a different NPUSCH coverage level based on the eNodeB measurements of the uplink signal characteristics. This is actually a fundamental update happening to the NB-IoT when compared to MTC [62][63]. To reduce complexity and power consumptions, the UE is no longer asked to report local channel quality indication. For this reason, the functionality of the uplink control channel becomes very thin and it actually reduces to only sending ACK/NACK. Indeed, this task can be easily handled by the usual data channel and hence no dedicated control channel is defined for NB-IoT. Two uplink physical channels are only supported for NB-IoT, namely the Narrowband Physical Random Access Channel (NPRACH) and the Narrowband Physical Uplink Shared Channel (NPUSCH).

Since UEs in extreme coverage are power limited and their performance is sensitive to power amplifier efficiency, a single tone transmission is desirable to achieve a Peak-to-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

Average Power Ratio (PAPR) that is close to 0dB irrespective of their coupling loss. Indeed, the 3GPP standardization body has established various studies from independent companies to evaluate and validate the NB-IoT system numerology. A summary of the evaluation is presented in [64]. The results have considered the performance aspects, the capacity, the modes of operation, the UE complexity, the UE battery life or power consumption, the coverage, and the cell size. After analysing the tradeoff, it has been agreed that a single tone transmission is supported for uplink NB-IoT systems whether by utilizing 15KHz or 3.75KHz as a subcarrier spacing. This is an interesting feature for NB-IoT in the uplink side that would require significant revisions to the uplink frame structure and various channel processing. It is worth to mention that the NB-IoT UE support for single carrier is mandatory. However, the support of the legacy multi-tone transmission can be indicated by the UE during the random access procedure.

*1) **Narrowband Physical Random Access Channel (NPRACH)**:* The random access procedure starts with random access preamble transmission from the UE to eNodeB [65]. To achieve enhanced coverage in NB-IoT system, the LTE-MTC procedure has been partially adopted. The main difference is the information about the time/frequency resources allocated for NPRACH. Thus, in general, a small number of PRACH coverage levels is defined and the PRACH coverage enhancement is achieved through repetition. Different coverage levels correspond to different NPRACH resources (i.e., different time resources, different frequency resources, preamble set, and repetition factors) and the available resources are signalled in system information messages [66]. The UE selects the initial NPRACH coverage level and associated NPRACH resource set based on its own DL measurement such as the Reference Signal Received Power (RSRP) measurement [67]. The eNodeB can get a rough estimate of the UE coverage level by observing the NPRACH coverage level for the successful NPRACH preamble transmission. If the UE fails to access the network after the maximum number of attempts at the highest NPRACH repetition level, the UE should stop further attempts at the highest NPRACH repetition level and report the failure to higher layers.

Indeed, there exist various design tradeoffs in choosing the subcarrier spacing for the single tone frequency hopping NPRACH. For example, for a given configured NPRACH bandwidth, the larger the subcarrier spacing, the smaller the number of subcarriers. Since different single tone frequency hopping NPRACH preambles are effectively separated in the frequency domain, using smaller subcarrier spacing implies a higher number of available preambles. On the other hand, utilizing larger subcarrier spacing may help improve the time-of-arrival estimation performance at the eNodeB and is less sensitive to carrier frequency offset in the uplink. Since the later issue is attached to eNodeB complexity not the UE side, it has been agreed to utilize the smallest possible subcarrier spacing, namely 3.75KHz, as the only mode of operation for NPRACH [68]. With the limited 180KHz bandwidth, this choice results in up to 48 different preambles from the frequency allocation perspective.

To reduce the overhead, four symbols are combined and

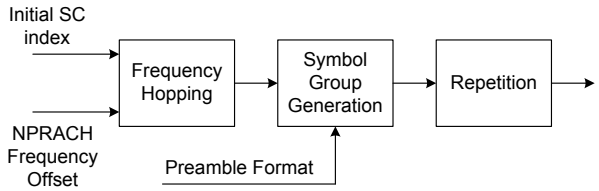

Fig. 9. Block diagram for the uplink random access channel processing in NB-IoT systems. The transmission for NPRACH is applied only to 3.75KHz subcarrier spacing mode.

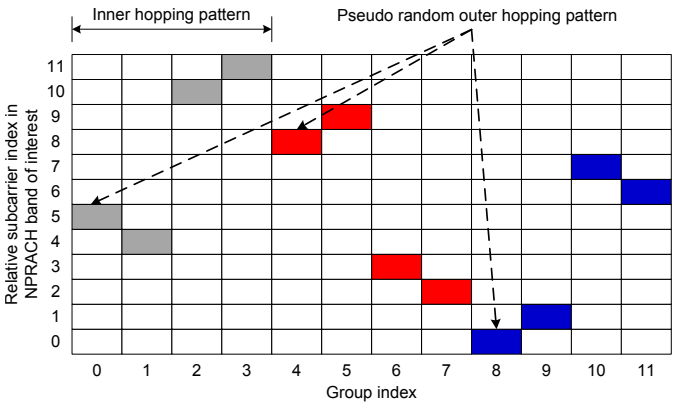

Fig. 10. Illustration for frequency hopping pattern in NPRACH. fixed inner hopping pattern within 4 groups is applied while pseudo random shift is applied as an outer hopping sequence.

only a single cyclic prefix is added [54]. The symbols and the CP constitute the new introduced concept of symbol groups. The preamble consists of one symbol in time and occupies only one tone in the frequency domain with 3.75KHz subcarrier spacing. However, the NPRACH transmission dynamically hops from one tone to another within 12 adjacent subcarriers. Within the available 48 subcarriers, a subset of these subcarriers $\mathrm{N_{sc}^{NPRACH}}$ is defined for a given cell to be the active NPRACH frequency resources. In addition, an offset parameter is introduced to point to the first subcarrier allowed for this cell. To select the initial subcarrier index prior to hopping, the UE randomly selects a subcarrier index for NPRACH within $\mathrm{N_{sc}^{NPRACH}}$, adds the initial cell specific offset to the selected number, and then use the resulting modulo-sum as the starting subcarrier index for the hopping process. Actually, the number of allowed NPRACH frequency resources (i.e., $\mathrm{N_{sc}^{NPRACH}}$) has been partitioned into two sets, where the subcarrier indices falling within the second set indicate that the UE supports multi-tone transmission for the RAR in addition to the default single-tone mode. Thus, the UE has to be careful with the subcarrier set from which the random number is chosen based on its transmission capabilities. Fig. 9 shows the block diagram of the NPRACH transmitter at the UE side with the three main blocks: the hopping support, the group symbol generation, and repetition. Two preamble formats with different sequence lengths are provided for NB-IoT system. As usual, the preamble format is selected based on the channel conditions and coverage level.

Frequency hopping is essential for NPRACH in order to facilitate the Time of Arrival (ToA) estimation at the eN-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

odeB from which a time advance is reported to the UE so that synchronization is achieved. To provide large ToA range (i.e., large cell sizes) and accurate ToA estimation, a two layer hopping pattern is utilized for NPRACH [69]. The inner hopping is chosen to be fixed for simplicity and small to provide large ToA range. Indeed, hopping is applied among four symbol groups with a fixed pattern to ensure a ToA estimation range of about 8km cell size when utilizing 3.75KHz subcarrier spacing. On the other hand, an output hopping layer is employed to enhance the ToA estimation accuracy. For this layer, a pseudo random hopping pattern in reused from the legacy PUSCH hopping. A cell specific random pattern is utilized to mitigate the cell interference. Without pseudo random hopping, the NPRACH transmissions in one cell may cause persistent interference to the NPRACH and/or NPUSCH transmissions in the neighbouring cells. In addition, an NPRACH capacity reduction is expected due to the fact that neighbouring cells configure different frequency resources for NPRACH to avoid inter-cell interference. This reduction can be somehow compensated if random hopping is applied. Last, the pseudo random nature of the outer hopping introduces flexibility to the NPRACH assignments. Indeed, a single cell may configure different NPRACH bandwidths not just a single number of active subcarriers, $\mathrm{N_{sc}^{NPRACH}}$. NPRACH transmission with one-level fixed hopping plus additional pseudo random hopping can be readily scaled as the bandwidth increases [63]. Fig. 10 shows one example to illustrate the frequency hopping feature for the NPRACH channel.

*2) **Narrowband Physical Uplink Shared Channel (NPUSCH)**:* Due to the introduction of the single carrier 3.75KHz mode, the symbol period has been expanded to four times its original value. Accordingly, the frame structure for uplink NB-IoT system has been revised. Indeed, for NPUSCH in 3.75KHz mode, the radio frame consists of only 5 slots numbered from 0 to 4 where each slot spans 2msec period. The subframe concept is dropped in this case and only slot handling is considered. The slot still consists of 7 SC-FDMA symbols such that the OFDM symbol length becomes 512 samples when sampled at 1.92MHz. Unlike the classical LTE system for Normal CP type, the cyclic prefix length for NPUSCH in 3.75KHz mode has a uniform period of 16 samples [62]. Thus, the remaining 144 samples within the slot, when compared to the legacy 960 samples slot period, are left as guard time to accommodate for a possible collision with any sounding reference signal from the legacy LTE system.

The NPUSCH channel has two formats, namely Format 1 and Format 2 [63]. The first format is the conventional data transmission mode of the NPUSCH channel. However, the second format is dedicated to carry the control information represented in only ACK/NACK. It is mandatory for a UE to transmit both formats through a single-tone configuration. However, format 1 may be also transmitted through a multi-tone structure only when conventional 15KHz spacing is utilized and when the UE capabilities permit. In multi-tone scenario, there are three possible configurations to allocate the frequency subcarriers. Only 3, 6, or 12 subcarriers can be active during NPUSCH format 1 transmission. Indeed, the concept of subframe can be still used in this case because actually, in this mode, nothing has changed when compared to legacy LTE.

Table V
NPUSCH PARAMETERS IN NB-IOT SYSTEMS

NPUSCH Format	Δf	$\mathrm{N_{sc}^{RU}}$	$\mathrm{N_{slots}^{RU}}$	$\mathrm{N_{RU}}$	$\mathrm{Q_m}$	DMRS indices
1	3.75KHz	1	16	{1,2,3, 4,5,6, 7,8,10}	{1,2}	4
	15KHz	1	16			3
		3	8		2	
		6	4			
		12	2			
2	3.75KHz	1	4	1	1	0,1,2
	15KHz	1	4			2,3,4

To maintain compatibility and flexibility in the description for both 3.75KHz or 15KHz modes, the concept of Resource Unit (RU) is developed for NB-IoT NPUSCH to provide the essential framework for resource mapping [70]. A resource unit is defined to be $\mathrm{N_{symb}N_{slots}^{RU}}$ consecutive SC-FDMA symbols in the time domain and $\mathrm{N_{sc}^{RU}}$ consecutive subcarriers in the frequency domain, where $\mathrm{N_{symb}} = 7$ is the number of SC-FDMA symbols per slot. Similar to the downlink, fragmentation is allowed at the physical layer to segment the data packet into multiple units, namely $\mathrm{N_{RU}}$. As a special case, NPUSCH Format 2 always employs the smallest possible transmission unit to carry the ACK/NACK message (i.e., a single RU is utilized or $\mathrm{N_{RU}}$=1). Table V summarizes the different parameters for NPUSCH under different supported modes.

In case of Format 1, the transport block size is selected based on modulation, coding, and the assigned number of sub-carriers per symbol whenever multi-tone transmission is considered. After Cyclic Redundancy Check (CRC) attachment, the code block is encoded. Turbo coding and rate matching schemes in legacy LTE have been reused for NPUSCH [55], because it provides significantly higher coding gain than convolutional coding. Although the decoding complexity of turbo coding is higher than that of convolutional coding, the decoding is performed at the eNodeB side, where high complexity is considered acceptable. During rate matching, the number of available RUs is assumed. One HARQ process for dedicated transmissions is supported for uplink. To minimize the downlink signalling overhead, it has been approved that only two RVs, namely 0 and 2, are supported for NPUSCH. Due to the wide variation of the transmission duration between different coverage levels, it is hard to fix the time interval between first transmission and re-transmission. Consequently, asynchronous HARQ is utilized. However, after $\mathrm{M_{identical}}$ codeword transmissions, the RV index is toggled within the same packet transmission if repetition is enabled, where $\mathrm{M_{identical}} = \min(4, \mathrm{N_{Rep}})$ and $\mathrm{N_{Rep}}$ is the repetition count [63].

After modulation, repetitions are applied at slot/subframe level. The number of supported repetitions for NPUSCH are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

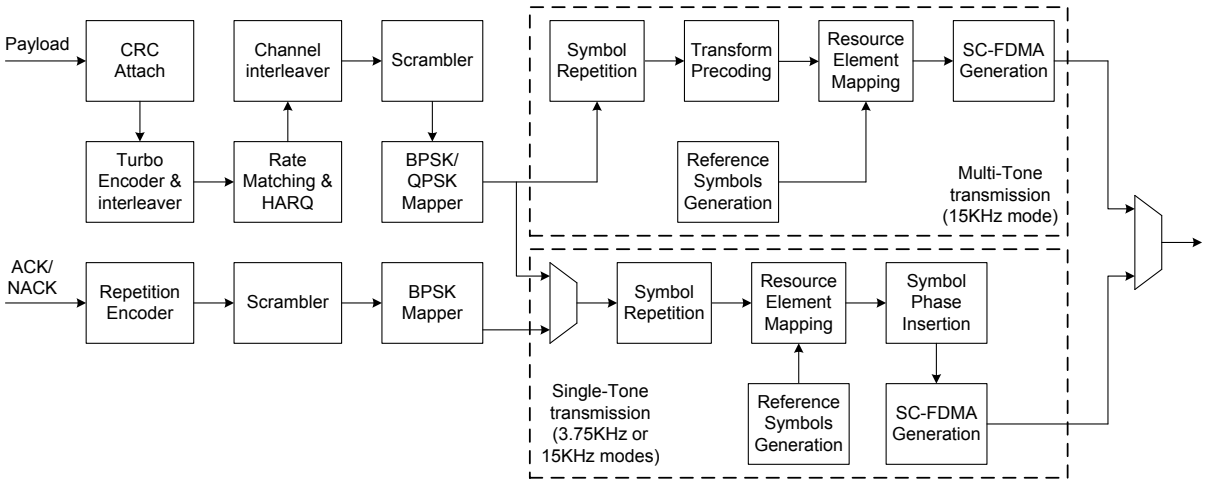

Fig. 11. Block diagram for the uplink shared channel processing in NB-IoT systems.

{1, 2, 4, 8, 16, 32, 64, 128}, where the repetition count is indicated in the DCI [70]. The repeated slots are then transmitted over a single-tone chain or a multi-tone chain. It was agreed that QPSK and BPSK are supported for single-tone NPUSCH transmission where phase rotation is introduced to reduce PAPR and out-of-band emission. To obtain the benefits, phase rotation should be implemented in a contiguous way at symbol level including both data symbol and DMRS symbols. On the contrary, the multi-tone processing follows the conventional process of employing a transform precoder to support SC-FDM, a resource element mapper to fill the time-frequency grid with the proper resource elements, and finally synthesize the time domain baseband signal by utilizing the SC-FDMA generation block. The detailed block diagram for the NPUSCH is shown in Fig. 11.

In [71], simulations were performed to investigate the link level performance of NPUSCH assuming different DMRS densities. Results show that by increasing the DMRS density from 1 symbol per slot (i.e. the same as in legacy LTE) to 2 symbols per slot, the block error rate performance is only improved by 0.5 dB for low mobility channel. The gain cannot even compensate for the loss due to the decrease of data symbol density from 6 to 5 per slot. In fact, the target Mutual Coupling Loss (MCL) of 164dB [33] is comfortably met for NPUSCH by reusing the legacy LTE DMRS density. Hence, it was agreed that NPUSCH reuses the LTE uplink DMRS pattern for the 15 kHz subcarrier spacing. For the 3.75 KHz subcarrier spacing, a similar pattern as legacy LTE DMRS can be employed for DMRS. The little difference from legacy LTE DMRS is to avoid the possible collision between DMRS and LTE sounding signal.

In case of NPUSCH Format 2, the number of subcarriers available per RU is always 16. Therefore, the single bit representing ACK/NACK is encoded by a repetition code to 16 bits which are modulated by BPSK modulation [55]. When repetition is enabled, the symbols are mapped to the available consecutive $\mathrm{N}_{\mathrm{Rep}}^{\mathrm{AN}}$ resource units, where $\mathrm{N}_{\mathrm{Rep}}^{\mathrm{AN}}$ is the repetition factor for the ACK/NACK message. Of course, the ACK/NACK resource assignment is signalled to the UE through the DCI format N1. For both subcarrier spacings, the DMRS density is adopted from the legacy control channel Format 1/1a, which uses three DMRS symbols per slot.

VI. Implementation Challenges

A. Low Power Support

Battery longevity depends on how efficiently a device can utilize various idle and sleep modes that allow large parts of the device to be powered down for extended periods. The NB-IoT specification addresses the physical layer technology and idling aspects of the system. Like LTE, NB-IoT uses two main protocol states: IDLE and CONNECTED. In IDLE mode, devices save power, and resources that would be used to send measurement reports and uplink reference signals are freed up. In CONNECTED mode, devices can receive or send data directly. Discontinuous reception (DRX) is the process through which networks and devices negotiate when devices can sleep and can be applied in both IDLE and CONNECTED modes. For CONNECTED mode, the application of DRX reduces the number of measurement reports devices send and the number of times downlink control channels are monitored, leading to battery savings. 3GPP R12 supports a maximum DRX cycle of 2.56 seconds, which has been extended to 10.24 seconds in R13 (eDRX). However, any further lengthening of this period is as yet not feasible, as it would negatively impact a number of RAN functions including mobility and accuracy of the system information. In IDLE mode, devices track area updates and listen to paging messages. To set up a connection with an idle device, the network pages it. Power consumption is much lower for idle devices than for connected ones, as listening for pages does not need to be performed as often as monitoring the downlink control channel.

Compared with legacy LTE, the link budget of NB-IoT has a 20dB margin, and use cases tend to operate with lower data rates. The coverage target of NB-IoT has a link budget of 164dB, whereas the current LTE is 142.7 dB. The 20dB improvement corresponds to a sevenfold increase in coverage area for an open environment, or roughly the loss that occurs when a signal penetrates the outer wall of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

a building. Standardization activities in 3GPP have shown that NB-IoT meets the link budget target of 164dB, while simultaneously meeting the M2M application requirements for data rate, latency, and battery life.

B. Low Cost Support

NB-IoT devices support reduced peak physical layer data rates: in the range of 100-200kbps or significantly lower for single-tone devices. To facilitate low-complexity decoding in devices, turbo codes are replaced with convolutional codes for downlink transmissions, and limits are placed on maximum transport block size (which is 680 bits for DL and 1000 bits for UL). The performance requirements set for NB-IoT make it possible to employ a single receiver antenna. As a result, the radio and baseband demodulator parts of the device need only a single receiver chain. By operating NB-IoT devices in half duplex so that they cannot be scheduled to send and receive data simultaneously, the duplex filter in the device can be replaced by a simple switch, and only a single local oscillator for frequency generation is required. In fact, these optimizations reduce cost and power consumption. At 200kHz, the bandwidth of NB-IoT is substantially narrower than other access technologies including LTE-MTC systems. The benefit of a narrowband technology lies in the reduced complexity of analog-to-digital conversion (ADC), digital-to-analog conversion (DAC), reduced number of HARQ processes, and subframe buffering. Since all physical channels utilize a unified transmission mode, channel estimation can be adopted for all subframes unlike LTE-MTC in which coherent decoding for the data channel requires a stand-alone channel estimation rather than the control channel one. All these features and others bring benefits in terms of low cost and low power consumption. NB-IoT brings about a significant design change in terms of the placement of the device's power amplifier (PA). Integrating this element directly onto the chip, instead of it being an external component, enables the cheaper single-chip modem implementations.

C. Challenges and Implementation Aspects

1) Initial Synchronization in CAT-M: From CAT-M perspective, in literature, there are various techniques presented to perform initial synchronization, cell search, frequency tracking, and typical chain decoding. During initial synchronization and cell search, all techniques [72][73][74][75][76][77] share the same procedure in the following order: (1) A coarse symbol timing has to be obtained first so that the received signal can be converted from time domain to frequency domain. At this stage, there are algorithms to estimate the fractional part of CFO as well [72][73]. (2) PSS (or sector ID) will be detected in the second step. (3) SSS (or cell ID group) will be found next [74][75][78]. (4) The detection of the integer part of CFO can be fulfilled. Some algorithms have been presented to enable this estimation within either Step 2 or Step 3 [76]. Other algorithms are based on different time domain approaches [77].

Since LTE-MTC introduces new challenges to the system represented in the limited degrees of freedom regarding the

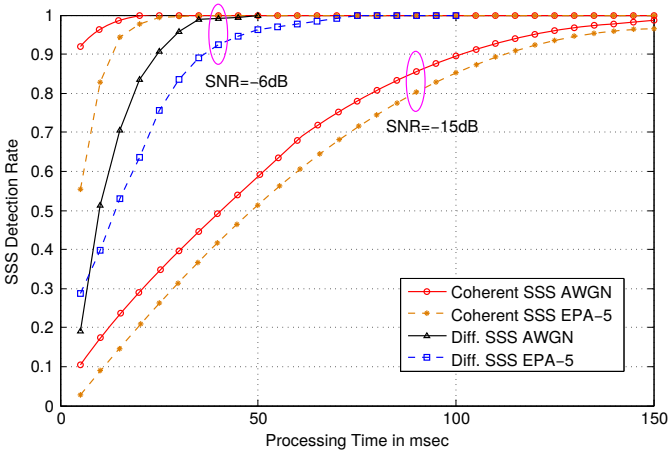

Fig. 12. Detection probability versus processing time for SSS under different detection techniques. Different channel conditions are considered with SNR=-6dB and -15dBs [79].

number of antenna ports and the operating SNR, conventional cell search and initial synchronization techniques have to be revised. One fundamental approach is defined in [79] by applying time-averaging over different decision statistics to enhance the accuracy of the legacy techniques. For example, Fig. 12 shows the coherent SSS detection (where the channel state information is assumed to be known) versus the differential SSS detection for the legacy LTE under different averaging periods. It is clear that detection accuracy can be enhanced by increasing the averaging period. However, high Doppler effects have not been addressed. Research efforts are encouraged in this direction to provide innovative low-cost solutions for this harsh environment.

2) Frequency Tracking in CAT-M: Even after the initial synchronization stage, frequency tolerance is always present due to the Doppler shift and uncompensated residual errors, hence frequency tracking is required. As an OFDM system, legacy LTE systems can employ the conventional Maximum-Likelihood estimation and compensation loops for the frequency tracking [80][81][82]. Two issues arise with the introduction of LTE-MTC: (1) During EDRX cycles, frequency tracking is deactivated and DRX wake-up procedure requires re-synchronization. (2) Enhanced coverage UEs are required to track frequency errors in very low SNR regimes. A new challenge is then introduced to keep tracking loops with high accuracy at these low SNRs. In this environment, the legacy techniques can be inefficient and hence new approaches are also encouraged. As an initial solution, the authors in [83] have defined a frequency tracking approach through the repetitive nature of the broadcast channel mapping which is utilized basically for the enhanced coverage support. However, the most recent specifications left it open for the broadcast repetition to be cell-specific feature. That is, broadcast channel repetition may not be employed at least for 1.4MHz cell.

3) Channel Estimation in CAT-M: When it comes to various chain processing, channel estimation and equalization are the main challenges for LTE-MTC systems. Conventionally, in LTE systems, reference signals are inserted within the transmitted signal to assist the channel estimation process

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

which is required for coherent detection. Generally, several channel estimation schemes that vary in their complexity and performance have been presented [84], [85]. A 2-D Minimum-Mean Squared Error (MMSE) channel estimation technique has been introduced in [86]. However the proposed channel estimation technique depends on the knowledge of the channel statistics and the operating SNR which are usually unknown. A robust MMSE channel estimation technique has been introduced in [85], [86] in order to remove the dependency on the exact channel statistics. In this case, filter coefficients are calculated based on worst-case channel conditions and are used in the estimation process at the expense of minor performance degradation. Another simple estimation scheme can be used for systems that have uniformly distributed pilots, and where pilot separation satisfies the sampling theory conditions. In this case, an ideal low-pass filter can be used in order to reconstruct the original signal from its samples [87]. Again, the performance measures for these techniques have been designed and optimized for the legacy operating SNR values and under the assumption that high speed channels are totally supported. Conversely, LTE-MTC would require special treatment to maintain enough performance at low complexity and deep coverage conditions.

It is to be noted that, special reference signal is attached to the new introduced MPDCCH channel to help pilot-aided channel estimation techniques. In [88], the channel power-delay profile is approximated to be only described by the mean delay and the root-mean-square delay spread. A Linear MMSE filter is introduced to estimate those parameters for the LTE Multi-Input Multi-Output (MIMO) system where the user specific pilot pattern (i.e., the same pilot structure utilized by MPDCCH) is employed. The main issue with this approach is the complexity. For the same pilot structure, an iterative 2-D MMSE channel estimation method is considered in a multi-user environment [89]. The approach aims not only to cancel the interference effect, but also to enhance the channel estimates iteratively by introducing a mean-square error criterion after each iteration. Again, the technique was not designed for a single user downlink reception purpose and it is somehow complex. To the best of the authors knowledge, practical channel estimators for MPDCCH have not been addressed. One can guess that such process has been addressed before and no revisions are required since the DMRS structure for MPDCCH is inherited from the classical EPDCCH channel [88][90]. However, there are couple of challenges introduced to MPDCCH that would require this revision. (1) The operating SNR for MPDCCH has been reduced to -15dBs. (2) Repetition is supported for MPDCCH and hence channel estimators quality can be enhanced. (3) The channel estimator has to consider frequency hopping. (4) Complexity is a real issue for MTC framework, thus reduced complexity is essential for the channel estimators. For these reasons, channel estimation for MPDCCH requires a revision and new proposals.

4) Synchronization and Frequency Tracking of NB-IoT: NB-IoT intends to occupy a narrow bandwidth of only 200KHz, which is not backward compatible to the supported bandwidths by the legacy LTE [61]. During initial synchronization, carrier frequency offset (CFO) is estimated and compensated to enable proper signal detection. The UE acquires the cell ID by employing the cell search procedure. To cope with these changes, NB-IoT employs new set of synchronization signals, namely NPSS and NSSS. The new sequences have different bandwidth, mapping, periodicity, and generation when compared to the legacy LTE synchronization signals. Unlike conventional LTE, cell ID is encapsulated only in the secondary sequence without involving the primary sequence. One of the challenges is to acquire the initial timing, frequency acquisition, and efficiently search for the serving cell ID. Although it looks straightforward to apply cross-correlation with the known reference for these detection hypothesis, the detection performance and complexity are the main challenges for such algorithms especially under low SNR and various channel conditions [91]. To highlight the issue, we have simulated the NB-IoT system to detect the cell ID under perfect synchronization environment. Differential cross-correlation is employed to reduce the effect of the channel. However, Fig. 13 shows a significant degradation in the detection performance when the Channel State Information (CSI) is available, even with decision statistic averaging across M windows or radio frames.

One more challenge is to maintain the UE in synchronization with the eNodeB at very low SNR regimes. There are two aspects for this issue. First, the basic cell search may encounter a loss in detection. Since the NSSS sequence, that carries the Cell ID information, spreads across consecutive OFDM symbols, the effect of the fractional frequency offset has to be carefully investigated. For example, with only 1KHz frequency offset and subcarrier spacing of 15KHz, the phase over one slot (i.e., 960 samples at 1.92MSamples/sec rate) would change by $2\pi \times 960 \times (1/15)/128 = \pi$, meaning that all NSSS subcarriers contained by the second slot will experience a flipped sign when compared to the original transmitted sequence. This will certainly reduce the detection accuracy. Therefore, a special attention has to be paid for the synchronization assumptions for cell search and data decoding. Second, when compared to legacy LTE, the number of reference symbols for DL NB-IoT is insufficient to utilize the conventional pilot-based frequency tracking mechanisms [82]. Furthermore, the repetition structure for the mapped symbols are performed on the subframe level unlike MTC in which the broadcast channel mapping has a repetitive structure. This MTC PBCH repetitive structure enables the differential phase to track the frequency offset and hence maintain the UE in synchronization [83]. On top of that, the NB-IoT system supports a multi-carrier operation in which the eNodeB can dynamically switch NB-IoT UE to another band in which neither NPSS nor NSSS is present. In this case, reference signals are the only data aided symbols to be utilized for synchronization. Research effort is encouraged to investigate such an issue.

5) Channel Estimation in NB-IoT: Although the main theme of the NB-IoT devices to be stationary due to the significant reduced MCL requirements, the specifications left it open for the vendors to support mobility with high Doppler spread [63]. It is unforgotten that even with good coverage NB-IoT UE from the power perspective, the UE losses both

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2017.2728013, IEEE Communications Surveys & Tutorials

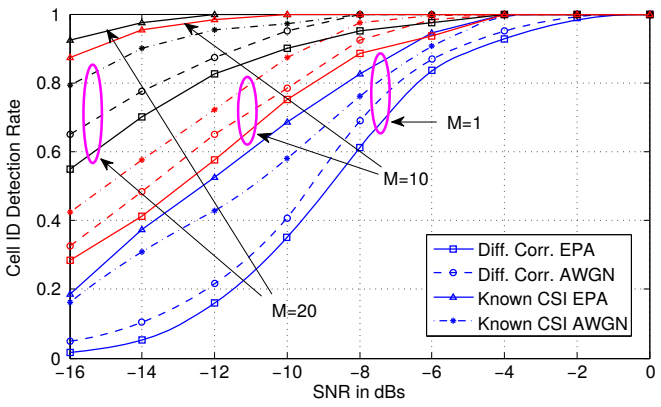

Fig. 13. Simulation for the cell detection for NB-IoT system for two scenarios and under different fading conditions. A differential cross-correlation is compared to a direct correlation with known CSI. Various averaging windows are utilized to show the effect of averaging on the decision statistics.

frequency and spatial diversities due to the reduced cost and reduced bandwidth features. Therefore, channel estimation algorithms have to be revised to provide reasonable performance at very low SNR values while supporting mobility. Indeed, it is always the tradeoff between performance and complexity to design such channel estimation algorithm. However, in NB-IoT, reduced complexity is a key target and hence the compromise has to be carefully investigated and analysed.

VII. IoT and Future Directions

A. Air Interface Scalability

As MTC and IoT require supporting tens of thousands of connected devices in a single cell, LTE cellular networks should explore new avenues of research and development, such as massive MIMO [92][93] to help the network air interface to accommodate such increased number of connections. In essence, massive MIMO is an evolving technology resulting from up-scaling the traditional MIMO systems. In massive MIMO system, large-size arrays can serve a massive number of user terminals using spatial multiplexing [94]. As one of the most promising ingredients of the emerging 5G technology, massive MIMO is a commercially attractive solution since a hundred-fold higher capacity is possible with the same number of base stations. Such gain is made possible due the recent advances in directional beamforming with low power, and flexible beam adjusting with low peak-to-average power ratio in MIMO-OFDM systems [95][96][97][98].

However, some challenges are associated with such increase in number of antennas is case of MTC. For example, when large number of UEs are very close to each other, the system cannot render such highly correlated channel vectors as orthogonal which will affect the massive MIMO performance, therefore, user-scheduling algorithms should be aware of such fact.

Moreover, inexpensive and low-power components still need more investigations to build such massive MIMO [92]. Channel state information, associated with large number of antennas for massive MIMO systems and coordination among different UEs induces a huge amount of information exchange overhead and affects the UE power consumption and complexity. The efficiency of multicasting with massive MIMO, in non-cooperative setups, is also a limiting factor [99]. As the number of base station antennas increases the number of the channel estimates also increases for each terminal, which in turn needed hundred times more uplink slots to feedback the channel responses to the base station [100].

B. 5G enabling Technologies

Despite the spent effort to enhance and optimize the current networks and their interfaces to accommodate the increasing demand of IoT applications, other directions should be explored to provide alternative technologies to enable the 5G. For example, all the current communication systems use bi-directional communications without time or frequency duplex which limits the capabilities of the devices. Full-Duplex breaks such barrier by transmitting and receiving at the same time and on the same frequency, introducing the potential of doubling the system capacity and reducing the system delay. Also, the current multiple access techniques schedule the users on orthogonal channels i.e. different time and/or frequency which greatly limits the system capacity. A newly proposed technique that can overcome this limitation is the nonorthogonal multiple access (NOMA). Such new techniques can benefit the development process of new radio access for the next generation networks.

VIII. Conclusion

The new applications introduced by the IoT framework forced new challenges on the existing cellular technologies. While such technologies are initially designed to support human-generated traffic, new designs are proposed to accommodate for the emerging machine-generated traffic which has different characteristics. In this paper, we addressed in details the development on the LTE to support MTC and IoT. New UE categories has to be introduced to support the new requirements of each system, namely, CAT-M and CAT-N. Each category has a distinct set of specifications and limitations. While traditional coverage enhancements techniques are not applicable in the new categories, the new alternatives have been discussed to extract diversity gain through time repetitions and frequency hopping. Some challenges to the implementation to support low cost and low power operations are also discussed.

References

[1] A. Ali, W. Hamouda, and M. Uysal, "Next generation M2M cellular networks: challenges and practical considerations," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 18–24, September 2015.

[2] V. Gazis, "A Survey of Standards for Machine to Machine (M2M) and the Internet of Things (IoT)," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, 2016.

[3] Z. Fan, R. J. Haines, and P. Kulkarni, "M2M communications for E-health and smart grid: an industry and standard perspective," *IEEE Wireless Commun.*, vol. 21, no. 1, pp. 62–69, February 2014.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[6] B. Panigrahi, H. K. Rath, R. Ramamohan, and A. Simha, "Energy and spectral efficient direct Machine-to-Machine (M2M) communication for cellular Internet of Things (IoT) networks," in *Int. Conference on Internet of Things and Applications*, Jan 2016, pp. 337–342.

[7] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 10–21, June 2011.

[8] M. Levesque, F. Aurzada, M. Maier, and G. Joos, "Coexistence Analysis of H2H and M2M Traffic in WiFi Smart Grid Communications Infrastructures Based on Multi-Tier Business Models," *IEEE Trans. Commun.*, vol. 62, no. 11, pp. 3931–3942, Nov 2014.

[9] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11AH: the WiFi approach for M2M communications," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 144–152, December 2014.

[10] T. Taleb and A. Kunz, "Machine type communications in 3GPP networks: potential, challenges, and solutions," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 178–184, March 2012.

[11] X. Xiong, K. Zheng, R. Xu, W. Xiang, and P. Chatzimisios, "Low power wide area machine-to-machine networks: key techniques and prototype," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 64–71, September 2015.

[12] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, 2017.

[13] W. Guibene, K. E. Nolan, and M. Y. Kelly, "Survey on Clean Slate Cellular-IoT Standard Proposals," in *2015 IEEE Int. Conf. on Computer and Information Technology; Ubiquitous Computing and Commun.; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Oct 2015, pp. 1596–1599.

[14] J. P. Bardyn, T. Melly, O. Seller, and N. Sornin, "IoT: The era of LPWAN is starting now," in *ESSCIRC Conf. 2016: 42nd European Solid-State Circuits Conf.*, Sept 2016, pp. 25–30.

[15] F. Ghavimi and H. H. Chen, "M2M communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 525–549, Secondquarter 2015.

[16] Sigfox. (2017). [Online]. Available: http://www.sigfox.com/

[17] LoRa. (2017). [Online]. Available: https://www.lora-alliance.org/What-Is-LoRa/Technology

[18] Semtech. (2017). [Online]. Available: http://www.semtech.com/

[19] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for lora technology," in *2015 14th Int. Conf. on ITS Telecommunications (ITST)*, Dec 2015, pp. 55–59.

[20] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the Internet of Things," in *2016 Int. Wireless Commun. and Mobile Computing Conf. (IWCMC)*, Sept 2016, pp. 439–444.

[21] T. PetriÄĞ, M. Goessens, L. Nuaymi, L. Toutain, and A. Pelov, "Measurements, performance and analysis of LoRa FABIAN, a real-world implementation of LPWAN," in *2016 IEEE 27th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, Sept 2016, pp. 1–7.

[22] P. Neumann, J. Montavont, and T. NoÃńl, "Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study," in *2016 IEEE 12th Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob)*, Oct 2016, pp. 1–8.

[23] Ingenu Tech. (2017) RPMA technology for the Internet of Things. [Online]. Available: http://theinternetofthings.report/Resources/Whitepapers/4cbc5e5e-6ef84455b8cdf6e3888624cb_RPMA%20Technology.pdf

[24] IEEE, "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (lr-wpans)–amendment 5: Physical layer specifications for low energy, critical infrastructure monitoring networks." *IEEE Std 802.15.4k-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, and IEEE Std 802.15.4j-2013)*, pp. 1–149, Aug 2013.

[25] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios," *IEEE Wireless Commun.*, vol. 23, October 2016.

[26] T. Myers, D. Werner, K. Sinsuan, J. Wilson, S. Reuland, P. Singler, and M. Huovila, "Light monitoring system using a random phase multiple access system," Jul. 2 2013, uS Patent 8,477,830. [Online]. Available: https://www.google.com/patents/US8477830

[27] S.-Y. Lien, K.-C. Chen, and Y. Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 66–74, 2011.

[28] E. Soltanmohammadi, K. Ghavami, and M. Naraghi-Pour, "A Survey of Traffic Issues in Machine-to-Machine Communications over LTE," *IEEE Internet Things J.*, vol. PP, no. 99, pp. 1–1, 2016.

[29] A. Rico-Alvarino, M. Vajapeyam, H. Xu, X. Wang, Y. Blankenship, J. Bergman, T. Tirronen, and E. Yavuz, "An overview of 3GPP enhancements on machine to machine communications," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 14–21, June 2016.

[30] 3GPP, "Standarization of Machine-type Communications," 3rd Generation Partnership Project, Tech. Rep. V0.2.4, June 2014.

[31] A. Rajandekar and B. Sikdar, "A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 175–186, April 2015.

[32] S. Chen, S. Sun, Y. Wang, G. Xiao, and R. Tamrakar, "A comprehensive survey of TDD-based mobile communication systems from TD-SCDMA 3G to TD-LTE(A) 4G and 5G directions," *China Commun.*, vol. 12, no. 2, pp. 40–60, Feb 2015.

[33] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *IEEE Wireless Commun. and Networking Conference Workshops*, April 2016, pp. 428–432.

[34] M. Wang, J. Zhang, B. Ren, W. Yang, J. Zou, M. Hua, and X. You, "The Evolution of LTE Physical Layer Control Channels," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1336–1354, Secondquarter 2016.

[35] C. Shahriar, M. L. Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, Firstquarter 2015.

[36] G. Ku and J. M. Walsh, "Resource Allocation and Link Adaptation in LTE and LTE Advanced: A Tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1605–1633, thirdquarter 2015.

[37] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013.

[38] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 4–16, First 2014.

[39] N. Abu-Ali, A. E. M. Taha, M. Salah, and H. Hassanein, "Uplink scheduling in LTE and LTE-Advanced: Tutorial, Survey and Evaluation Framework," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1239–1265, Third 2014.

[40] F. Capozzi, G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, "Downlink Packet Scheduling in LTE Cellular Networks: Key Design Issues and a Survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 678–700, Second 2013.

[41] M. A. Mehaseb, Y. Gadallah, A. Elhamy, and H. Elhennawy, "Classification of LTE Uplink Scheduling Techniques: An M2M Perspective," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1310–1335, Secondquarter 2016.

[42] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," *IEEE/ACM Trans. Netw.*, vol. 21, no. 6, pp. 1960–1973, Dec 2013.

[43] X. Jian, X. Zeng, Y. Jia, L. Zhang, and Y. He, "Beta/m/1 model for machine type communication," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 584–587, March 2013.

[44] M. S. Ali, E. Hossain, and D. I. Kim, "LTE/LTE-A random access for massive machine-type communications in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 76–83, January 2017.

[45] M. Laner, P. Svoboda, N. Nikaein, and M. Rupp, "Traffic models for machine type communications," in *ISWCS 2013; 10th Int. Symp. on Wireless Communication Systems*, Aug 2013, pp. 1–5.

[46] 3GPP-TR, "Study on ran improvements for machine-type communications (release 11)," Technical specification group radio access network, Tech. Rep. 37.868, 2011.

[47] A. Laya, C. Kalalas, F. Vazquez-Gallego, L. Alonso, and J. Alonso-Zarate, "Goodbye, aloha!" *IEEE Access*, vol. 4, pp. 2029–2044, 2016.

[48] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of lte and lte-a suitable for m2m communications? a survey of alternatives," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 4–16, First 2014.

[49] J. Choi, "On the adaptive determination of the number of preambles in rach for mtc," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1385–1388, July 2016.
[50] S. Dama, T. V. Pasca, V. Sathya, and K. Kuchi, "A novel rach mechanism for dense cellular-iot deployments," in *2016 IEEE Wireless Commun. and Networking Conf.*, April 2016, pp. 1–6.
[51] M. Vilgelm, H. M. GÃijrsu, W. Kellerer, and M. Reisslein, "Latmapa: Load-adaptive throughput- maximizing preamble allocation for prioritization in 5g random access," *IEEE Access*, vol. 5, pp. 1103–1116, 2017.
[52] D. Flore. (2015, Feb) Evolution of LTE in Release 13. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1628-rel13
[53] J. Gozalvez, "New 3GPP Standard for IoT [Mobile Radio]," *IEEE Veh. Technol. Mag.*, vol. 11, no. 1, pp. 14–20, March 2016.
[54] Ericsson, "Introduction of NB-IoT," 3GPP TSG RAN WG1 Meeting-85, Tech. Rep. R1-165971, May 2016.
[55] Huawei and HiSilicon, "Introduction of Rel-13 feature of NB-IoT in 36.212," 3GPP TSG RAN WG1 Meeting-85, Tech. Rep. R1-166045, May 2016.
[56] M. Hua, M. Wang, K. W. Yang, and K. J. Zou, "Analysis of the frequency offset effect on zadoff-chu sequence timing performance," *IEEE Trans. Commun.*, vol. 62, no. 11, pp. 4024–4039, Nov 2014.
[57] J. Hu, M. Wang, K. J. Zou, K. W. Yang, M. Hua, and J. Zhang, "Enhanced lte physical downlink control channel design for machine-type communications," in *2015 7th Int. Conf. on New Technologies, Mobility and Security (NTMS)*, July 2015, pp. 1–5.
[58] M. Wang, W. Yang, J. Zou, B. Ren, M. Hua, J. Zhang, and X. You, "Cellular machine-type communications: physical challenges and solutions," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 126–135, April 2016.
[59] J. Lorca, "Increasing coverage and maximum CFO in DFT-s-OFDM for Machine-Type Communications," in *Int. Conf. on Commun.*, 2015, pp. 982–987.
[60] Y. E. Wang *et al.*, "A Primer on 3GPP Narrowband Internet of Things (NB-IoT)," *CoRR*, vol. abs/1606.04171, 2016.
[61] Motorola Mobility, "Introduction of NB-IoT," 3GPP TSG RAN WG1 Meeting-85, Tech. Rep. R1-165111, May 2016.
[62] MCC Support, "Final Report of 3GPP TSG RAN WG1-84 v2.0.0," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-163406, April 2016.
[63] ——, "Final Report of 3GPP TSG RAN WG1-85 v1.0.0," 3GPP TSG RAN WG1 Meeting-85, Tech. Rep. R1-166056, Aug 2016.
[64] Huawei and HiSilicon, "Summary of NB-IoT evaluation results," 3GPP TSG RAN WG1 Meeting-83, Tech. Rep. R1-157741, Nov 2015.
[65] Nokia Networks, Alcatel-Lucent, and Alcatel-Lucent Shanghai Bell, "Random Access Procedure for NB-IoT," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160458, Feb 2016.
[66] Sony, "NB-PRACH Coverage Levels," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160768, Feb 2016.
[67] Ericsson, "Introduction of NB-IoT," 3GPP TSG RAN WG1 Meeting-85, Tech. Rep. R1-165973, May 2016.
[68] Intel Corporation, "NB-PRACH and random access procedure," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160415, Feb 2016.
[69] Huawei, HiSilicon, and Neul, "NB-PRACH design," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160316, Feb 2016.
[70] Intel Corporation, "NB-PUSCH design and scheduling," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160414, Feb 2016.
[71] Huawei and HiSilicon, "NB-PUSCH design," 3GPP TSG RAN WG1 Meeting-84, Tech. Rep. R1-160325, Feb 2016.
[72] J.-J. van de Beek, M. Sandell, and P. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Signal Process.*, vol. 45, no. 7, pp. 1800–1805, 1997.
[73] S. Ma, X. Pan, G.-H. Yang, and T.-S. Ng, "Blind Symbol Synchronization Based on Cyclic Prefix for OFDM Systems," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1746–1751, 2009.
[74] I. Kim, Y. Han, and H. K. Chung, "An efficient synchronization signal structure for OFDM-based cellular systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 99–105, 2010.
[75] Y. Tsai, G. Zhang, D. Grieco, and F. Ozluturk, "Cell search in 3GPP long term evolution systems," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 23–29, 2007.
[76] K. Manolakis, D. Gutierrez Estevez, V. Jungnickel, W. Xu, and C. Drewes, "A Closed Concept for Synchronization and Cell Search in 3GPP LTE Systems," in *IEEE Wireless Commun. and Networking Conf.*, 2009, pp. 1–6.
[77] H. Setiawan and H. Ochi, "A low complexity physical-layer identity detection for 3GPP Long Term Evolution," in *Int. Conf. on Advanced Communication Technology*, vol. 1, 2010, pp. 8–13.
[78] C.-C. Liao, P.-Y. Tsai, and T.-D. Chiueh, "Low-Complexity Cell Search Algorithm for Interleaved Concatenation ML-Sequences in 3GPP-LTE Systems," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 280–283, 2012.
[79] A. Ali and W. Hamouda, "Cell search evaluation: A step towards the next generation LTE-MTC systems," in *2016 IEEE Wireless Commun. and Networking Conf.*, April 2016, pp. 1–6.
[80] W. Xu and K. Manolakis, "Robust Synchronization for 3GPP LTE system," in *IEEE Global TeleCommun. Conf.*, 2010, pp. 1–5.
[81] K. Guo, W. Xu, and G. Zhou, "Differential Carrier Frequency Offset and Sampling Frequency Offset Estimation for 3GPP LTE," in *IEEE Veh. Tech. conf.*, May 2011, pp. 1–5.
[82] F. Classen and H. Meyr, "Frequency synchronization algorithms for OFDM systems suitable for communication over frequency selective fading channels," in *IEEE Veh. Tech. conf.*, Jun 1994, pp. 1655–1659 vol.3.
[83] A. Ali and W. Hamouda, "Employing Broadcast Channel for Frequency Tracking in LTE-MTC Systems," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 436–439, Aug 2016.
[84] J. J. van de Beek, O. Edfors, M. Sandell, S. K. Wilson, and P. O. Borjesson, "On channel estimation in OFDM systems," in *IEEE Veh. Tech. conf.*, vol. 2, Jul 1995, pp. 815–819.
[85] G. Auer and E. Karipidis, "Pilot aided channel estimation for OFDM: a separated approach for smoothing and interpolation," in *IEEE Int. Conf. on Commun.,*, vol. 4, May 2005, pp. 2173–2178.
[86] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul 1998.
[87] E. A. Ahmed and M. M. Khairy, "Semi-adaptive channel estimation technique for LTE systems," in *IEEE Symp. on Computers and Commun.*, June 2011, pp. 457–482.
[88] C. Y. Hsieh, D. W. Lin, and C. Ma, "LMMSE-Based Channel Estimation for LTE-Advanced MIMO Downlink Employing UE-Specific Reference Signals," in *IEEE Veh. Tech. conf.*, May 2015, pp. 1–5.
[89] W. J. Hwang, J. H. Jang, and H. J. Choi, "An enhanced channel estimation with partial interference cancelation for MU-MIMO system," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1232–1235, August 2012.
[90] T. Kamenosono, M. Kaneko, K. Hayashi, and M. Sakai, "Compressed sensing-based channel estimation methods for LTE-Advanced multi-user downlink MIMO system," in *IEEE Veh. Tech. conf.*, May 2015, pp. 1–5.
[91] Intel Corporation, "Receiver algorithms and complexity analyses for NB-IoT synchronization," 3GPP TSG RAN WG1 Ad-Hoc Meeting, Tech. Rep. R1-161897, March 2016.
[92] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for Next Generation Wireless Systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, February 2014.
[93] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An Overview of Massive MIMO: Benefits and Challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct 2014.
[94] J. Nam, J. Y. Ahn, A. Adhikary, and G. Caire, "Joint spatial division and multiplexing: Realizing massive MIMO gains with limited channel state information," in *2012 46th Annual Conf. on Information Sciences and Systems (CISS)*, March 2012, pp. 1–6.
[95] A. Pitarokoilis, S. K. Mohammed, and E. G. Larsson, "On the optimality of single-carrier transmission in large-scale antenna systems," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 276–279, August 2012.
[96] C. Studer and E. G. Larsson, "PAR-Aware Large-Scale Multi-User MIMO-OFDM Downlink," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 303–313, February 2013.
[97] S. K. Mohammed and E. G. Larsson, "Per-Antenna Constant Envelope Precoding for Large Multi-User MIMO Systems," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1059–1071, March 2013.
[98] Y. Zeng, R. Zhang, and Z. N. Chen, "Electromagnetic Lens-Focusing Antenna Enabled Massive MIMO: Performance Improvement and Cost Reduction," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1194–1206, June 2014.
[99] Z. Xiang, M. Tao, and X. Wang, "Massive MIMO Multicasting in Noncooperative Cellular Networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1180–1193, June 2014.
[100] R. Deng, S. Zhou, and Z. Niu, "Scalable Non-Orthogonal Pilot Design for Massive MIMO Systems with Massive Connectivity," in *2016 IEEE Globecom Workshops (GC Wkshps)*, Dec 2016, pp. 1–6.