

REVIEW

Open Access



A survey on the handover management in 5G-NR cellular networks: aspects, approaches and challenges

Amiraslan Haghras^{1*} , Mehran Pourmohammad Abdollahi¹, Hosein Azarhava¹ and Javad Musevi Niya¹

*Correspondence:
amiraslanhaghras@tabrizu.ac.ir

¹ Faculty Of Electrical
And Computer Engineering,
University of Tabriz, Tabriz, Iran

Abstract

With the purpose of providing higher data rate and ultra-reliable and low-latency communications for the users, employing the small cells in the upcoming Fifth-Generation-New Radio (5G-NR) cellular networks and beyond is leading to the serious challenges in mobility management due to dynamicity of the user equipments (UEs). Among different issues related to the mobility of the UEs, the handover management is one of the key procedures to let the UEs experience a high quality of service (QoS)/quality of experience (QoE). So far, many protocols and algorithms have been proposed to enhance the mobility management in 5G-NR from various aspects, but still a thorough survey has not been incorporated to summarize the recent advances and future directions of the mentioned issue. Thus, the handover management and the corresponding challenges stand in the center of concentrations in this paper, with a glance on 4G to the advancements of 5G-NR. The challenges include QoS/QoE, throughput, delay, traffic load, the attacks during authentication process and resource allocation. To overcome the mentioned challenges, the handover procedure is evaluated by some key performance indicators such as handover ratio, handover failure, radio link failure and such like which depend on the received signal quality. The lack of new advancements and novel aspects of handover plus the separation of security and handover issues in previous works are perceived as research gaps and motivations for the current paper. In this regard, this paper aims to specify and analyze the technical issues, to provide an overview on the proposed methods and recent advances and to bring the future directions into the limelight. We categorize the concurrent standards and methods about the handover, and then, we survey the proposed algorithms including theoretical, algorithm-based and pattern-capturing approaches following the authentication process along with the vulnerabilities and the algorithms to counteract the attacks during handover. Also, we study various issues corresponding to network performance during the handover procedure. Finally, we discuss the open problems and future research directions.

Keywords: 5G-NR cellular network, Handover management, Authentication, MmWave, Multi-connectivity

1 Introduction

To cover a wide geographical area and increase the number of users, the cellular networks divide the area into several cells in which the communications between the users inside or outside of the region are achieved through one or more fixed base stations (BS) or temporary replaceable aerial BSs such as hovering unmanned aerial vehicles (UAVs). The prospect of high data traffic growing by 1000 times in future years imposes a great challenge on wireless communications [1]. The International Telecommunication Union Radio communication sector (ITU-R) started the investigations on next-generation cellular networks in 2012 by researching on development of International Mobile Telecommunications (IMT) standards for 2020 and later which was called IMT-2020. Then, in 2015, the ITU-R published some viewpoints and aims about the upcoming generation of cellular network based on the worldwide researches abbreviated in the following approaches [2]:

- *enhanced mobile broadband (eMBB)*. Performance improvement in eMBB-based scenarios and highly integrated user experience in comparison with existing mobile broadband technologies,
- *Ultra-reliable and low-latency communications (URLLC)*. Supporting fastidious requirements for operational power, delay and availability for users such as wireless control of industrial productions, tele-surgery, automation of smart grids and securing the transportation systems,
- *massive machine-type communications (mMTC)*. Supporting an untold number of connected UEs insensitive to delay with low data rate.

The fifth-generation of cellular networks is composed of three main parts: *a)* User equipment (UE): the device which is used by an end user to access the provided services by an operator in the cell; *b)* next-generation radio access network (NG-RAN): The set of devices which provide radio access technology and lay between the UEs and core network as an interface; and *c)* 5G-NR core network: The infrastructure which connects the different parts of the cellular network to each other or other networks. The access control, session control, routing and connecting the other networks could be considered as the main duties of a core network. The utilized hardware and software in 5G-NR could be considered as:

- *gNB*: the connection point of the UE to the network (BS),
- *Access and mobility function (AMF)*: the mobility management entity (MME) in 4G is superseded by access and mobility function (AMF) in 5G networks which takes the burden of accessing of UE to the network such as registration and connection and the mobility management, authentication and cryptography [3],
- *User plane function (UPF)*: the main unit for separation of user plane and control plane [4],
- *Session management function (SMF)*: a fundamental unit with responsibility for interactions with user plane and also, creating, updating and eliminating PDU and UPF management,
- *Data network (DN)*: responsible for operator's service such as Internet,

- Next-generation application protocol (NG AP): the interface to exchange control messages between BS and AMF,
- Xn application protocol (XnAP): the interface to exchange control messages between gNBs.

The prospect of 4G and 5G networks is summarized in Table 1 [1, 5]. The table shows an incredible growth of UE density in 5G networks compared with that of 4G. To tackle the subsequent problems of these issues, the coverage areas are shrunk and higher frequencies are utilized. The condensed coverage areas in addition to the high-speed users in these networks make the handover management an essential challenge to provide a seamless connection. The mmWave communications, separation of user plane and control plane and multi-connectivity are potential solutions for the mentioned problem. However, the frequent changes in the radio links affect the performance of the other layers and units in the network. Figure 1 exhibits the involved units in the handover procedure in 5G networks.

The heterogeneous networks (HetNets) could be dubbed as the radio networks with different coverage areas such as macrocells and smallcells and integration of different

Table 1 Summary of parameters and consideration in mobility management from LTE toward 5G-NR

Parameter	LTE requirement	5G target
User plane latency (RTT)	20 ms	1 ms
Control plane latency (idle-to-active time)	100 ms	10 ms
Handover execution time	40 ms	0 ms
Supported maximum coupling loss	140 dB	164 dB
Connection density	10 ⁵ connection/km ²	10 ⁶ connection/km ²
Mobility	350 km/h	500+ km/h
Traffic volume density	0.1 Tbps/km ²	10+ Tbps/km ²
Peak data rate	1 Gbps	10+ Gbps

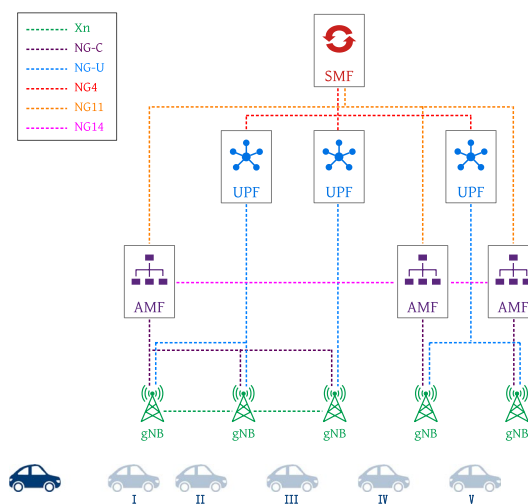


Fig. 1 Handover mechanism in 5G networks

technologies such as 4G legacy networks, Internet of things (IoT), vehicular ad hoc network (VANET) and wireless local access network (WLAN). The HetNets' goal is to increase the coverage area and the user capacity in the network [6]. The smallcells could be added to the network at the presence or absence of Macrocells, in open or covered places and in dense or sparse configurations. Applying smallcells in 5G networks affects the network with the following concepts [7]:

- The smallcells could enable many devices like mMTCs to connect the network which have to be handled by high capacity Macrocells in their absence.
- The smallcells could improve the signal quality received by the UE and decrease the delay as an improvement for URRLC.
- Increasing the power of smallcells increases the throughput of the network and obviates the UEs' avarice for high data rates such as high-quality live video streaming.

The coexistence of various cells covered by several technologies comes at the price of severe interference between the BSs and UEs. To avoid the interference between adjacent cells, different resources are deployed in the coverage area corresponding to each cell. This can be attained by allocating different frequencies to each cell or allocating different frequencies along with directional antennas. In the last one, different frequencies could be used in a cell to cover the area. A resourceful method to obviate the demand for high data traffic created by mobile users in a cellular network is to reuse the available frequencies by reducing the coverage area of BSs and their aggregation. Hence, the mobile users intersect different cells continuously, depending on their velocities.

According to 3GPP reports, three connection modes related to radio resource control (RRC) indicate the UE's connection states to gNB in 5G networks: RRC-Idle, RRC-Connected and RRC-Inactive. In the RRC-Idle mode, the equipment is turned on, but not registered in any BS, and also, the mobility management is to choose the primary BS to receive service. In the RRC-Connected or RRC-Inactive modes, a radio channel is allocated to UE and the registration is accomplished [8, 9]; then, the mobility management is to change the BS regarding the movement and the quality of received signal in the UE to maintain or improve the quality of service [10, 11]. The RRC-Inactive mode is added to the state machine in radio resource allocation control unit to manage energy and delay, as well. The concept of mobility management in RRC-Connected mode is to change the BS based on the network requirements which is referred as handover management. Due to high-speed users specially in 5G networks and beyond, the handover management requires more attention to overcome the related challenges. To maintain a desired service in ultra-dense networks, the handover management is required to provide an integrated service with high quality in the coverage area. To this, a swap between the BSs has to be done without ceasing the service, the user must be authenticated in the new BS and the resources must be allocated to the user if available. The handover management is achieved through three main procedures; a) Cell/Beam Selection/Reselection, b) Authentication and c) Network Reconfiguration. The direct consequence of reducing the coverage area and aggregating the BSs is the intense growth of mentioned procedures needed by the users, due to numerous swaps between the coverage areas of different BSs. Increasing the number of handovers and authentications between BSs increases the

number of controlling messages which subsequently causes the reduction in the operational performance of the system and increasing the delay.

1.1 Review of related surveys

In this subsection, we provide a brief review of existing surveys whose main domains are related to this paper, namely mobility/handover management, mobility prediction and security/authentication.

In the context of mobility management, the contribution in [12] provided a precise review on cell recognition, access control, cell search, cell selection and handover in Femtocell included networks. Likewise, the available handover methods and corresponding decision-making algorithms were discussed in two-tier networks based on the received signal quality, velocity, cost function, interference and energy consumption. The article [13] presented an overview on the structure of mobility management in 5G, categorizing the challenges in mmWave frequencies, dual connectivity, carrier aggregation, etc. Furthermore, they discussed the potential solutions such as conditional handovers and multi-connectivity for the mentioned challenges. The authors in [14] investigated the mobility management specially the concepts of RRC, initial access, involving units and exchange of control messages during handover in 5G networks. They provided various dual connectivity solutions, SDN-based solutions and conditional handovers for corresponding challenges in 5G, as well. The beam-level and cell-level managements in 5G were discussed in [15] from the aspect of URLLC requirements for vehicle to everything (V2X) networks. The authors categorized the mobility management under beam misalignment, beam's coverage area and frequent beam swap branches with three class of solutions; cost-aware handover decision, mobility-aware handover decision and beam management development. In the other approach, the authors in [16] distinguished the discrepancies and main challenges of handover management in 4G, 5G and HetNets and restated the enhancements of 5G compared with the 4G. Moreover, they paid attention to the handover management in high-speed scenarios, beam-level handovers and uplink handovers. The main concentrations of the authors in [17], are handover and real-time video streaming in vehicular ad hoc networks (VANETs). They surveyed the constraints of existing handover mechanisms and handover failures as the causes of service disintegrity. The solutions to handover management were widely discussed from the aspect of mathematical prediction models, channel characteristics, speed of vehicle and use of mobile IP, and the solutions for handover failures were classified in mobility, interference, communications jamming, blockage and coverage area categories. A comprehensive study on machine learning algorithms, the advantages and deficiencies were achieved in [18], based on the resource of inputs. The inputs were classified into visual data and network data sets, and the considered algorithms were divided into supervised learning, unsupervised learning, reinforcement learning and distributed learning methods. In another study, the authors reviewed the reinforcement learning techniques in ultra-dense small cell (UDSC) providing a comparative observation for different handover scenarios [19]. The importance of handover challenges and mobility management in drone networks was clarified in [20], as well. Since the mobility prediction is very important for handover management, resource allocation and location-based services, the authors in [21] surveyed several topics such as Markov chain, hidden Markov chain,

artificial neural networks, Bayesian networks and data mining methods which predict the moving direction, transition probability, future location of UE and target BS.

In the other approach, the authors in [22] reviewed the structure and benefits of deploying V2X communications in cellular networks, providing the solutions to enhance the authentication algorithms in 4G and D2D communications and the security methods for employing V2X in 5G. The security requirements and vulnerabilities and evolved packet system authentication and key agreement (EPS-AKA) algorithms in 4G and the corresponding solutions for enhancements and standards issued by 3GPP in 5G were reviewed by S. Behrad et al. [23, 24]. In addition, the authors in [25] studied the security performance of 5G networks beside the vulnerabilities and requirements of newly developed concepts such as mMTC, D2D, V2X and network slicing, coming to the conclusion about the various solutions to consolidate the authentication process. Likewise, the handover was classified based on RAT and frequency in HetNets and the privacy and security threats during vertical handovers (within 3GPP, between 3GPP and non-3GPP,

Table 2 Summary of relevant surveys/overviews on authentication, mobility and handover management and mobility prediction

Main domain	Target network	Sub topics	Refs.
Mobility management	LTE-A	<ul style="list-style-type: none"> • Interference Investigations in Femtocells • Mobility Management in Two-Tier Cellular Networks • Cell Identification, Cell Search • Cell Selection/Reselection, Access Control • Handover Decision, Handover Execution 	[12]
	5G	<ul style="list-style-type: none"> • A Brief Overview on Handover Techniques, • mmWave, Dual Connectivity, Carrier Aggregation 	[13]
	5G	<ul style="list-style-type: none"> • Initial Access Resource Control 	[14]
	5G (V2X)	<ul style="list-style-type: none"> • Beam-Level Management 	[15]
Handover management	4G/5G	<ul style="list-style-type: none"> • Handover Mechanisms in 4G and 5G and Comparisons • Target BS Selection 	[16]
	5G (VANET)	<ul style="list-style-type: none"> • Handover Failures and Proposed Solutions in VANETs 	[17]
	5G/Beyond	<ul style="list-style-type: none"> • Machine Learning Algorithms 	[18, 19]
	5G/beyond (Drones)	<ul style="list-style-type: none"> • Handover Challenges of Drones' Users 	[20]
Mobility prediction	4G/5G	<ul style="list-style-type: none"> • Importance of Mobility Prediction and Methods Based on: • Learning Algorithms, Markov Chains, Hidden Markov Model, • Artificial Neural Network, Bayesian Networks, Data Mining 	[21]
Security/ authentication	4G/5G (V2X)	<ul style="list-style-type: none"> • V2X Overview, Advantages of Using Cellular Networks in V2X, • V2X Security Vulnerabilities, • Potential Attacking Threats on V2X 	[22]
	4G/5G (V2X)	<ul style="list-style-type: none"> • Structures and Protocols of Authentication in 4G, • Vulnerabilities in 4G and Perspectives on 5G 	[23, 24]
	5G	<ul style="list-style-type: none"> • An Introduction to Security Performance of 5G, Massive IoT, • D2D Communications, V2X Communications, Network Slicing 	[25]
	HeTNeTs	<ul style="list-style-type: none"> • Vertical Handovers: Handovers within 3GPP Networks, Between 3GPP and non-3GPP Networks, Between non-3GPP Networks • Horizontal Handover: Intra-Mobile Service Controller, Inter-Mobile Service Controller Handovers 	[26]

between non-3GPP) and horizontal handovers (intra-mobile service controller (MSC), inter-MSC) and the solutions to foil them, were discussed in [26].

Table 2 briefly summarizes related surveys. It could be observed that an assortment between these surveys is perceptible in which the papers that consider handover issues do not involve the authentication, new aspects of handover or all of the network parameters. To fulfill the research gaps, a comprehensive survey including recent advances in 5G related to the handover is required to gather all issues together. Table 3 shows the comparison between the topics included in previous surveys and the contribution of this paper.

1.2 Contribution

The handover is one of the most important characteristics of the cellular networks. The growth of these networks in recent decades has brought new challenges, and a large number of studies have been published to enhance the network performance. Aggregation of the high-speed users such as trains and aerial vehicles to the networks in 5G and beyond, the handover management has become an outstanding subject, and it has been alluring to the interest of many researchers. The main contributions of this survey discuss three categories of handover after providing a brief tutorial on handover mechanism which makes the reader familiar to the procedure. Then, the methods to execute the handover and corresponding issues are represented. The authentication process during the handover and vulnerabilities are explained well. The main contributions of this paper are summarized as follows:

- After a glance on the corresponding units and functions on handover mechanisms in 5G, we provide a thorough study of recent advances on the handover management, authentication and many involving parameters together, which the previous works lack such an approach specially for 5G networks.
- We represent a new approach-based classification on handover management including theoretical, algorithmic and experimental methods. Also, a comparison between the studied KPIs for each method and corresponding advantages are well prepared.
- We include the interactions between handover procedure and network structure consisting of resource management, auxiliary technologies (such as multi-connectivity, D2D and mmWave communications), backhaul (such as NF placement) and TCP, which have been rarely paid attention.

1.3 Paper organization

Section 1 is a prelude on the involving units and features of handover in 5G, followed by a comparison between several surveys/overviews related to the present paper. In Sect. 2, a brief tutorial on the handover mechanism and different categories are provided and the corresponding characteristics in 5G are identified along with the involving units and some of important discrepancies with 4G, including different handover initializations from the aspect of UE and network. Different protocols for initiation time of handover procedure and choosing the proper target BS for reconnection are elaborated and

categorized into theoretical approaches, algorithm-based and other methods, and the comparisons are prepared precisely in Sect. 3. The users' numerous authentications could increase the delay and create security problems. The investigations of various literatures and proposed protocols to solve these problems and also various attacks during handover and preventive actions to counteract these attacks in recent investigations are represented in Sect. 4. Section 5 describes the mutual effects between network parameters and handover procedure and several approaches for better realization. The challenges of handover management and directions for future works are represented in

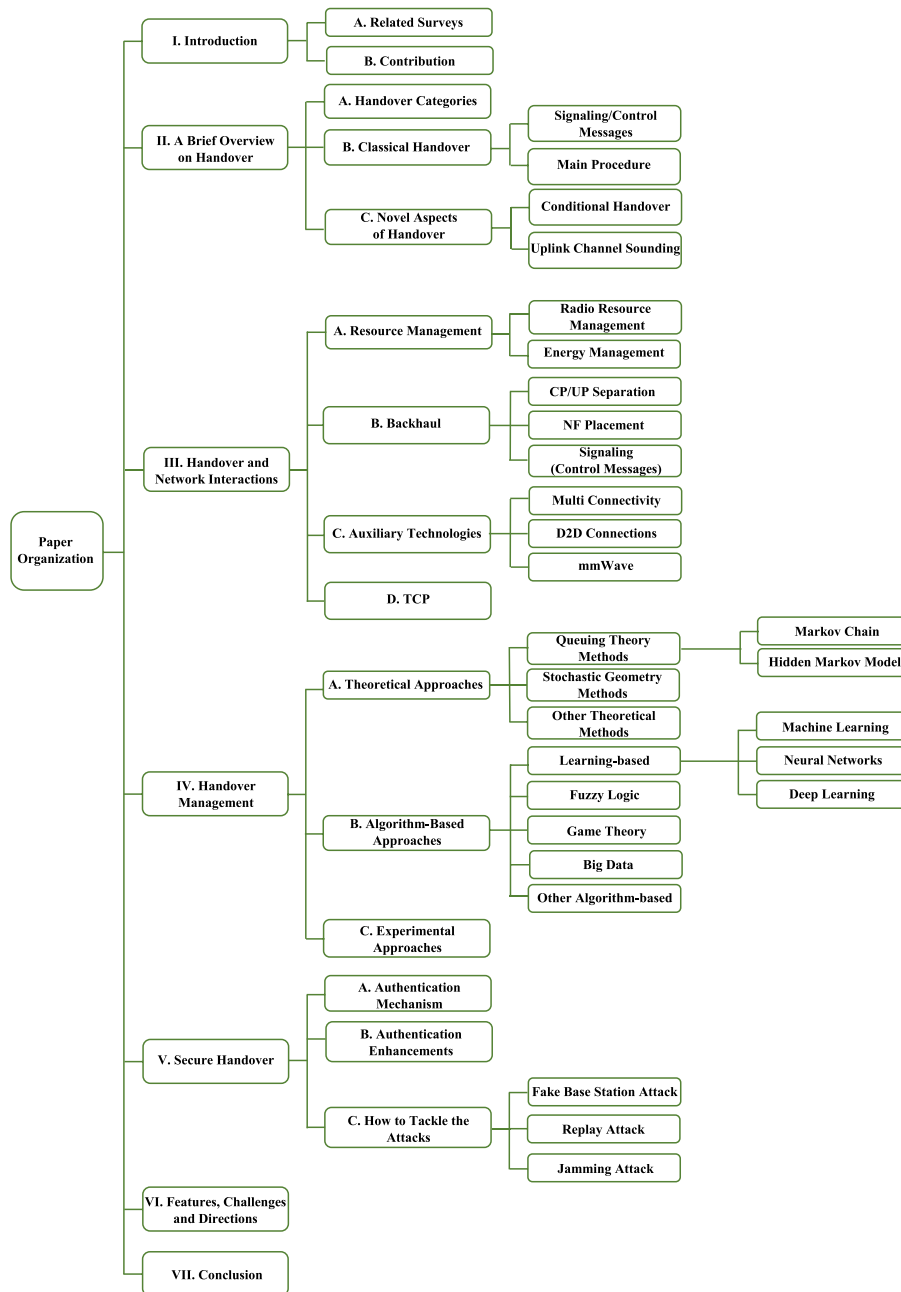


Fig. 2 Paper organization

Sect. 6. The organization of the paper is exhibited in Fig. 2. Also, a list of acronyms is provided in Abbreviations.

2 A brief overview on handover

To acquire a better realization on the handover mechanism and the affected parameters, we briefly discuss the various handover categories, involving units and parameters, corresponding units and functions exploited in 5G networks. The handover could be interpreted as the most important part of the mobility management in cellular networks to preserve an integrated communication with good quality of service. In fact, the handover is to deliver the service of an active connection from one BS to another one without any disconnection. This process is executed for various purposes, such as preserving the signal quality being lost due to exiting the coverage area of serving BS, resource allocation, network load balancing and energy savings [27, 28]. The decision to handover is made based on the received signal quality in downlink, the transmitted signal quality in uplink, the coordinations of UE and BSs, user mobility direction, velocity of the user, etc. QoS, QoE and such parameters have been used to evaluate the mentioned criteria. The handover procedure could be classified in different categories based on size, type, radio access technology of serving and target base stations, interface used to transmit control messages, participated network functions in the handover procedure, etc. Each category has its own features and characteristics and adds extra challenges to the handover procedure which should be considered in the handover management.

2.1 Handover categories

In this subsection, we study the categories of handover from different aspects.

2.1.1 Access-based handover

Three scenarios could be considered in handover management, based on the size, type and radio access technology, as follows:

- *Intra-/inter-frequency*. If both serving and target BSs use the same frequency, the handover is considered as intra-frequency, and if they use different frequencies, it is considered as inter-frequency.
- *Intra-/inter-cell*. If both serving and target BSs are similar from the aspect of femto-cell or macrocell, the handover is considered as intra-cell, and if they are in different hierarchy (one as femtocell and the other as Macrocell), it is considered as inter-cell.
- *Intra-/inter-RAT*. If both serving and target use the same technology like 4G, the handover is considered as intra-technology and else it is considered as inter-technology.

2.1.2 Network function-based handover

The handover procedure varies based on the participated network functions. Different scenarios are available in Fig. 1 where the serving gNB, AMF, user plane, NG and Xn are involved in this procedure. The scenarios are described as follows [6, 29]:

- *Intra-gNB*. The serving and target gNBs are the same and the handover procedure occurs in the frequency level or in the beam level.
- *Inter-gNB (intra-AMF/intra-UPF)*. The serving and target gNBs share the same AMF and UPF and hence the handover procedure could be achieved on gNB level if interface Xn exists.
- *Inter-gNB (intra-AMF/inter-UPF)*. Since only the AMF is the same for both gNBs, the handover procedure could occur on gNB level if Xn exists. The control messages could be exchanged via NG interface.
- *Inter-gNB (inter-AMF/inter-UPF)*. Since the AMF and UPF are not the same for serving and target gNBs, the handover procedure is handled in NG level between two AMFs.
- *Inter-gNB (inter-AMF/intra-UPF)*. The handover procedure is handled in NG level between two AMFs, while the UPF remains the same for gNBs.

2.1.3 Beam-level/cell-level handover

The coverage area of a BS in 4G networks encompasses a circle or a sector of circle which covers a vast area. However, engaging the high frequencies of mmWave communications in 5G networks attenuates the signals severely, and the resulted path loss thins this area. This problem is overcome via beamforming antennas so that the signal power is concentrated on small regions. In the last release of LTE standards, only a few of beams have been applied to cover the target area, while in 5G standards, using 64 beams by a gNB has been considered for that area [30]. As a result, the handover procedure could be done in both cell level and beam level. Due to exiguity of the regions covered by serving beams, the UEs have to change their serving beams continuously. Thus, one of the most important issues in these networks is the handover management in beam level with low latency and high reliability. To decrease the delay, this kind of handover is managed in physical and MAC layers without involvement of RRC layer [28].

2.1.4 Standalone (SA)/non-standalone (NSA) handover

The 3GPP organization has confirmed two implementation options for 5G networks: SA and NSA. These options have been introduced in technical report [31] as follows:

In NSA architecture, LTE network and EPC infrastructure core networks cooperates with the 5G-NR access technology which is called E-UTRA-NR dual connectivity (EN-DC) or architecture option 3. In SA architecture, only NR access technology is used alongside with the 5G core network. In NSA architecture, the LTE anchor tackles the control messages and UE's mobility management issues. Regarding these architectures for 5G networks and signaling, the handover procedure becomes different [32].

2.1.5 UE-initiated/network-initiated

The UE-initiated handover begins if the request to handover is issued by UE, which mostly occurs to maintain the quality of service during channel degradation. On the other hand, if the network decides to initiate handover for some purposes such as load balancing, the handover will be a network-initiated type [28].

2.1.6 Xn/NG interface-based

If the handover management is achieved via the Xn interface between serving and target BSs but without the involvement of network function, then it is called Xn-based. If the AMF, UPF and other units are involved, the control messages are sent via NG interface and the handover is kind of NG based or network based [33]. It was shown that the handover delay in interface-based method is six times smaller than that of network-based on the condition that the X2/Xn interface exists [34].

2.2 Classic handover procedure

Since the handover procedure is initiated if the signal qualities are satisfied, the measurements are one of the most important stages in the handover procedure. The signal quality could be measured either in downlink or uplink to manage handover in 5G networks. According to the resource grid of NR physical layer, some standard signals called reference signals are defined to measure the quality of received signals. The reference signals include synchronization signal block (SSB) and channel state information reference signal (CSI-RS) block in downlink and sounding reference signal (SRS) in the uplink which is used by gNB. It is reminded that in the LTE networks, this measurement is only done in SSB and cell-specified reference signal in downlink direction [28, 35]. It is implied that for experiencing better services in the connected mode, the handover management has to be executed in a proper manner. The on-time decision to change the BS is achieved by channel quality measurements. These measurements could be attained either in downlink by the UE in classic approaches, or in the uplink by the BS which could be found in recent studies [36]. In the measurements in downlink direction, the UEs send the information and measured values about the serving and neighbor cells to the serving cell in a frame of control message called measurement report (MR). The MR comprises different data such as received signal quality in downlink from serving and target BSs. The MR consists of two phases: In the first phase, RRC message including the configuration of this process is sent to UE by gNB and in the second phase, the UE measures the signals in the required format and sends them to gNB. These measurements are processed and averaged via L1 filter in physical layer and L3 filter in RRC layer [11, 37]. Then, this message is sent to the serving BS to begin the handover process. Due to channel fluctuations in high frequencies, consecutive measurements of signal quality are prepared instead of one measurement which would not be proper for decision-making process. The three common criteria to evaluate the channel quality in 4G and 5G are:

- *Reference signal received power (RSRP)*: the average received power without considering noise and interference.
- *Received signal strength indicator (RSSI)*: the total received power including noise and interference.
- *Reference signal received quality (RSRQ)*: the ratio of rsRP to RSSI.

3GPP standards provide detail description of these parameters for LTE and NR, respectively, [38, 39]. Also, based on the method or transmission time, the MR is classified [11, 37] as:

- *Event-based MR*: The MR is sent if a specific event is occurred such as reducing the power of serving BS from a given value specified in the network.
- *Periodical MR*: The MR is sent during specified periodic intervals.
- *Requested MR*: The MR is sent if asked by serving BS.

Many approaches based on measurements of signal qualities in uplink or downlink have been provided, and mathematical models have been applied via the help of stochastic geometry considering technology, coverage area, interferences, the user movement models, etc., to find the optimum points. The outcomes could result in setting up the network parameters in order to increase the successful handovers. The following KPIs are considered to analyze the performance of handover and enhance the operational performance of the system:

- *Handover frequency* It is equal to the number of attempts per second in the serving BS which increases by increasing the speed of mobile user and coverage area reduction. As a trade-off, increasing the handover frequency decreases the handover failure rate [40].
- *Handover success rate* It is defined as the ratio of the number of successfully performed outgoing handover procedures to the number of attempted outgoing handover procedures [41].
- *Handover failure rate* It is defined as the ratio of failed handovers to the total handover attempts in the serving BS [40].
- *Ping-pong handover rate* It is equal to the number of ping-pong handovers per second which occurs if the connected UE to the target BS returns back to the serving cell during a small time interval [42].
- *Data latency* It is defined as the average time duration between the last transmitted packet before the beginning of handover process in the BS and the first received packet in the target BS after handover process [43].

Although the mentioned KPIs exhibit the handover performance, the early setup handover, late setup handover and inappropriate selection of target BS could be the most important reasons for a handover process to be failed.

2.2.1 Main procedure

A general example of classical handover is shown in Fig. 3. In this procedure, based on measuring the received signal power from serving and neighbor BSs in downlink direction, a successful handover is achieved through five stages as follows [27, 28]:

- *A3 event condition* The handover procedure is initiated if the defined conditions about the received signal quality are satisfied. As shown in Fig. 3, the handover begins within A3 event if the quality of received signal from the neighbor BS is better than that of serving BS plus threshold. Note that several events have been foreseen at the handover preparation phase in 5G networks [11, 37].

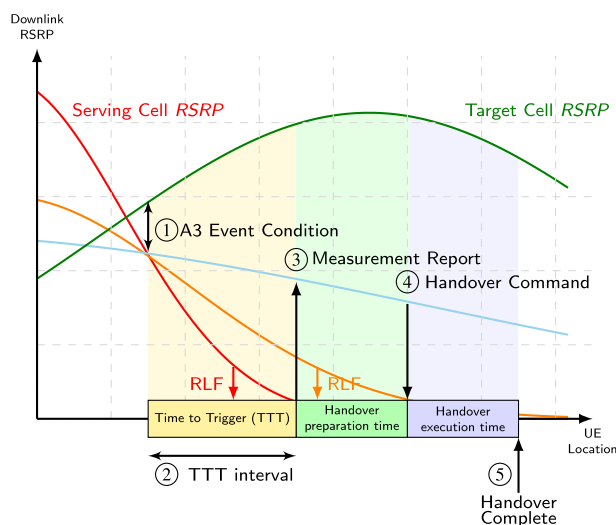


Fig. 3 The classic handover procedure

- *Time-to-trigger (TTT) interval* This is considered as the time to be sure about start of handover procedure, that is, the UE awaits for TTT before sending any report or handover request to the BS. TTT is defined by the network operator to prevent the ping-pong handovers.
- *Measurement report* If the start of handover procedure lasts for TTT, the UE transmits MR or handover request to the serving BS.
- *Handover command* If the serving BS confirms the request of handover and makes the agreement with target BS, a command is sent to set up handover and sends control messages to the UE.
- *Handover complete* After a successful handover, the procedure ends by transmitting an ending message to the attached BS.

Based on the above discussion, optimizing the classical handover procedure is to determine optimum TTT, handover entering conditions (e.g., A3 offset) and L1 and L3 filter coefficients.

2.2.2 Control messages

The handover procedure requires different levels of internal communications between network functions and signaling, based on the type of handover and involving units. The simplest kind of this process from the aspect of signaling complexity is the inter-gNB communications via Xn. Figure 4 shows the general structure of signaling order. The decision to initiate the handover procedure is made by receiving the MR in the serving BS. Note that in the Xn handover, the AMF and UPF units do not get involved and if they do, more signaling processes have to be done which increase the delay in the network.

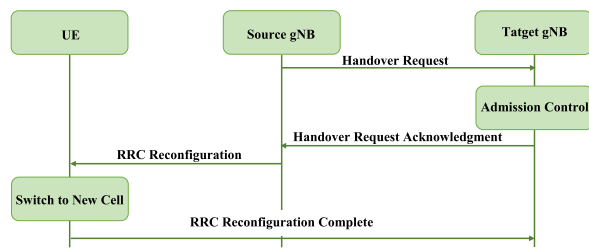


Fig. 4 Inter-gNB Xn handover procedure

2.3 Novel aspects of handover

2.3.1 Conditional handover

In 16th release of 3GPP standards [37], the conditional handover (CHO) has been introduced to increase the robustness of mobility management during handover by decreasing the number of RLFs. As explained in Fig. 3, the handover request and transmitting control messages like MR in classic handover were initiated when the radio link experienced serious attenuation. Initializing the handover during the channel attenuation, causes the failure in transmitting MR or receiving handover command which fails the handover procedure. In conditional handover this command (indicating the target BS) is sent to the UE before channel attenuation, to be saved and used in the proper time for handover [37, 44].

A general example of CHO is shown in Fig. 5 in which the CHO procedure is achieved through the following stages:

- *CHO add event* The handover procedure is initiated if the defined conditions about the received signal quality are satisfied.
- *CHO add TTT interval* The UE awaits for TTT due to radio link fluctuations.
- *CHO add MR* If the start of handover procedure lasts for TTT, the UE transmits MR about the candidate BSs to the serving BS.

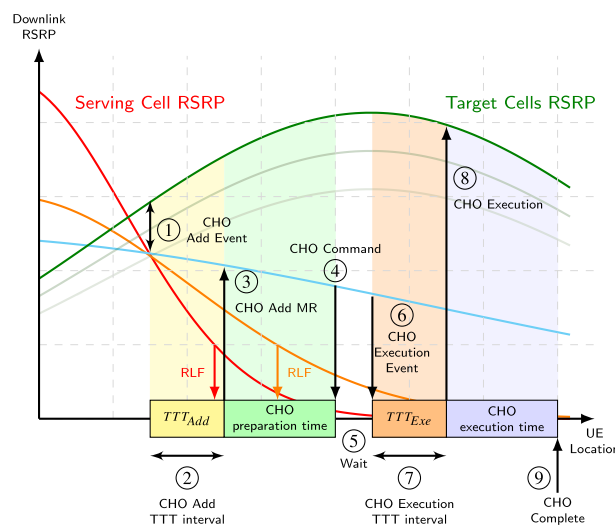


Fig. 5 The conditional handover procedure

- *CHO command* The RRC reconfiguration command, including the confirmed target BSs is sent to the UE by serving BS.
- *Wait* The UE awaits for the CHO to be satisfied. However, the information about the candidate BSs could be updated by *replace and remove* command.
- *CHO execution event* If the conditions are satisfied, the CHO is initiated.
- *CHO execution TTT interval* This is the awaiting time to be sure of UE's conditions.
- *CHO execution* The UE executes CHO based on the RRC reconfiguration command.
- *CHO complete* After a successful handover, the procedure ends by transmitting an ending message to the attached BS and reserved resources and candidate BSs are released.

Figure 6 depicts the signaling process of conditional handover via Xn interface. This kind of handover is initiated if the conditions are satisfied, similar to the classic handover, but the difference is in the use of saved RRC reconfiguration message instead of transmitting MR and handover preparation. In the other words, the resources are allocated to UE before handover initiation and remain as spare until the handover is done which is not suitable for high-load scenarios. Since the UE has saved the handover command in advance, there is no need to search the target BS in the failure situations and the procedure would be accomplished to connect to gNB which decreases the delay. Likewise, this type of handover improves the RLF in medium and high UE velocities. On the contrary, the increased number of early preparations for CHO is the cause of a great deal of signaling overheads in the network. A novel prediction-based CHO (PCHO) was offered in [45] to compensate the weakness of CHO using deep learning method, which shows 98.8% accuracy in predicting the next gNB. A. Prado et al. introduced enhanced CHO (ECHO) based on the user's mobility and reserved resources in that trajectory. Then, they developed a sequence to sequence (Seq2Seq) prediction model which reduces handover rate up to 23%, RLFs up to 77% and control messages up to 69% [46]. The simulations of baseline handover proved that CHO decreases the RLF and the system recovery process accelerates reconnections up to 80% despite RLF occurrence [47]. Moreover, the extension of fast CHO (FCHO) was introduced to decrease the handover failures and signaling load and resource allocation time [48, 49].

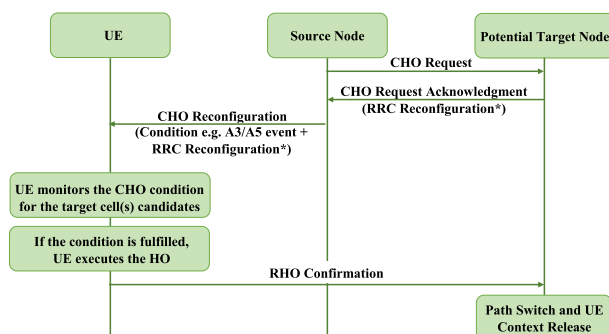


Fig. 6 The conditional handover signaling

2.3.2 Uplink channel sounding

The decision for trigger the handover procedure is made on the downlink signal quality in present generation of telecommunication network. Since the coverage area is wide, the handover occurs rarely. The juxtaposed or even intersected shrunk cells in 5G networks make the mobile UEs experience handover frequently and cause larger amount of signaling overhead and consequently the higher delay for waiting the response of transmitted MR to the BS. Using the uplink signal quality for handover and transmission of synchronization signals by BS periodically help the network to acquire information about the angular directional space without a need to search over [50, 51]. It was shown that eliminating the MR transmission in the uplink method and sharing the UE's uplink signal quality between serving and target BSs improve the paging miss rate up to 38% and decreases the energy consumption by 63% [52]. Actually, the algorithms based on the uplink signal quality decrease the delay and handover failure rate while increasing the network reliability [53].

3 Handover and network interactions

Cellular networks consist of a core network and a radio access platform. The core network allocates resources and provides routing and the communication between sub-networks and UEs. Also, it is responsible for transferring the control messages between serving and target BSs during handover, resource reallocation and rerouting data according new conditions. The access network contains all software and hardware, to make the wireless transmissions possible. Recently, many efforts have been made to develop and enhance both core and access networks. The main concerns of handover and network interactions consist of resource management, backhaul communications, auxiliary technologies and TCP. The following subsections pertain to the related discussions on handover and the mutual effects over various parts of the network.

3.1 Resource management

The resource management during handover procedure could be subcategorized as radio resource management (RRM) and energy management which is critical for dense small-cell regions. The following subsections describe the advancements in this area.

3.1.1 Radio resource management

The growth of low-power BSs near the railways comes at the cost of more frequent handovers. To investigate such high mobility scenarios, the performance of the network was evaluated by a reinforcement learning algorithm for different combinations of speeds and handover parameters showing that the handover parameter adaptation mechanism finds the optimal handover parameters [54]. W. Y. Lee et al. developed a unified mobility-aware framework in which a proper handoff mechanism is selected to minimize the switching latency, and an inter-cell resource allocation improves the network performance [55]. Although it seems that the movements of UEs in cellular networks happen completely by accident, they do have specific directions between the source and destination in real scenarios. Most of UEs show a repetitive movement pattern in their daily activities such as transportation between home and their office or work place, which is called diurnal mobility and could be useful in accurate prediction

of their future locations. The knowledge on the location of UEs would achieve better resource allocation in the network. Kuruvatti et al. exploited the diurnal mobility information of UEs to prognosticate the next cell as the next routes of the UEs in a real urban scenario. The authors monitored the UEs in a while to obtain the number of connecting BSs and calculate the probability of transition to another BS based on a Markov model. This model was improved by incorporating the source of UE to the previous model. They showed that resource allocation under sustain streaming/full buffer services, increases the throughput of UEs significantly even in coverage holes, in such scenarios [56]. In the other approach in a wireless mesh network (WMN), Qin et al. employed some access points (APs) with the same frequency to serve some UEs which move and switch from one AP to another one. The authors have studied the UE's throughput with fairness constraints in long-term period which exploits the resources via handoff management and timeline allocation. In handoff management channel allocation (HO-CA), a heuristic handoff decision is made based on the link efficiency between UEs and APs, whereas in channel allocation handoff management (CA-HO), the channel is assigned based on the APs' interferences and then, UE is allowed to proceed the handoff. Both methods maintain a high fairness, while the HO-CA has higher throughput [57]. Jangsher introduced a femtocell-based resource allocation in which a macrocell base station uses OFDM to communicate with two kinds of femtocells: fixed and moving femtocells with deterministic velocities and directions. The author has used the data about the speed and trajectory of the femtocells to derive the interference in between and specify them as an interference graph in different times. Then, a cluster-based resource allocation has been analyzed which shows that the scenario including moving femtocells is approximately similar to the scenario without moving femtocells, but it has better performance compared with the random resource allocation [58].

3.1.2 Energy management

The development of communication networks and high demand to data transfer have led to consuming more energy in this industry. The concern on energy consumption would be concentrated on both BS and UE sides in cellular networks. Besides, the corresponding methods have to be conformed according to the dynamic network topology. The on/off strategy for BSs based on UE's movement behavior was considered as one of the methods to optimize the energy consumption in 5G networks [59]. The fluctuation of energy consumption is due to heterogeneity of the network traffic, and most of the energy is consumed in lower layers of the network compared with the higher layers. An apt-RAN problem was solved to minimize the energy consumption in UE and the number of handovers under separation of planes. The proposed solution, called lightweight polynomial time heuristic, reduces the computational load and properly maps the neighbor distributed units (DUs) to UEs which is an important factor in energy consumption [60].

3.2 Backhaul

The backhaul communication as an underlying infrastructure includes user plane/control plane separation, network function (NF) placement and control messages from the

handover perspective. In the following, we describe the mutual interactions between these modules and handover.

3.2.1 User plane/control plane separation

To obviate the demand for capacity, 5G networks exploit the frequency bands higher than 5GHz up to 300GHz to achieve more spread spectrum. The severe attenuation in this frequency band makes it harder to cover the target area and increases the RLF. Separation of control plane and user plane is a potential solution to increase the capacity while providing integrated and reliable communications. The user plane maintains the high capacity in higher frequencies, and the control plane keeps integrity and reliability. L. Yan et al. [61] proposed a new structure to physically separate the user plane and control plane in railways telecommunications so that the user plane remains connected when the control plane, connected to the macrocell BS, executes the handover to another BS; similarly, the control plane remains connected when the user plane, connected to the smallcell BS, executes the handover. In another train scenario [62], it was shown that installing two antennas in front and at the end of a train maintains a stable communication and achieves soft handover with lower outage probability as a metric for reliability. On the other hand, this kind of separation improves the successful handover rate while reducing the outage probability and increasing the throughput. Since the handover is necessary for both user and control plane, an SDN-based strategy was developed upon predicting the available resources which decreases the handover delay and handover failure rate compared with the traditional methods in LTE networks. In this approach, Markov model was used to obtain the probability of UE's transition to the other cell [63]. However, the advantages and deficits of separating these planes were investigated compared with unseparated planes and the results demonstrated that in traditional networks, the growth of macrocell BSs in unseparated planes and growth of smallcell BSs in separated planes reduces the handover costs [64]. The effect of separating user plane and control plane on the handover management was investigated, and then, it was shown that the presence of small auxiliary BSs on the boundaries between serving and target cells could handle the control messages between macrocells and increase the number of successful handovers while improving the handover procedure delay by maintaining the connectivity [65].

3.2.2 NF placement

The NF module offers the required flexibility and reactivity and enables the operators to dynamically reconstruct the network, regarding their requirements, and to assign the resources to each function according to the demand for data. The placement of NFs has a great role in decreasing the delay and network costs in cellular communications. For example, in [66], the authors showed that by taking the user plane closer to the BS, the control message load decreases. The virtual NF (VNF) placement was optimized in [67], considering the UE's moving models to reduce the handover delay and a divide-and-conquer subgraph-based method was proposed to find the proper place of VNF for large topologies. Despite the centralized handover management in LTE networks in which the whole network could be disrupted by increasing the number of UEs, the authors in [68]

considered a distributed handover management method, equipped with SDN. In this method, the P-GWs are located around radio access network and reduce the handover delay by two-level buffering technique. Regarding the separated structure of NG-RAN into central units and DUs, and also the lack of security between them in 5G networks, a new protocol was represented in two phases: initial access and handover. The first phase is responsible for mutual AKA between the UE and gNB-DU, and the second phase secures the link between the UE and gNB-DU. Both phases are achieved via a master key (MSK) and the other keys derived from MSK [69].

3.2.3 Control messages and S1-X2/Sn-Xn interfaces

The plethora of control messages is the consequence of numerous smallcells and the growth of the UEs with high mobility in 5G networks. Hence, updating and the optimization of the structure of these messages and their transmission procedure are necessary to improve the network performance. A new unit named integrated MME/SDN controller (IMSC) was added to the core network to improve signaling mechanism at the initiation stage of handover, which is responsible for establishing tunnels and reduction of handshakes between various parts of the network and it can decrease retransmission costs [70]. Likewise, an optimized signaling method with three stages less than present protocols was proposed to estimate the probability of handover failures and to control the handover procedure at the stage of initiation or failure situations. This is achieved by preventive actions and reduces the computational costs and occupation of channels which are needed for transmission of the control signals [71]. A predictive mobility management (PrMM) algorithm was introduced in [72] to mitigate the cost of signaling overhead in the idle mode at dense paging areas and lower cell crossing rates.

3.3 Auxiliary technologies

The 5G network and beyond are very keen on newly developed technologies specially device-to-device (D2D) connections, mmWave and multi-connectivity. Despite quenching some parts of the ever-ending thirst of data rates by these technologies, they bring new challenges in delivering the superior experiences for subscribers. The following subsections discuss these opportunities and problems corresponding to the handover issues.

3.3.1 Multi-connectivity

To overcome the bombastic demand for exorbitant data rates in 5G networks and beyond, the use of high frequencies seems unavoidable which are very susceptible to blockages. A potential solution to this problem is to connect UE to several BSs simultaneously, so that the UE will remain connected if the main link degrades. An analytical approach in [73] was represented to evaluate the impact of multi-connectivity in THz frequencies on out-of-service and RLF probabilities, resulting in that increasing the coverage comes at the cost of increased initial access and base station discovery times. Although the dual connectivity to LTE and 5G in the urban areas seems immature from the aspect of reliability [74], the authors in [75] optimized control plane applications such as handover, beam tracking and initial access for

uplink multi-connectivity which improves the energy consumption and outperforms the cell selection process compared with the downlink-based methods. In the other study in a dual connectivity mode, the 4G data and 5G data were split optimally via applying MDP model on the handover management [76]. However, the multi-connectivity imposes some negative effects like the growth of control messages. A fractional duplication method instead of full packet duplication was applied in [77] to decrease the load of control messages by taking the advantages of fade duration outage probability (FDOP) information. A theoretical analysis on the effects of higher degree of multi-connectivity was suggested considering the dynamic blockages and self-blockages in mmWave and THz links which could envision abundant bandwidth for 6 G networks [78]. K. Qi et al. employed a dual connectivity method to reduce the handover delay and increase the reliability. They used predictive resource reservation scheme to improve outage probability, throughput and fairness, and also, they used proactive handover scheme to decrease the frequent handovers and complexity [79].

3.3.2 D2D connections

The D2D technology enables a direct communication between devices besides the communication with base station. One of the benefits of D2D links is to reduce the computational load and data traffic of the cellular network which increases the throughput of the core network and decreases the energy consumption. The D2D sidelinks could increase the reliability by helping the handover procedure of UEs which are not in the coverage area of base stations [80]. The authors in [81] designed a multi-layer neural network to select the optimal D2D relay in mmWave communications for the UEs out of the direct beam of the BS. Also, the D2Ds are very effective in the handover procedure of UEs with group mobility. Y. H. Chang et al. [82] classified these vehicles in three groups with the following duties:

Main leader: transmitting reference signal to all followers, gathering the information of link quality between all nodes and BS, transmitting the gathered data to BS,

Sub-leader: gathering the information of link quality between all nodes except BS,

Followers: measuring the signal quality of main leader, sub-leader and BS and transmitting them to main leader and sub-leader.

This classification helps the network to decrease the handover failures and increase the service integrity in V2V communications. On the contrary, a mode selection map was prepared based on the UE's trajectory and its distance from the boundary of coverage area to manage the handover procedure under the interference of D2D links [83]. The D2D communications completely benefit the context-processing capacities of the network and UEs' behaviors. But, the mobility of UEs results in instability of D2D communications. X. Yuan proposed a two-dimensional social--physical model for the movements of the UEs which pertains to the history and diurnal mobility. In this model, the

communication pattern switches to the cellular one, if the quality of D2D links degrade due to mobility of the UEs [84]. A peer-to-peer (P2P) method was utilized so that gNB could identify the best operating mode, either direct or D2D, which provides a seamless handover. Also, it was shown that D2D mode-based handover outperforms the direct mode with negligible latency [85]. Integrating fuzzy logic into SDN assisted UE to discover FAPs and D2Ds and select the best network to reduce the unnecessary handovers [86]. In the other approach, it was shown that SDN-based handover with D2D candidates reduces signaling overhead [87]. A mobility-aware femtocaching scheme was proposed to reduce the frequent handovers due to numerous FAPs supported by D2D pairs [88].

3.3.3 mmWave

The directional transmission is one of the beneficial methods to compensate the high path loss of beamforming technique. However, the mobility of the UEs creates severe inter-beam interferences. Shen et al. proposed the mobility-aware subband and beam resource allocation (MSBA) for subband--beam massive multi-input multi-output (SB-MMIMO) systems which decreases the complexity of calculations while maintaining the QoS for UEs. The authors have allocated the resources in the first phase, whereas they have specified the beam width and transmission direction in the second phase based on the analytical results [89]. Another analytic model was represented to expose the trade-off between the handover constraints and impact of multi-connectivity on delay and reliability [90]. Also, a dynamic matching game between UEs and BS was expressed to find a handover mechanism in mmWave- μ W communications which obviates the handover failures, UE's limited cache size and reduces the energy consumption [91]. In a very recent study, the reconfigurable intelligent surfaces (RISs) helped the UE to make a new path during the handover when a moving object like a vehicle, randomly cuts the mmWave signals in line-of-sight (LoS) direction between the serving cell and UE. This blockage-aware method could reduce the number of RLFs in the network and maintain seamless handover [92]. To estimate the behavior of mmWave radio links, the combination of two methods called, jump Markov linear system-deep reinforcement learning (JMLS-DRL) was represented which can decrease the redundant handovers below 5% within 200 episodes [93].

3.4 TCP

In 1970, TCP was designed and utilized for wired telecommunication networks for the first time. The immobility of devices and wired links were the basis of characteristics of this design. Due to efficiency of this protocol, it was deployed in the advanced wireless communications later. However, the mmWave channels and their susceptibility to blockages and the mobility of users, on the other hand, the performance of TCP has demonstrated some infirmity which need to be paid attention by researchers. For example, the authors in [94] showed that even short flows in TCP highly affect the LTE-A performance during handover from D2D to BS. The effect of TCP in mmWave communications was simulated under short/long blockages and frequent handovers, and the performance of TCP congestion control algorithms was compared with each

other such as Cubic, new Reno, Scalable TCP, Vegas, Westwood, YeAH and BBR. It was inferred that Cubic algorithm is more stable and combinational methods like YeAH improves RLFs [95]. Applying IrVegas, Westwood and new Reno in multi-hop wireless networks brought the following results: (a) The drop-based congestion algorithms would decrease the size of the congestion window (CWND) for false drops, (b) the delay-based congestion algorithms would decrease the number of CWNDs for wrong estimation of RTT (i.e. additional path switch delay during handover), (c) wrong estimation of RTT results in wrong estimation of band width. The fluctuation of CWND, besides the flat changes of CWND, leads to spoiling the bandwidth and throughput reduction [96]. The handover management based on X2-interface and its effects on TCP showed that Cubic is the optimum method from the aspect of fairness, and Cubic and Scalable TCP have optimum performance from the aspect of goodput [97]. However, high packet data rate could be counted as the weakness of the handover management algorithms.

It was shown that the performance of TCP is highly dependent on the appropriate combination of multi-connectivity, frequent handovers, size of packets, 3GPP stack parameters, edge and central services, but the congestion management algorithms in mmWave communications seem feeble in accommodation of CWND with available bandwidth [98]. The multi-path TCP allows the communication systems to send/receive packets on several paths with different RATs to make optimal use of resources [99]. This multi-path protocol is a potential solution for integrity of service in HetNets under multi-connectivity, handover procedure and RLFs. The purpose of multi-path TCP configuration is to aggregate the band width, but it can be used as a compromising factor between network performance and energy consumption. It was used in vehicular networks to estimate the UE's trajectory and find a new route for data transfer [100]. Also, it was used to track UE via distributed anchor points which improves delay and data rate in dedicating the new routes for data during handover [101]. In another paper, the multi-path TCP between WiFi and cellular network sped up the seamless handover via MultiMob method. Although the simultaneous connection in two paths is not justified, the MultiMob reduces the energy consumption in smart phones, but improves the TCP performance [102]. As an experimental method, the authors in [103] compared the Cubic, LIA and OLIA algorithms on multi-path TCP from the aspect of energy consumption in which OLIA outperforms the others. The YeAH also outperformed Cubic under hierarchical mobile IPv6 (HMIPv6) in both one-path and multi-path connections [104]. To reduce the ping-pong handover and the consequent delay in heterogeneous networks, an SDN-enabled vertical handover was proposed based on the estimation of user's location, network selection and handover execution. This method keeps at least one Subflow multi-path TCP connected during handover and decreases the number of handovers about 10% to 30% compared to the traditional algorithms [105].

Table 4 summarizes the interactions between handover and network. Some of the unexplained references will be elaborated in the next sections to show how the above-mentioned subjects affect the handover procedure.

Table 4 Handover and network interaction

Main topic	Main issues	Refs.
Resource management	Load balancing Optimum resource reservation in conditional handover Optimum resource reservation in multi-connectivity	[55–60, 84, 89, 103, 106]
CP/UP separation	Growth of handover rate High signaling traffic CP/UP Signaling synchronization Growth of authentications Optimum placement of CP/UP nodes	[61, 62, 64, 65, 75, 76, 107]
NF placement	Dynamic NF placement Adaptive NF placement Fully autonomous NF placement Optimal signaling between separated NFs	[67–69, 108]
Signaling	Smooth transition from current to future cellular networks Latency, transmission and processing costs. Inter-RAT signaling 3GPP/non-3GPP signaling	[70–72, 86, 87, 109–113]
Multi-connectivity	Optimal selection of secondary BSs Soft path switch (Minimize path switch delay) Higher signaling load Radio resource management Energy management	[36, 62, 73–78, 100–103, 114–117]
D2D connections	Interference cancellation Network discovery Security Beam forming at device side Selection and establishment of relay stations	[80–89, 91, 94, 118]
mmWave	Severe channel intermittency Highly susceptible to blockage Beam forming needed due to high isotropic pathloss High handover frequency Imprecise signal quality measurement	[36, 45, 50, 51, 64, 65, 73, 75, 78, 81, 89, 91, 95, 98, 113, 114, 119–127]
TCP	Congestion control algorithm Optimum TCP packet size Buffer size in different protocol stack layers	[94–96, 98, 100–103]

4 Handover management

We categorize various studies in theoretical, algorithm-based and experimental methods which have tried to overcome the handover issues. Our classification has been prepared according to the approaching methods as follows.

4.1 Theoretical approaches

Based on the BS's coverage area, interference, type of access technology, UE's moving model and velocity, various mathematical models have been propose to analyze the handover procedure and find the optimal points of the network. These tools could be enumerated as stochastic geometry, queuing theory and such like. The main purpose of these methods is to expose the effect of network parameters in RLF, handover successful probability and finally help the optimal configuration of the network parameters in different scenarios. Some of dominant works in this area are explained in the following.

4.1.1 Queuing theory methods

4.1.1.1 Markov chain The Markov processes would be described as an extension to independent processes in which the output of the current state only depends on the previous state, i.e. the past events do not affect the future events in these processes. The Markov chain is a special case of Markov processes that the states are countably limited and the evaluation of the future state only depends on the present state not on the way that the system has entered to this state [128]. The Markov chain model has been used in mobility management either in management of handover procedure or in the prediction of user movement behaviors.

In [114], a simple but precise and effective Markov model was proposed to analyze the dynamic behavior of link blockage which considers all movements of UEs, blockers and APs (like UAVs). Also, an extension was added to the model to cover multi-connection communications which is a potential method to decrease the number of RLFs in 3GPP-5G. This model is capable of calculating the SNR and capacity process dynamics, probability that the system is at blockage or non-blockage state at time t , fraction of time in blockage state and the mean and distribution of time to outage. The authors in [118] proposed a novel 2D Markov model including two separate queuing systems: the handover from first cell to the second cell and vice versa, to analyze the probability of D2D blocks, handover failures and number of unnecessary handovers between D2D pairs which follow a reference point group mobility (RPGM) as the moving model. It was shown that increasing the number of channels increases the successful D2D communications. In the other method, the radio frequency fingerprint (RFF) accelerated the localization of femtocell access points (FAPs) by UEs in two-tier HetNets and improved the vertical and horizontal handovers. The FAP is selected according to UE's traveling time and achievable capacity and the probability of transition between vertical and horizontal handovers is derived via a semi-Markov model. To be more precise in selecting the FAP, the probability to handover is regularly measured in RFF region, but it is limited to a dynamic sensing interval to save energy by canceling the excessive measurements and skipping non-proper handovers [106]. However, most of the mathematical models apply the single-input memoryless exponential distribution which is not capable of depicting a multi-dimensional entity for handover requests. A new model based on matrix exponential (ME) was proposed which considers all moving characteristics together and derives the handover blockage probability in terms of time to process the handover request, available resources and the capacity of buffer for received requests [129]. A local mobility management was proceeded in 5G networks with dense smallcells based on locator identifier separation protocol (LISP) and local mobility anchoring considering the fast handover concepts. The authors divided the area to more smaller regions and analyzed total signaling costs, data delivering costs handover latency and packet loss using a discrete-time Markov model, which improves the performance of handover management and decreases the computational complexities by 90% [130].

The discrete-time stochastic control process is called Markov decision process (MDP) in which includes a set of possible states, a set of transition model for moving one state to another one, a set of possible actions to determine the next state and a real-valued reward function for a decision, resulting in a specific action [131]. S. Zang et al. used MDP algorithm to optimize the handover management and improve the quality of

experience for the users. The method defines a three-dimensional state as network connection to MBS or SBSs, location of mobile user in $x - y$ plane and the velocity of the user in that plane. Then, a two-factor action was taken considering the user network connection and receiver beamforming beam width with attributed rewards which include the characteristics of mmWave communications. The reward purpose is to decrease the beam-formed signal blocking and beamforming misalignments which could be considered as QoE. Maximizing the reward function has been achieved for high and low mobility situations which has better performance in comparison with traditional schemes. Also, reducing the action space by eliminating the beam width factor has reduced the complexity of the MDP and has decreased the processing time [119]. B. Canberk et al. studied the handover management with delay approach to avoid the mobility interruption in eMMB services of virtual EPC (vEPC) with $4ms$ end-to-end (E2E) delay constraint in 5G networks. The study on mobility interruption would be incomplete if core and edge delays are not considered along with the three stages of a handover, consisting of preparation, execution and completion processes. The authors have designed a software-defined ultra-dense network (SUDN) which eliminates the execution stage and makes use of four states instead of seven states. The proposed SUDN has increased the packet delivery ratio and E2E delay by decreasing the time complexity process and memory usage in the network [132]. In addition, the predictions about the future locations of the UE have shown great improvements in handover procedures (see HMM methods); hence, they could be used as the states of a Markov chain. Prognosticating the location of a user was achieved by studying the movement behaviors of the mobile user which is deduced from the information about the previous locations and movement histories of the user [133].

4.1.1.2 Hidden Markov model The hidden Markov model (HMM) is similar to Markov model with nuance differences. The HMM takes the unknown and imperceptible parameters to the account to model the system; hence, the challenge becomes the effort to obtain these hidden parameters which cannot be observed directly. In the other word, HMM is a probabilistic model in which the sequences are generated by coexistence of two stochastic processes [134]. One of the processes moves between the states of the model, and the other process generates the system output corresponding to that state for indirect recognition of unobservable system. However, HMM is also memoryless like Markov model. The HMM has been extensively used to investigate the handover procedure and optimize the network parameters.

The handover could be triggered using the estimation of received signal and considering the trajectories of the UE. He et al. proposed an adaptive handover trigger strategy (AHTS) to estimate RSSI and guarantee the precise handover trigger. First, the movement patterns of the users were classified to predict the users' trajectories and then, the HMM was trained to predict RSSI which decreases the unsuccessful handovers in the system [107]. The more precise the trajectory, the better the training and hence successful handover is achieved. (The prediction of the user movement behavior--based on user's life style--was improved by HMM to increase the accuracy about the points of interest [135].) Yap et al. applied the predicted behavior of the user's visiting points to

find the proper target BS where the number of handovers and the received signal quality have become the evaluating parameters [136].

4.1.2 Stochastic geometry methods

Since the quality of received signal from neighbor base stations is the main criterion to proceed the handover procedure, a new model was proposed based on this parameter considering the UE's velocity and base station coverage area. Then, the effects of classic handover parameters such as TTT and sampling period on the performance of L1/L3 layer were investigated and the closed-form expressions were extracted for probability of handover failure and probability of cell selection in ping-pong conditions under fading channels for different scenarios [137]. In the other approach, the same model was exploited to introduce radio environment map (REM) algorithm based on the UE's trajectory, which stores local distribution of RSS average in each cell. This method decreases the number of ping-pong handovers by at least 10% in different scenarios without any influence on the handover failure [138]. To decrease the handover rate while maintaining longer connectivity duration, R. Arshad et al. considered four strategies to ignore some of base stations in the network as follows [139]:

- *Best connected strategy*, in which the UE is always is connected to the BS with the best RSS.
- *Femto skipping strategy*, in which the UE ignores some of the BSs based on the trajectory.
- *Femto disregard strategy*, in which all BSs within Femtocells are compromised for handover.
- *Macro skipping strategy*, in which some of BSs are ignored in high-speed scenarios.

The velocity-aware model was employed to evaluate the mentioned strategies via the help of stochastic geometry which aimed to enhance the average rate of the UEs. It is implied that the introduced strategies improve the network performance by compensating the destructive effects of handover procedures in high-speed scenarios with dense cells. The authors in [120], derived the closed-form expressions for handover rate and coverage probability in HetNets consisting of active BSs in mmWave (M) and μ Wave (μ) frequency bands, with distribution intensities of λ_M and λ_μ . They showed the relationship between handover rate and coverage probability under handover between these frequencies indicated by $HO_{\mu 2M}$, $HO_{M 2M}$, $HO_{M 2\mu}$ and $HO_{\mu 2\mu}$ conditions where the $HO_{\mu 2M}$ and $HO_{M 2M}$ increase by λ_M but $HO_{M 2\mu}$ experiences reduction, the $HO_{\mu 2\mu}$ is not influenced by λ_M , as well. As an outcome, if the blockage of radio link is the matter of important, it is favorable to increase the number of mmWave links, whereas the μ wave links could coexist with mmWave links in trivial situations. Likewise, a closed-form expression was obtained to specify the number of beams within a cell or a mobile terminal to optimize the area spectral efficiency (ASE). This beam management considers the antenna configurations, signal propagation, physical layer, coding, interferences, resource share and mobility management all together [121]. H. Zhang et al. derived the formula of handover probability for user plane and control plane based on multi-connectivity in dense

cellular networks. In this method, the UE is connected to several APs where the best AP remains as an anchor to establish the connection with control plane and causes 40% reduction in handover rate compared with the classic handover [115].

4.1.3 Other theoretical methods

Regarding the rigorous susceptibility of mmWave frequencies to blocking, even a temporal passing of a human or a vehicle could cause RLF. A simple way to overcome the problem is to cover the target area with a lot of BSs so that the blocked radio link would be replaced by the others to keep the integrity of the communication. The $M/GI/\infty$ queuing system was proposed to calculate the duration, rate and probability of channel blocks at the presence of temporal blockers where M indicates the arrival of blockers with Poisson distribution and GI is the distribution of blocking time which depends on the velocity and moving direction of the blockers. The authors showed that the minimum number of BSs to satisfy the QoS for URLLC applications is dominantly determined by the channel blockers and delay, instead of coverage probability or channel capacity parameters [122]. To obviate the beam problem in mmWave communications, the effective beam coverage probability (EBCP) was introduced to calculate the probability that a UE is exposed to a serving beam after a while, under Gauss--Markov moving model. In this strategy, the decision to handover is made not only upon the received signal quality but also upon TTT and EBCP which reduces the handover rate by 35% without a significant impact on the throughput [123]. Apollonian circles and the straight line were the geometry elements to model the handover procedure in self-organizing networks (SON) and jointly analyze the RLF and ping-pong handovers [140], and it was revealed that the velocity of the UE and TTT has scaling and shifting effects, respectively. The individualistic dynamic handover parameter optimization algorithm based on an automatic weight function (IDHPO-AWF) was offered in [141] to estimate the handover control parameters (HCPs). The method uses bounded functions, namely UE's SINR, UE's speed and cell's load, and then, the output is prepared as an input for AWF to optimize HCPs. This can outperform the handover parameter self-optimization (HPSO) methods for different scenarios from the aspect of velocity. Recently, a bio-inspired algorithm similar to genetic algorithms was suggested to minimize the cost function for an aircraft dual connectivity problem, under model for predictive control (MPC) constraints [116].

4.2 Algorithm-based approaches

This subsection investigates the methods which acquire specific data as system input to process and decide about the actions. Then, a network parameter is used to evaluate the performance of the network under these decisions.

4.2.1 Learning algorithms

The growing complexity of 5G/beyond networks imposes substantial costs from the aspect of management and operational configurations. The artificial intelligence (AI) is a potential solution to manage the various parameters in cellular networks. The hindrances of employing AI were discussed, and the challenges of AI-enabled 5G/beyond networks such as training issues, lack of bounding performance, lack of explainability,

uncertainty in generalization and lack of interoperability were introduced in [142]. The machine learning, neural networks and deep learning are the dominant AI algorithms which have been the cases of study to evaluate the handover performance. The next discussions belong to this category.

4.2.1.1 Machine learning The network topology ceaselessly changes in cellular networks, due to continuous movements of UEs, and the proposed methods based on the stochastic models do not seem to have adequate performance. In a totally different approach, a multi-purpose learning method has been introduced in which the parameters such as delay, network load, service rate, price and energy cost are used as the inputs of the system instead of network stochastic data [143]. These parameters define the QoS and QoE in the network that are used to attribute a score to each BS. Then, the algorithm is evaluated by handover rate and satisfaction ratio which is defined as the proportion of the score of the selected BS to the score of the best BS that could have been chosen. This would help the handover rate while maintaining QoS/QoE. The handover data are also useful to specify the coverage areas in ultra-dense networks (UDNs). Since the manual drive test (MDT) is not proper for UDN, T. Zhang developed a four-stage algorithm---including data collection, pre-processing block, data mining block and localization block---to precisely determine the coverage area based on the UEs' handover information [144].

To select the best BS based on data rate, sojourn time and cell load indicators, an optimization problem was defined over the following conditions: RSRP of target Cell, RSRP of serving Cell, distance, UE speed, movement direction of UE, angle between UE and corresponding cell, maximum number of nodes that can be connected to a cell and the number of nodes connected to the corresponding cell. This problem has been solved by linear programming (LP) to keep delay under $1ms$ in 5G networks. The algorithm runs in two phases: data collection and handover execution, which reduces the handover rate by selecting the best BS [109]. Regarding the alternatively changes in link quality and the sensitivity of mmWave communications to blockages, M. Giordani introduced a novel method to trace the quality of communication link in such networks. On the knowledge of radio link quality, the prediction of rate, time and target BS to handover and also monitoring and adjusting the transmission parameters become easier. In traditional methods, the directions of all available beams are scanned in every orientation periodically in a duration of T_{PR} . In an enhanced method, first, every orientation is scanned to find the proper beam and then, the previous and next beams are scanned in duration of less than T_{PR} to modify the beam direction. The results have shown that the beam direction modification increases the data rate specially in scenarios including moving vehicles [124]. The mmWave links are very sensitive to blockages which cause the missing of LoS and sever decrease in received signal. A geometry method dependent on the angle of arrival (AoA) and angle of departure (AoD) of the beam could predict the occurrence time of LoS blockages and duration of the blockage. This could lead into an on-time handover decision and avoid the unnecessary handovers [125]. A. Alhammadi developed a method to recognize too early handovers, too late handovers and wrong cell selections, and hence, TTT and handover margin (HM) could be determined based on RSRQ which decreases the ping-pong handovers and number of RLFs [145].

A supervised machine learning method was proposed for sub-6GHz with LTE radio access technology and with mmWave for 5G technology to increase the number of successful handovers. The method decides based on the previous successful handovers and the corresponding measurements such as location data, distance, present RSRP and previous ones. Not only the successful handovers are increased but also the requirement of measuring the signal quality between different RATs are decreased [113]. It is favorable to prevent throughput decline while reducing the number of handovers. Zhao succeeded to decrease the number of handovers compared to the classical handovers via a multi-connection algorithm which estimates the received signal quality. This method is composed of preparation, decision making and execution stages in which the received signal quality measurements are prepared by UE for estimation and finally for decision so that the connection between one or more BSs is created [117]. However, such algorithms that use the received signal quality for handover management would not meet the QoS requirements in telecommunication networks. Considering the complexity of QoS-based methods, the SDN technology was applied to make decisions regarding the attributed scores, based on RSS, delay, bandwidth, application type based priority, block error rate and jitter. This method enhances the network throughput by reducing the controlling messages and handover rate [110].

Despite the Q-learning methods which include one neural network as a nonlinear approximator function, a new learning method was exploited which uses a linear approximator function for state--action pair. The goal of reward function is to jointly optimize the throughput and latency. This method reduces the unnecessary handovers by 20% and the delay by 58% and improves the throughput up to 12%, while the number of handover failures comes to zero [146]. The frequent handovers are one of the main challenges in ultra-dense networks due to their high dynamicity. An online learning called Cost-aware Cascading Bandits Neighbor Cell List (CCB-NCL) configuration algorithm was introduced to reduce the number of scanned BSs and shorten the length of NCL which decreases the signaling costs and latency of handovers [147].

4.2.1.2 Neural networks Inspired by the performance of human brain in which billions of integrated neurons process the input data, a neural network is formed of an input layer, one or two hidden middle layers and an output layer. The relation between the neurons is specified by given weights. A neural network with the mentioned properties could be used as a global approximator to approximate any favorable function. These networks are employed in situations that the number and type of data entries are too vast to estimate, or predicting the functions/relations between the untold number of input data are too complex [148]. This complexity is the main reason for the attention on neural networks in management and configuration of the parameters in next generation of telecommunications networks specially in handover procedures which need jointly configuration of many parameters.

Zineb et al. [149] investigated a neural network composed of two subnetworks in decision making for handover trigger: The first subnetwork estimates mean opinion score (MOS) as QoE indicator from the gathered data about QoS indicators, such as user's data rate, delay, latency and jitter, and the second subnetwork decides about the handover trigger based on QoE indicator of first subnetwork's output, RSS,

SNR, battery charge level, velocity and QoS classes. The proposed vertical handover method has shown improvement compared with the fuzzy methods and multi-attribute decision making (MADM) [150] by decreasing the number of handovers and packet loss ratio. Likewise, Schmidhuber trained a recurrent neural network using long short-term memory (LSTM) [151] via the help of RSS to connect the UE to three close target BSs in which the proposed algorithm makes a correct decision on choosing the right target BS in 98% of the scenarios [152]. A mobility prediction algorithm including neural networks and Markov chains was combined with an online Lyapunov-based optimization solver to specify when and where the computation services (Virtual Machines) migrate in vehicular 5G networks [153].

4.2.1.3 Deep learning It can be interpreted as a branch of machine learning which is based on neural networks and the word “*Deep*” indicates the existence of several layers in these networks. The purpose of these layers is to distinguish the linear and nonlinear relations between the inputs accurately and to learn the characteristics from the raw data. Similar to the neural networks, the learning could be supervised, semi-supervised and unsupervised [154]. Regarding the complexity and heterogeneity of 5G and the next generation of cellular networks and also the increasing size of effective and usable data for configuring network parameters [155], the deep learning algorithms have attracted the attentions of many researchers.

Deep learning algorithms are very beneficial in predicting the handover failures, UE’s velocity, UE’s location and the proper time to handover. S. Khunteta has designed a two-stage learning algorithm to predict the successful and unsuccessful handovers based on RSRP and RSRQ. The first stage makes an estimation about the channel condition via recurrent neural network of type LSTM, and the second stage classifies the handover procedure data in successful and unsuccessful categories based on the first-stage data. The second stage itself applies feed forward neural network (FNN) and K-nearest neighbor (KNN) in which FNN shows better performance for simulation cases with equal successful and unsuccessful handovers. But for real data with lower unsuccessful handovers, KNN outperforms FNN. This method has proven that the handover failure could be predicted several hundreds in milliseconds which is very workable for handover procedure [156]. In another method, Shubyn predicted the UE’s movement behaviors from one coverage area in a BS into another one, via recurrent neural network process. Using an altered network called gated recurrent units (GRUs) instead of traditional recurrent neural networks with low memory has increased the prediction accuracy about UEs’ traffic data up to 90% [157]. M. Elkourdi proposed virtual cell (VC) and coordinated multipoint (CoMP) as the proper solution to maintain the radio link quality in the cell edge of BSs which seems very lucrative for next generation of cellular networks to avoid the data rate reduction. The time to trigger and selecting the BS in activating this protocol has been very challenging. A GRU-based algorithm was taken to account for on-time activating/deactivating of VC. In this method, the next RSS is estimated regarding the previous information about RSS and activation of VC is learnt which implies a 92% success for on-time activations [158]. Deep learning method has been utilized for next-generation SONs for handover procedure in which the data relating to all layers of protocol stack are

taken to account in decision process. A multi-layer LSTM with the mentioned characteristics has been trained in decision process to improve QoE which provides 18% improvement in comparison with classical handover which considers received signal quality for decision making [159]. Besides, an autoencoder and a multi-layer perceptron (MLP) neural network were added to traditional LSTM to accurately detect the nonlinear dependents of input data. Likewise, the handover procedure was modeled by MDP in which the selection of BS has been considered as an action and the RSRQ from serving and other cells forms the state vector of the system. Then, a reward is defined as the proportion of throughput to the handover rate in the reinforcement learning algorithm, and the optimization problem is solved via the help of recurrent neural network of kind LSTM. Since all of the users participated in the learning algorithm, the speed and accuracy of the learning increased [160].

Due to urgent demand on efficient mobility management algorithms in beamforming nodes in 5G, a deep learning method based on the dynamic optimization of the network parameters has been explored. In this method, two neural network has been considered: The first one estimates the location of UE, while the second one is used for handover management through the whole network [161].

4.2.2 Fuzzy logic

The fuzzy logic belongs to multi-value methods capable of taking any real number between zero and one. Besides two concepts: the absolute rightness for “1” and absolute wrongness for “0,” a partial rightness could be realized for any real number between zero and one. The fuzzy logic as a flexible and adaptable method is utilized in wide variety of engineering applications. Its privilege is to manipulate the mathematical models of the phenomena based on verbal expressions. That is, the performance of a system is described by verbal expressions. A fuzzy logic is composed of three main phases: a) fuzzification: in which the crisp numbers as the system inputs are converted to fuzzy sets; b) inference engine: in which the input data is processed based on “if-then” rules; and c) defuzzification: in which the outcomes as the fuzzy sets are converted to crisp numbers [162, 163]. Various parameters corresponding to the handover procedure could be processed to make a decision via the help of fuzzy logic. E. Cardoso et al. proposed a fuzzy logic system which triggers the handover procedure in SON by an intelligent adjustment of A2 entrance condition threshold. The system includes 48 base-rules on the velocity of the user, RSRQ and the current A2 entrance condition threshold to predict the subsequent threshold. This dynamic threshold controlling decreases the handover rate specially for high-speed users [164]. Although considering diverse inputs in decision making could enhance the handover performance, it increases the number of base-rules which results in complexity and delay in the system. Zhao has proposed a three-layer hierarchical fuzzy logic based on the physical layer requirements with SDN capability to solve this problem: the first layer as mobility fuzzy logic controller, the second layer as network fuzzy logic controller and the third layer as personalized fuzzy logic controller. The first layer extracts the user’s sojourn time in serving cell based on the distance between the user and BS, velocity and direction, the second layer gets RSSI, throughput and the output of the first layer as the inputs and returns a QoS metric, and finally, the third layer considers the monetary cost, user specific QoE preferences

and application-specific requirements to select the proper BS using a fuzzy set as {Accept,Probably Reject,Probably Accept,Reject}. This method decreases the number of handover rate in the network [111]. Liu achieved the handover management through the optimized weighting of decision factors based on network and service type and user configurations in HetNets including 4G, 5G and WLAN. In this method, the received signal quality, network traffic, available bandwidth, energy consumption and packet loss rate were optimally weighted as the key inputs to a fuzzy logic controller for final decision. Choosing the proper type of network and BS improves the handover from the aspect of delay, by decreasing the number of handover rate and increasing the network throughput [165]. Another method called weighted fuzzy self-optimization (WFSO) [166] considered SINR, traffic load of serving and target BSs and UE velocity to exploits 27 base-rules (less rules than [164]) in handover decisions. WFSO acquires the appropriate TTT and threshold value to begin handover which could decrease the RLFs, average handover failures and number of ping-pong handovers. On the other hand, O. Semenova has proposed the neuro-fuzzy controller (NFC) including 27 base rule for 5G networks in which RSSI, the distance between UE and BS and the velocity of the UE have been used as linguistic input parameters to make term for the handover indicator. Considering three terms as low, medium and high for each of the inputs, HI is evaluated by five terms: very low, low, medium, high and very high. Then, the fuzzy handover technique is optimized via the five-layer adaptive network fuzzy inference system (ANFIS) which incorporates the fuzzy handover with a learning element. The ANFIS decreases the handover failures, and the learning element improves the BS selection among many other BSs by providing a proper time for handover trigger which could decrease the unnecessary handovers [167]. Gong incorporated the fuzzy logic system and gray correlation analysis to combine the long-term network stochastic data and instant handover data in decision process. The method exploits RSS, sojourn time in small cell and traffic load of BS which results in reduction of unsuccessful and ping-pong handovers [168]. The BSs in Cloud-RAN (CRAN) are divided into base band unit (BBU) and remote radio head (RRH). The densification of short-range RRHs and mobility of UEs cause frequent handovers. Rodoshi et al. used fuzzy logic to optimize the handover parameters such as TTT, and then, they chose the best RRH via reinforcement learning method with accelerating technique (virtual reward) for faster convergence [169]. This can handle the mass of control messages by reducing the unnecessary handovers before re-association of UE to the RRH.

4.2.3 Game theory

The game theory as a modeling tool comprises players, actions, payoffs and information known as rules of the game. The modeling purpose is to express a situation based on the rules of the game theory, which results in the recognition of the happenstance in a specific situation. Each player tries to increase its productivity in decision making processes. In fact, the game theory models the performance of the players who affect the other players' performances; hence, if there is no influence on each other, the game theory becomes useless [170]. In cellular networks, the UEs act as the players in game theory approaches.

Peddi et al. exploited the game theory and introduced media independent handover (MIH) in which the handover procedure begins if the UE experiences a severe decrease in received signal quality. Thus, the achievable data rate, battery power and bandwidth have been taken to the account to set up a handover, which results in lower delay and higher performance [171]. S. Goudarzi et al. also applied MIH in cellular networks where the UAVs are used as BSs. The proposed algorithm maximizes QoS while decreasing the handover costs by recognizing the proper UAV selection. The optimization problem is solved with game theory approach in which the UAV saves more energy while providing more coverage area for the users. This method uses the SDN technology to keep an integrated connection during the handover and to decrease E2E delay and the control messages resulting in higher throughput in the network [172].

4.2.4 Big data

The big data includes the collecting and analyzing the set of data which is extraordinary huge, diverse or complex and cannot be processed with traditional methods. Using big data leads into discovering delicate patterns and heterogeneity between components and inputs which is impossible in small-scale data [173]. Daily increasing active users in telecommunication networks and the variety of inputs and parameters in optimal configuration of these networks have exposed the algorithms and methods based on big data to be very appealing for the researchers in recent years.

Cia has gathered the information about data traffic and movements of urban vehicles in London via sensor networks to specify TTT and handover improvement. The big data was exploited to optimize the handover range expansion bias for HetNets and the number of virtualized mobility management entity (MME) which decreases the ping-pong handovers and increases the spectrum efficiency [174]. The search time to find the appropriate beam direction using the stored data about previous beams increases the beamforming efficiency in both line-of-sight (LoS) and non-line-of-sight (NLoS) directions. This causes delay and discontinuity in data services. M. Huang proposed a two-stage algorithm based on big data in which the data about previous handovers are adjusted and managed via a learning algorithm in the first stage, and the appropriate beam selection is executed using the data about previous UEs' handovers, while a new UE enters the handover region in the second stage of the algorithm. This process is achieved needless to new measurements and decreases the delay specially in NLoS conditions [126].

4.2.5 Other algorithmic methods

To improve handover procedure and equipoise the load between two BSs while keeping the QoS, the BS capacity, UE's trajectory, received signal quality and data traffic are the essential parameters in reduction of delay and packet loss during the handover [65]. Also, a simulation was provided to determine the relation between the velocity of UE and the number of handover rates [175]. For the heterogeneous networks with dense small cell BSs, downlink SINR, user transmitted power, cell capacity and predicted time of stay (ToS) are collected for the stations with $RSRP < RSRP_{th}$ conditions and the corresponding equivalent weighted vector is formed by analytical hierarchy process (AHP). Then,

the gray rational analysis (GRA) ranks the BSs to find the best station which decreases handover frequency and RLF and improves the energy efficiency compared with the traditional methods [176]. In a recent study, a six-stage algorithm consisting of configuration, decision making, filtering, narrowing, selecting the highest RSSI and handover triggering phases was represented for dense heterogeneous 5G networks which adapts with the UE's characteristics such as velocity, direction, sojourn time and traffic load. This algorithm increases the UE's data rate but decreases the handover rate compared to the similar methods based on RSSI measurements [177]. A recovery process is executed if RLF is recognized in the network. Although RLF recovery timer (T_{312}) accelerates this process, it cannot guarantee an access stratum (AS) and eliminates the disconnection time completely. An event-based RLF trigger was proposed which decreases the recovery time and approximately cancels the disconnection time [178].

4.3 Experimental methods

Due to dense establishment of base stations with different technologies in HetNets, and also, due to effect of different parameters and criteria in handover management, the proposed theoretical approaches to control and management of handover do not divulge an optimized performance in many real scenarios. To measure the involving parameters of the handover more precisely, the researchers have developed hardware to extract various data in real scenarios, such as received signal quality in different frequencies and directions, velocity and UE's moving direction. Such experimental data provides a better overlook at HetNets and 5G networks to analyze and obtain effective algorithms. Also, this data is very helpful for learning-based algorithms in handover management.

To evaluate the performance of ultra-dense networks based on geographically localizing the active UE, USRP X-series was employed which makes the integrated handover possible. It was shown that the UE's location could be followed by measuring received signal quality in the uplink so that the handover is initiated by the network. That is, the initiation and handover management using UE's location would be feasible for next generation of telecommunication networks [179]. The authors in [180] studied road trip time (RTT) and uplink throughput and the effect of handover interruption time on these KPIs and highlighted the inefficiency of some KPIs in practical situations. Collecting the related data was achieved in duration of three month via the help of MONROE platform in urban and rural environments, which implies that the handover interruption time has deep impact on RTT, whereas its effect on throughput could be negligible. Recently, a testbed was experimented to evaluate performance of fast handover in a vehicular communication system on a highway, in 22--23 GHz frequency bands, as well [127].

4.4 Summary of handover management

According to the above discussions, each method includes some advantages and disadvantages. Due to variety of scenarios and diverse configuration of many parameters corresponding to the handover, preparing an analogy between the papers for specific parameters would not be a reasonable comparison. Thus, we provide two different analogies for discussed approaches: a table to clarify which algorithm and which KPIs have been included in the paper and a figure to demonstrate the characteristics of applied

the UE [183]. To solve the problem in 3G networks, the AKA and the mutual authentication mechanism were added to the procedure [184]. The key agreement is to generate a secret key based on a given procedure in two or more devices. However, the authentication was improved in 4G networks by applying universal mobile telecommunication system AKA (UMTS-AKA) compared with the third generation [185]. Providing an effective performance, the AKA has been employed in 5G networks with trivial changes and improvements to be harmonized with the new structure of these networks [28]. Regarding the deep separation of user plane and control plane and also, introducing the structures, based on the network function which considers one specific responsibility per function, the authentication server function (AUSF) is in charge for authentication. As an example for improvement of 5G-AKA, the generated key in AUSF could be used for 3GPP and non-3GPP connections without any re-authentication procedure. Since the number of handovers would be increased due to existence of plenty of smallcells, it is obvious that consequently the number of authentications increases and as a result the network costs grows severely. This makes the authentication an important procedure in 5G handover management.

5.1 Authentication mechanism

In order to secure the communication link in telecommunication networks, the authentication/re-authentication is needed during connecting/re-connecting of the UE to the network. To connect the UE to the target BS in handover procedure, the re-authentication has to be done which includes different scenarios based on the source and destination radio access technology and the authentication units in that service provider. The common model for handover key chaining is depicted in Fig. 8 [33]. Based on RAT, three different states happen during authentication as follows:

Intra-5G-NR (LTE-EPS): In this case, the target and serving cells share the same radio access technology. To insure a secure channel between UE and gNB, the AMF unit and UE have to obtain the K_{gNB} and next-hop (NH) parameters from K_{AMF} . Regarding

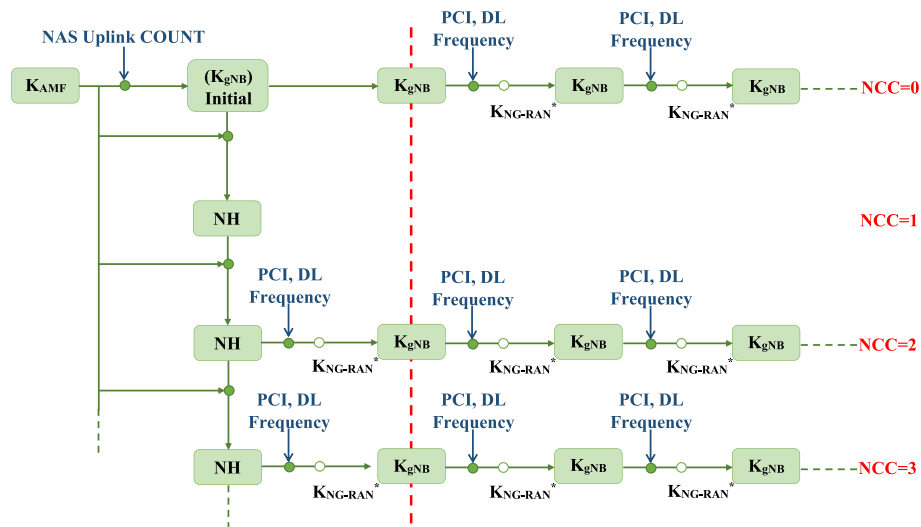


Fig. 8 Model for the handover key chaining

the corresponding units and BSs during handover, the key generation and authentication comprise three cases as follows:

- *Intra-gNB-CU (intra-ng-eNB) handover*: where the gNB decides upon a predetermined policy to insure which condition is proper to use existing K_{gNB} and which condition is proper to use new one. The UE is informed by gNB via a handover control message to use the existing key or generate a new key. The issued algorithm in Annex A.11/A.12 [33] is used to generate the new key, if needed.
- *Xn handover*: where the serving BS generates the new key on the knowledge of $\{NH, NCC\}$ pair. The algorithm in Annex A.11/A.12 [33] computes the K_{NG-RAN} key and sends the $\{K_{NG-RAN}, NCC\}$ pair to the target BS via Xn interface which is used when the UE connects to that BS. At the end of handover procedure, the NGAP-PATH-SWITCH command is sent to the AMF to update the UE's condition and to be used for generating new keys in next handover procedures.
- *N2 handover*: where the AMF unit of serving and target BSs are different. If the AMF in the serving BS does not change the active K_{AMF} and it is not necessary to generate AS key, the AMF generates the key based on specified algorithm in Annex A.11/A.12 [33] and sends $\{NH, NCC\}$ pair to the target BS to be used in handover procedure. If the serving AMF has activated a new K_{AMF} , then a new AS key is needed to be generated in UE and this process is achieved by serving AMF policies.

Note that the authentication procedure is the same for all above scenarios from the aspect of the UE.

Inter-3GPP: In this case, two scenarios could happen depending on the serving and target BSs as follows:

- *Handover from 5GC to EPS*: where the UE is connected and registered in 5G network and a security context is assigned to UE by the network. This information is sent to the MME of target cell via N26 interface so that it is convinced that the AMF of serving cell is a MME, as well.
- *Handover from EPS to 5GC*: where the UE is connected and registered in 4G network and there is a security context in MME of serving BS. Receiving a handover message, the MME checks whether the UE's security is capable of connecting to the 5G network or not. Thus, the MME sends the information to AMF which is need to generate security context.

3GPP and non-3GPP: Another authentication unit has been considered in 5G networks to support the IoT devices with lower process and power consumption which employ Bluetooth or WiFi protocols for communications. The security of connection between non-3GPP and 5G network has been satisfied via IKEv2 to setup one or more IPsec ESP security associations. In this condition, the UE starts IKE request and non-3GPP interworking function (N3IWF) responses to IKE request. Also, the AMF generates the K_{N3IWF} from K_{AMF} key and sends it to N3IWF which is used for authentication between UE and N3IWF.

5.2 Authentication enhancements

Due to a plethora of BSs with small coverage areas and high-speed users specially in 5G networks, the frequent authentications during handovers bring new challenges such as security gaps, security attacks, throughput reduction and increasing delay. Various protocols and mechanisms have been proposed to achieve faster and more persistent solutions for the mentioned problems. A mobile relay node (MRN) was introduced to reduce the authentication overheads in 5G high-speed rail networks by fixed-trajectory group pre-handover authentication (FTGPHA) schemes based on aggregate signcryption technique. In this scheme, the next BS could accomplish the authentication before the arrival of MRNs and achieve a seamless handover [186]. The authors in [187] proposed a new authentication and re-authentication protocol for group-based handover which deals with multiple UEs' requests in mMTC applications while improving the bandwidth and controlling messages. A fast SDN-based authentication using EAP-TLS was exploited to directly request a certificate from the external network instead of requesting from certificate issuance unit. Thus, it is more persistent against stealing identity, denial-of-service (DoS) attacks and MitM [188]. To overcome the security challenges, a new protocol called distributed IP mobility management (DMM) was introduced which depends on layer two and performs mutual authentication, confidentiality, integrity, key exchange, privacy and defense against redirection attacks by malicious AMF or CMDf [108]. W. Haddar introduced a new authentication method for the equipments with PMIPv6 protocol to provide a robust authentication during handover from LTE to WiFi network [189]. The security gaps from the aspect of location and the time of occurrence were investigated by demarcation of possible points for handover based on SINR [190, 191]. A temporary encrypted identity was used in initial access and subsequent authentications to reduce the computational load by 50% in V2X networks [192]. The authors in [193] updated EAP-AKA for frequent handovers in 5G networks which jointly reduces the delay and increases the security. Merging MIH and F-PMIPv6 led to new protocol, called MIH-based secure cross-layer handover protocol for Fast Proxy Mobile IPv6 networks (MIH-SPFP) which has the capability of decreasing the re-authentications during handover between inter-mobile access gateways (MAG), resulting in lower delay [194]. It is expected that a wide variety of devices join the 5G networks with different capabilities. Hence, to decrease the authentication costs, an authentication handover module is embedded in the SDN controller as an application to follow and monitor the location and movements of UE and prepare the authentication requirements before handover [112]. Also, a multi-purpose mutual authentication was used to achieve handover between 5G and non-3GPP networks via the help of Chameleon hash function and blockchain [195]. Recently, a region-based secure handover with user anonymity and fast revocation properties overcame the delay problem caused by authentication key exchange (AKE). This was achieved by issuing a region warrant with revocation possibility at the arrival of UE to a macrocell region, to revoke the UE's warrant if needed [196]. A joint optimum and secure authentication during handover to neighbor cells was achieved via Chinese reminder theory in [197], which counteracts the fake base attacks while reducing the energy consumption for high-speed users. The Chinese reminder theory was introduced for neighbor radio stations in 5G networks which is highly secure against the fake base station and DoS attacks while reducing the energy consumption and delay which

makes it an appropriate method for high-speed scenarios [198]. D. KWON et al. used elliptic curve cryptography in key agreement process in urban air mobility (UAM) scenario which is capable of terminating malicious or misbehaving UAVs. Real-or-random, Burrows–Abadi–Needham (BAN), automated validation of internet security protocols and applications (AVISPA) were used to prove the efficiency of the proposed method [199].

5.3 How to tackle the attacks

The security attacks on telecommunication networks predicate the set of impermissible actions to access, steal, alter and destroy data or network facilities. These attacks are divided into active and passive categories. The passive ones intend to access or steal data illegally without making changes or destruction of data or network infrastructure, and the main reason for these attacks is to trespass the confidentiality of data and UEs' privacies. On the other hand, the active attacks intend to ruin data or make disruption in the network infrastructure. In the following, we investigate the network vulnerabilities confronting the various attacks related to the handover procedure and the methods to counteract them.

5.3.1 Fake base station

The experiments show that the device capabilities are exchanged in the first connection to the network before authentication and without any security actions which could be used for further attacks [200]. The main goal of illegal radio base station or IMS catchers is to obtain the IMS information of UEs [201]. So far, there is no mechanism for UE to confirm the legitimacy of a BS in the first connection [202]. Lack of authentication in the first connection of UE to a high power quality BS allows the attacker to create an illegal BS for UE and make UE connect to that BS [203]. However, the composition of absolute priority-based cell reselection in eighth edition of LTE makes it possible for the attacker to foist itself as a high-priority BS by proper frequency configuration and compels the user to connect to itself even without meeting high-quality requirements [204]. Since the IMSI is not coded in 2G, 3G and 4G and is transmitted via a simple text message, it can be easily revealed for the illegal BS and to be used in further attacks. In 5G, a subscription permanent identifier (SUPI) is used to overcome the problem and an encoded version, called subscription concealed identifier (SUCI), is employed during a connection to a BS. Even in a wrong connection, the obtained data would be useless [33]. S. Gupta studied the characteristics of authentication in 5G networks and security vulnerabilities against fake base station and de-synchronization attacks [205].

An illegal BS could disrupt the network performance in addition to the data abduction. Most of the time, the handover is achieved according to the UE's received signal quality. This measurement is accomplished based on the SS block which contains a synchronous message/signal and master information block (MIB) signal without any protection. Suppose that the illegal BS C counterfeits itself as a legal BS B; hence, the serving BS A receives the corresponding MR containing the channel status of station C and assumes that the signal belongs to the station B, instead. Then, a handover command to the fake station B is released and the UE is connected to the station C. Since the station C does not have the security content of the UE, the UE disconnects itself from that base station.

But the station C is also capable of doing more attacks during this interval [201]. To solve the problem, a secondary measurement on channel state information reference signal (CSI-RS) is accomplished which is prepared by target BS for UE. Since the station C does not have any information about CSI-RS, the measurement will be done on the signal quality of station B. This time-consuming procedure which increases the delay in the network could be achieved in two manners: always-on and on-demand. The on-demand manner is executed if the number of handover failures exceeds a standard number in the network [206]. Saedi et al. presented a simulator to create a data set pertaining to the signal quality received from legitimate and rogue BSs, in 5G networks. The data set is used to train the algorithms in recognizing the rogue BSs [207]. Lee et al. proposed a blockchain-based method to insure the security of the network. The authors studied the fake station approaching by two aspects; if the fake station tries to join the network, it needs the block info from blockchain and cannot join if it does not have (even if the base station has copied all info about the identity of a legitimate station containing the block info), the lack of IP sessions in the new base station will result in handover failure [208]. Also, a learning algorithm called light-GBM has been applied to recognize the fake BS by network main parameters such as RSRP, system information block (SIB) [209].

Nyangaesi et al. decreased the delay using globally unique temporary identifier (GUTI)-based multi-factor authentication which is highly tolerable against DOS attacks, de-synchronization, session hijacking, masquerade and network impersonation during handover procedure. These factors include the information about next chain counter (NCC), next hop (NH), key derivation factor (KDF), physical cell identity (PCI), EUTRAN absolute radio frequency channel number on the downlink and randomized root key in GUTI algorithm. The GUTI solves the updating problems in LTE-AKA networks. Also, the environment has been classified into no handover region, low-probability handover region (LPHR) and high-probability handover region (HPCR) in which the time schedule based on the figure of merit prevents the DOS attacks. The figure of merit facilitates the handover in HPCR [210]. One of the fundamental attacks to UE's privacy is the abduction of UE's indicators which is used to recognize and follow UE. Nakarmi et al. have proposed multi-RAT false base station detector to recognize the false base station based on the UE's measurements which is compatible with all available radio access technology of 3GPP without any changes in UE. To this, some rules are written according to the network topology and UE's received signal quality and are used during handover procedure [211]. The group handover seems inevitable in densely crowded areas such as the presence of many UEs in a stadium or in a traveling train. The newfound drone-mounted BS technology was applied to achieve a group handover considering that the credential sharing step is called off between serving and target BSs to decrease the power consumption and handover delay. Since a fake base station can take the role of drone-mounted BS, the UE converts a public key to a private key by powering operation in the elliptic curve group to secure the authentication process [212].

5.3.2 *Replay attack*

In this kind of attacks, the attacker retransmits the previously communicated messages to make the device respond to a non-existing request. This could cause the message or request overflow in the receiver, DOS attack or stealing information [213]. The handover

procedure is highly vulnerable against replay attacks. When a handover request is sent to the target BS from serving BS, the attacker sends the message containing $\{N_{cc}, K_{gNb}\}$ to the target BS. Hence, the UE, which has received the duplicate $\{N_{cc}, K_{gNb}\}$, proceeds the reconnection since the UE perceives the handover failure during the authentication procedure [33].

Alam et al. represented a random Nonce method in UEs to confirm the freshness of the messages in the BSs which recognizes and prevents the replay attacks [214]. Likewise, Singh et al. improvised a fresh timestamp data in handover request message in addition to the exclusive key, during its transmission from serving radio to target BS which prohibits replay attacks [215]. Jover et al. used a signature in broadcasted messages to distinguish the legitimate and rogue base stations before retry for connection by UE. Also, they have added an indicator, representing the freshness of messages which prevents replay attacks [216]. Nyangaresi et al. used the hash mechanism for messages and timestamp when the attacker wants to manipulate the timestamp and show it as valid. Computing the hash by the attacker leads into a false result since the hash key is only available for UE and MME; therefore, the effort for altering the timestamp is not adequate for replay attack and the attack remains abortive [217].

5.3.3 Jamming attack

A jammer could be considered as a destructive node which intentionally makes interference in wireless cellular networks. Regarding the functionality of the jammer and its strategy in creating interferences, various types of the jammers could exist in the network [218]. A responsive jammer continuously monitors the wireless channel and only interferes when the transmitter is active and proceeds to send a signal [219]. Since the handover depends on different parameters and various messages are exchanged between UE, serving and target BSs, the jammer could fail the procedure by sending messages such as authentication message containing NCC or interfering in acknowledgment messages. Erpek et al. predicted the acknowledgment transmission time with deep learning method to mitigate the jamming attacks in a telecommunication network [220]. The physical layer of LTE/5G includes several physical channels and signals which carry special information in uplink and downlink for reliable and stable connecting and sending messages without interference over the links between UEs and base stations. Nonetheless, some of the jamming attacks on the physical channels disrupt the handover procedure.

In cellular networks, the synchronization, primary synchronization signal (PSS) and secondary synchronization signal (SSS) signals are very important in searching for BS which are used for primary connection before random access process and selecting and re-connecting during handover. Thus, any failure in receiving the correct synchronization signal leads into endless searching for BS. Since the location of this signal is known in the resource grid, the downlink is highly vulnerable against the jamming attacks [221]. Krenz et al. investigated the vulnerabilities of LTE networks against jamming attacks on physical channels and signals, such as synchronization signals. The experiments have been accomplished via USRP-NZIO as RF front end AmariLTE100 software. The authors have concluded that if the received jamming signal is 3dB greater than the main signal, the connection is dropped [222]. Regarding the structure of physical layer in LTE, the

jamming attack is not an optimum method to interfere the synchronization, PSS and SSS signals, because these signals have been designed by UE for low SNR conditions [223]. Lichtman et al. showed that spoofing the PSS signal and transmitting all three above-mentioned signals in physical layer frame by the attacker can prevent the access of new UEs to the BS [224].

The reference signals are sent in downlink frames via predetermined subcarrier to estimate the channel quality by UE. The UE would not demodulate the downlink frame/data at the presence of jamming on reference signals and, hence, cannot accomplish the handover procedure. But, it should be noticed that a successful jammer on these signals must have the previous information about the frames of the intended BS to find out the location of that signal in resource grid [225]. Likewise, Sodagari et al. concentrated on the jamming attacks on MIMO channels which distort the channel sounding signals like reference signals [226].

In wireless communication networks, the UEs connect to the BS via random access process to receive the service. During this process, a random access preamble is sent to the BS by UE in uplink channel. After receiving the preamble, the BS allocates the resources to the UE and the information is sent to the UE via PRACH signal to initiate the random access process [227]. The jamming attacks on random access signals deter the UE to connect to the network or create a new link in handover procedure. These attacks on PRACH signals have been introduced as the main vulnerabilities of LTE networks [228, 229].

6 Features and challenges

As studied in the literature, miscellaneous scenarios have been considered to evaluate the KPIs of the network. Many of the employed algorithms, particularly demonstrate an excellent performance for specific scenario, while they may fail to improve the KPIs in another scenario. It is inferred that finding a proper algorithm depends on the scenario and limited KPIs. Thus, it is vital to define a standard testbed to discern the algorithms and investigate the performance of the network and value of favorable KPIs.

The knowledge on the future location of the UEs would be very beneficial to proceed a successful handover. The Bayesian networks [230] have shown a good efficiency in predicting the future location of moving objects based on their movement histories [231, 232]. Due to lack of studies on the performance analysis of the handover management using Bayesian networks, the investigations on the combination of this method and algorithm-based approaches seem very interesting.

The fifth generation of cellular networks and beyond are expected to show a very dynamic topology due to the presence of high-speed users, D2D pairs and mmWave frequency bands. The combination of multi-connectivity method and D2D communications to achieve a seamless handover has not been studied, specially in the case that D2D pairs afford the signaling process, while multi-connectivity handles traffic. Nonetheless, a few studies have been done about finding uncorrelated links, in order not to lose primary and secondary links simultaneously. The method maintains a seamless handover, while it can be the cause of more energy consumption in the user and infrastructure facilities. That is, a trade-off between the energy consumption and

keeping multi-connections to provide an integrated service remains an open problem. In addition, the multi-path TCP has been introduced as a potential solution to reuse the resources where the UE could access to different RATs, but still the studies on the capabilities of this method in multi-connectivity and also considering the other layers' information such as RRC states in stack protocol for 5G networks, are insufficient or do not exist. Regarding the high sensitivity of mmWave links to the blockage, a precise 3D description of environment would be a potential solution for handover management before blockage. A 3D reconstruction of indoor space based on point clouds technique would be found in [233] which estimates the signal quality. Also, the authors in [234] used the point clouds technique to prognosticate the mmWave link quality. This method combined by machine vision seems very interesting for handover management in the next generation of communication networks.

On the other hand, the newly developed RIS technology has shown an outstanding performance in wireless communications, but the mobility management is still a challenging problem for RIS-aided wireless networks. Due to the rapid movements of the UEs, the BS may lose the connections unless agile mobility management schemes are used. Since RISs are passive elements, they cannot send pilot signals to track the movement of the users. Hence, it is much more challenging to track roaming UEs, especially when the direct links between the BS and the UEs are blocked. Additionally, it is expected that the combination of RIS-assisted networks with mmWave or D2D networks would be a potential solution to the stated problems.

Moreover, the researches in the network centric handover decision making, based on uplink channel sounding data and exploiting blockchain properties in authentication methods are in embryonic stages.

7 Conclusion

The forthcoming 5G cellular network and beyond are expected to host a great deal of gNBs within smallcells to provide a high data rate for UEs while satisfying the QoS requirements. The existence of numerous gNBs besides the UEs with different velocities is the causes for frequent handovers in the network which affects the network's KPIs. We have reviewed the handover mechanism and categories, and we have discussed how the handover impacts the performance of the network and vice versa and how the network implementation would affect the handover procedure. Also, we have addressed the handover issues, the proposed methods with different approaches, the advantages and disadvantages of enhancement techniques with various classifications, the authentication protocols and corresponding vulnerabilities in 5G networks. Finally, we have summarized the important challenges and future research directions.

Abbreviations

3GPP	Third-generation partnership project
AKA	Authentication and key agreement
AMF	Access and mobility function
AoA	Angle of arrival
AoD	Angle of departure
AP	Access point
AUSF	Authentication server function
BS	Base station

CHO	Conditional handover
CoMP	Coordinated multipoint
CSI-RS	Channel state information reference signal
D2D	Device-to-device
DC	Dual connectivity
DN	Data network
E2E	End-to-end
eMBB	enhanced mobile broadband
EPC	Evolved packet core
FAP	Femtocell access point
gNB	Next-generation node B
HO	Handover
HetNet	Heterogeneous networks
HMM	Hidden Markov chain
IMSI	International mobile subscriber identity
KPI	Key performance indicator
LoS	Line of sight
LTE	Long-term evolution
MDP	Markov decision process
MIH	Media independent handover
MIMO	Multiple input multiple output
MME	Mobility management entity
mMTC	massive Machine-type communications
MR	Measurement report
NCC	Next-hop chaining counter
NF	Network function
NGAP	Next-generation application protocol
NH	Next hop
NR	New radio
NSA	Non-stand alone
PSS	Primary synchronization signal
QoE/QoS	Quality of experience/quality of service
RAN	Radio access network
RAT	Radio access technology
REM	Radio environment map
RIS	Reconfigurable intelligent surface
RLF	Radio link failure
RRC	Radio resource control
RSRP	Reference signal received power
RSRQ	Reference signal received quality
RSSI	Received signal strength indicator
SA	Stand alone
SDN	Software-defined network
SE	Spectral efficiency
SIM	Subscriber identity module
SINR	Signal to interference plus noise ratio
SMF	Session management function
SNR	Signal-to-noise ratio
SON	Self-organized networks
SRS	Sounding reference signal
SSB	Synchronization signal block
SSS	Secondary synchronization signal
SUCI	Subscription concealed identifier
SUPI	Subscription permanent identifier
TTT	Time to trigger
UDN	Ultra-dense network
UE	User equipment
UMTS	Universal mobile telecommunications
UPF	User plane function
URLLC	Ultra reliable low latency communications
V2X	Vehicle to everything
VANET	Vehicular ad hoc network
VNF	Virtual network function
XnAP	Xn application protocol

Author contributions

Due to existence of multiple topics in the paper, the references of each section were studied separately by the authors, and finally, the investigations were gathered and the analysis and conclusions were derived after lots of discussions. All authors read and approved the final manuscript.

Funding

The authors declare that they have not used any financial funding.

Declarations**Competing interests**

The authors declare that they have no competing interests.

Received: 3 June 2022 Accepted: 9 June 2023

Published online: 22 June 2023

References

1. G. Liu, D. Jiang, 5G: vision and requirements for mobile communication system towards year 2020. *Chin. J. Eng.* **2016**(2016), 8 (2016)
2. M. Series, IMT vision–framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation ITU **2083** (2015)
3. 3GPP: 5g security assurance specification (scas); access and mobility management function (amf). Technical Specification (TS) 33.512, 3rd Generation Partnership Project (3GPP) (2019). Version 16.2.0
4. 3GPP: Study on enhancing topology of the service management function (smf) and the user plane function (UPF) in 5G networks. Technical Specification (TS) 23.726, 3rd Generation Partnership Project (3GPP) (December 2018). Version 16.0.0
5. M. Lauridsen, L.C. Gimenez, I. Rodriguez, T.B. Sorensen, P. Mogensen, From LTE to 5G for connected mobility. *IEEE Commun. Mag.* **55**(3), 156–162 (2017)
6. 3GPP: System architecture for the 5g system (5gs). Technical Specification (TS) 23.501, 3rd Generation Partnership Project (3GPP) (2019). Version 16.0.0
7. R.D. Kaliski, Heterogeneous network architecture and device-to-device communications in 5G cellular networks. *Wiley 5G Ref: The Essential 5G Reference Online*, pp. 1–24 (2019)
8. 3GPP: Non-access-stratum (nas) functions related to mobile station (ms) in idle mode. Technical Specification (TS) 23.122, 3rd Generation Partnership Project (3GPP) (2020). Version 17.0.0
9. 3GPP: Evolved universal terrestrial radio access (e-utra); user equipment (ue) procedures in idle mode. Technical Specification (TS) 36.304, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
10. 3GPP: Evolved universal terrestrial radio access (E-UTRA); requirements for support of radio resource management. Technical Report 36.133, 3rd Generation Partnership Project (3GPP) (2019). Version 16.0.0
11. 3GPP: Evolved universal terrestrial radio access (E-UTRA); radio resource control (RRC); protocol specification. Technical Report 36.133, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
12. D. Xenakis, N. Passas, L. Merakos, C. Verikoukis, Mobility management for femtocells in LTE-advanced: key aspects and survey of handover decision algorithms. *IEEE Commun. Surveys Tutorials* **16**(1), 64–91 (2013)
13. I. Shayea, M. Ergen, M.H. Azmi, S.A. Çolak, R. Nordin, Y.I. Daradkeh, Key challenges, drivers and solutions for mobility management in 5G networks: a survey. *IEEE Access* **8**, 172534–172552 (2020)
14. E. Gures, I. Shayea, A. Alhammedi, M. Ergen, H. Mohamad, A comprehensive survey on mobility management in 5G heterogeneous networks: architectures, challenges and solutions. *IEEE Access* **8**, 195883–195913 (2020). <https://doi.org/10.1109/ACCESS.2020.3030762>
15. A. Kose, H. Lee, C.H. Foh, M. Dianati, Beam-based mobility management in 5G millimetre wave V2X communications: a survey and outlook. *IEEE Open J. Intell. Transp. Syst.ms* **2**, 347–363 (2021). <https://doi.org/10.1109/OJITS.2021.3112533>
16. M. Tayyab, X. Gelabert, R. Jäntti, A survey on handover management: from LTE to NR. *IEEE Access* **7**, 118907–118930 (2019)
17. A.A. Ahmed, A.A. Alzahrani, A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology. *Trans. Emerg. Telecommun. Technol.* **30**(3), 3546 (2019)
18. M.S. Mollel, A.I. Abubakar, M. Ozturk, S.F. Kajjage, M. Kisangiri, S. Hussain, M.A. Imran, Q.H. Abbasi, A survey of machine learning applications to handover management in 5G and beyond. *IEEE Access* **9**, 45770–45802 (2021). <https://doi.org/10.1109/ACCESS.2021.3067503>
19. J. Tanveer, A. Haider, R. Ali, A. Kim, An overview of reinforcement learning algorithms for handover management in 5G ultra-dense small cell networks. *Appl. Sci.* **12**(1), 426 (2022)
20. J. Angjo, I. Shayea, M. Ergen, H. Mohamad, A. Alhammedi, Y.I. Daradkeh, Handover management of drones in future mobile networks: 6G technologies. *IEEE Access* **9**, 12803–12823 (2021)
21. H. Zhang, L. Dai, Mobility prediction: a survey on state-of-the-art schemes and future applications. *IEEE Access* **7**, 802–822 (2018)
22. M. Muhammad, G.A. Safdar, Survey on existing authentication issues for cellular-assisted V2X communication. *Veh. Commun.* **12**, 50–65 (2018)
23. S. Behrad, E. Bertin, N. Crespi, Securing authentication for mobile networks, a survey on 4g issues and 5g answers. In: 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp. 1–8 (2018). IEEE
24. S. Behrad, E. Bertin, N. Crespi, A survey on authentication and access control for mobile networks: from 4G to 5G. *Ann. Telecommun.* **74**(9), 593–603 (2019)
25. J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, L. Xiong, A survey on security aspects for 3gpp 5G networks. *IEEE Commun. Surveys Tutorials* **22**(1), 170–195 (2019)

26. D. Zhao, Z. Yan, M. Wang, P. Zhang, B. Song, Is 5g handover secure and private? A survey. *IEEE Internet Things J.* (2021)
27. 3GPP: Evolved universal terrestrial radio access (e-utra) and evolved universal terrestrial radio access network (e-utran); overall description; stage 2. Technical Specification (TS) 36.300, 3rd Generation Partnership Project (3GPP) (January 2020). Version 16.0.0
28. 3GPP: Nr; nr and ng-ran overall description; stage-2. Technical specification (TS) 38.300, 3rd Generation Partnership Project (3GPP) (January 2021). Version 16.4.0
29. 3GPP: Procedures for the 5g system (5gs). Technical Specification (TS) 23.502, 3rd Generation Partnership Project (3GPP) (March 2019). Version 16.0.0
30. 3GPP: Nr; physical layer measurements. Technical specification (TS) 38.215, 3rd Generation Partnership Project (3GPP) (July 2020). Version 15.7.0
31. 3GPP: Release 15 description; summary of rel-15 work items. Technical report (TR) 21.915, 3rd Generation Partnership Project (3GPP) (October 2019). Version 15.0.0
32. H.-C. Jang, K.-S. Chang, A study on handover mechanism in 5g non-standalone network. In: 2020 International Computer Symposium (ICS), pp. 7–12 (2020). IEEE
33. 3GPP: Security architecture and procedures for 5g system. Technical specification (TS) 33.501, 3rd Generation Partnership Project (3GPP) (July 2021). Version 16.7.1
34. K. Alexandris, N. Nikaein, R. Knopp, C. Bonnet, Analyzing x2 handover in lte/lte-a. In: 2016 14th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp. 1–7 (2016). IEEE
35. 3GPP: Nr; physical channels and modulation. Technical specification (TS) 38.211, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
36. M. Polese, M. Giordani, M. Mezzavilla, S. Rangan, M. Zorzi, Improved handover through dual connectivity in 5G mmwave mobile networks. *IEEE J. Sel. Areas Commun.* **35**(9), 2069–2084 (2017)
37. 3GPP: Nr; radio resource control (rrc); protocol specification. Technical Report 38.331, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
38. 3GPP: Evolved universal terrestrial radio access (e-utra); physical layer; measurements. Technical Specification (TS) 36.214, 3rd Generation Partnership Project (3GPP) (January 2020). Version 16.0.0
39. 3GPP: Nr; physical layer procedures for data. Technical Specification (TS) 38.214, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
40. X. Gelabert, G. Zhou, P. Legg, Mobility performance and suitability of macro cell power-off in lte dense small cell hetnets. In: 2013 IEEE 18th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 99–103 (2013). IEEE
41. 3GPP: Telecommunication management; key performance indicators (kpi) for the evolved packet core (epc); definitions. Technical Specification (TS) 32.455, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
42. M. Tayyab, G.P. Koudouridis, X. Gelabert, A simulation study on lte handover and the impact of cell size. In: International Conference on Broadband Communications, Networks and Systems, pp. 398–408 (2018). Springer
43. A. Ulvan, R. Bestak, M. Ulvan, The study of handover procedure in lte-based femtocell network. In: WMNC2010, pp. 1–6 (2010). IEEE
44. 3GPP: Ng-ran; xn application protocol (xnapp). Technical Specification (TS) 38.423, 3rd Generation Partnership Project (3GPP) (January 2020). Version 16.0.0
45. C. Lee, H. Cho, S. Song, J.-M. Chung, Prediction-based conditional handover for 5G mm-wave networks: a deep-learning approach. *IEEE Veh. Technol. Mag.* **15**(1), 54–62 (2020). <https://doi.org/10.1109/MVT.2019.2959065>
46. A. Prado, H. Vijayaraghavan, W. Kellerer, Echo: Enhanced conditional handover boosted by trajectory prediction. In: 2021 IEEE Global Communications Conference (GLOBECOM), pp. 01–06 (2021). IEEE
47. J. Stanczak, U. Karabulut, A. Awada, Conditional handover in 5g-principles, future use cases and fr2 performance. In: 2022 International Wireless Communications and Mobile Computing (IWCMC), pp. 660–665 (2022). IEEE
48. S.B. Iqbal, A. Awada, U. Karabulut, I. Viering, P. Schulz, G.P. Fettweis, On the modeling and analysis of fast conditional handover for 5g-advanced. In: 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 595–601 (2022). IEEE
49. S.B. Iqbal, S. Nadaf, A. Awada, U. Karabulut, P. Schulz, G.P. Fettweis, On the analysis and optimization of fast conditional handover with hand blockage for mobility. *arXiv preprint arXiv:2211.00573* (2022)
50. C.N. Barati, S.A. Hosseini, M. Mezzavilla, P. Amiri-Eliasi, S. Rangan, T. Korakis, S.S. Panwar, M. Zorzi, Directional initial access for millimeter wave cellular systems. In: 2015 49th Asilomar Conference on Signals, Systems and Computers, pp. 307–311 (2015). IEEE
51. C.N. Barati, S.A. Hosseini, S. Rangan, P. Liu, T. Korakis, S.S. Panwar, T.S. Rappaport, Directional cell discovery in millimeter wave cellular networks. *IEEE Trans. Wireless Commun.* **14**(12), 6664–6678 (2015)
52. H. Xu, X. Wang, W. Liu, W. Shao, An uplink based mobility management scheme for 5g wireless network. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6 (2019). IEEE
53. M. Tayyab, G.P. Koudouridis, X. Gelabert, R. Jäntti, Uplink reference signals for power-efficient handover in cellular networks with mobile relays. *IEEE Access* **9**, 24446–24461 (2021)
54. C. Wu, X. Cai, J. Sheng, Z. Tang, B. Ai, Y. Wang, Parameter adaptation and situation awareness of lte-r handover for high-speed railway communication. *IEEE Transactions on Intelligent Transportation Systems*, 1–15 (2020). <https://doi.org/10.1109/ITITS.2020.3026195>
55. W.-Y. Lee, I.F. Akyildiz, Spectrum-aware mobility management in cognitive radio cellular networks. *IEEE Trans. Mob. Comput.* **11**(4), 529–542 (2012). <https://doi.org/10.1109/TMC.2011.69>
56. N.P. Kuruvatti, W. Zhou, H.D. Schotten, Mobility prediction of diurnal users for enabling context aware resource allocation. In: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), pp. 1–5 (2016). <https://doi.org/10.1109/VTCSpring.2016.7504348>
57. L. Qin, D. Zhao, Channel time allocations and handoff management for fair throughput in wireless mesh networks. *IEEE Trans. Veh. Technol.* **64**(1), 315–326 (2015). <https://doi.org/10.1109/TVT.2014.2320596>

58. S. Jangsher, V.O.K. Li, Resource allocation in cellular networks employing mobile femtocells with deterministic mobility. In: 2013 IEEE Wireless Communications and Networking Conference (WCNC), pp. 819–824 (2013). <https://doi.org/10.1109/WCNC.2013.6554669>
59. X. Huang, S. Tang, Q. Zheng, D. Zhang, Q. Chen, Dynamic femtocell GNB on/off strategies and seamless dual connectivity in 5G heterogeneous cellular networks. *IEEE Access* **6**, 21359–21368 (2018). <https://doi.org/10.1109/ACCESS.2018.2796126>
60. H. Gupta, M. Sharma, A. Franklin, B.R. Tamma, Apt-ran: a flexible split-based 5G ran to minimize energy consumption and handovers. *IEEE Tran. Netw. Serv. Manage.* **17**(1), 473–487 (2020). <https://doi.org/10.1109/TNSM.2019.2948457>
61. L. Yan, X. Fang, Y. Fang, A novel network architecture for C/U-plane staggered handover in 5G decoupled heterogeneous railway wireless systems. *IEEE Trans. Intell. Transp. Syst.* **18**(12), 3350–3362 (2017)
62. J. Zhao, Y. Liu, Y. Gong, C. Wang, L. Fan, A dual-link soft handover scheme for C/U plane split network in high-speed railway. *IEEE Access* **6**, 12473–12482 (2018)
63. T. Bilen, B. Canberk, K.R. Chowdhury, Handover management in software-defined ultra-dense 5G networks. *IEEE Network* **31**(4), 49–55 (2017)
64. B. Yang, X. Yang, X. Ge, Q. Li, Coverage and handover analysis of ultra-dense millimeter-wave networks with control and user plane separation architecture. *IEEE Access* **6**, 54739–54750 (2018)
65. Z. Zhang, Z. Junhui, S. Ni, Y. Gong, A seamless handover scheme with assisted ENB for 5G C/U plane split heterogeneous network. *IEEE Access* **7**, 164256–164264 (2019)
66. M. Pozza, A. Rao, A. Bujari, H. Flinck, C.E. Palazzi, S. Tarkoma, A refactoring approach for optimizing mobile networks. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–6 (2017) IEEE
67. A. Patel, M. Vutukuru, D. Krishnaswamy, Mobility-aware vnf placement in the lte epc. In: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 1–7 (2017). IEEE
68. D. Battulga, J. Ankhzaya, B. Ankhbayar, U. Ganbayar, S. Sodbileg, Handover management for distributed mobility management in sdn-based mobile networks. In: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1–6 (2017). IEEE
69. J. Kim, D.G. Duguma, P.V. Astillo, H.-Y. Park, B. Kim, I. You, V. Sharma, A formally verified security scheme for inter-NB-DU handover in 5G vehicle-to-everything. *IEEE Access* **9**, 119100–119117 (2021). <https://doi.org/10.1109/ACCESS.2021.3107308>
70. A. Jain, E. Lopez-Aguilera, I. Demirkol, Enhanced handover signaling through integrated mme-sdn controller solution. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), pp. 1–7 (2018). IEEE
71. A. Jain, E. Lopez-Aguilera, I. Demirkol, Evolutionary 4G/5G network architecture assisted efficient handover signaling. *IEEE access* **7**, 256–283 (2018)
72. S.A. Hoseinitabatabei, A. Mohamed, M. Hassanpour, R. Tafazolli, The power of mobility prediction in reducing idle-state signaling in cellular systems: a revisit to 4G mobility management. *IEEE Trans. Wireless Commun.* **19**(5), 3346–3360 (2020). <https://doi.org/10.1109/TWC.2020.2972536>
73. L. Sun, J. Hou, T. Shu, Spatial and temporal contextual multi-armed bandit handovers in ultra-dense mmwave cellular networks. *IEEE Trans. Mob. Comput.* **20**(12), 3423–3438 (2021). <https://doi.org/10.1109/TMC.2020.3000189>
74. H. Martikainen, I. Viering, A. Lobinger, B. Wegmann, Mobility and reliability in lte-5g dual connectivity scenarios. In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), pp. 1–7 (2017). IEEE
75. M. Giordani, M. Mezzavilla, S. Rangan, M. Zorzi, An efficient uplink multi-connectivity scheme for 5G millimeter-wave control plane applications. *IEEE Trans. Wireless Commun.* **17**(10), 6806–6821 (2018)
76. T. Mumtaz, S. Muhammad, M.I. Aslam, N. Mohammad, Dual connectivity-based mobility management and data split mechanism in 4G/5G cellular networks. *IEEE Access* **8**, 86495–86509 (2020). <https://doi.org/10.1109/ACCESS.2020.2992805>
77. R.A. Paropkari, A.A. Gebremichail, C. Beard, Fractional packet duplication and fade duration outage probability analysis for handover enhancement in 5g cellular networks. In: 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 298–302 (2019). IEEE
78. M.F. Özkoç, A. Koutsafitis, R. Kumar, P. Liu, S.S. Panwar, The impact of multi-connectivity and handover constraints on millimeter wave and terahertz cellular networks. *IEEE J. Select. Areas Commun.* **39**(6), 1833–1853 (2021). <https://doi.org/10.1109/JSAC.2021.3071852>
79. K. Qi, T. Liu, C. Yang, S. Suo, Y. Huang, Dual connectivity-aided proactive handover and resource reservation for mobile users. *IEEE Access* **9**, 36100–36113 (2021)
80. K. Manolakis, W. Xu, Sidelink-assisted handover for cellular network, 1–5 (2017). IEEE
81. A. Abdelreheem, O.A. Omer, H. Esmail, U.S. Mohamed, Deep learning-based relay selection in d2d millimeter wave communications. In: 2019 International Conference on Computer and Information Sciences (ICCIS), pp. 1–5 (2019). IEEE
82. Y.-H. Chang, H.-H. Liu, H.-Y. Wei, Group-based sidelink communication for seamless vehicular handover. *IEEE Access* **7**, 56431–56442 (2019)
83. A. Morattab, Z. Dziong, K. Sohraby, Mode selection map-based vertical handover in d2d enabled 5G networks. *IET Commun.* **13**(14), 2173–2185 (2019)
84. X. Yuan, H. Tian, B. Fan, Mobility-aware joint resource allocation and power allocation for d2d communication. In: 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2019). <https://doi.org/10.1109/WCNC.2019.8885989>
85. S. Singh, D. Kedia, N. Rastogi, T. Velmurugan, P. Prakasam, P2p mobility management for seamless handover using d2d communication in b5g wireless technology. *Peer-to-Peer Networking and Applications*, Springer (2021). <https://doi.org/10.1007/s12083-021-01123-4>
86. M. Sadik, N. Akkari, G. Aldabbagh, SDN-based handover scheme for multi-tier LTE/Femto and D2D networks. *Comput. Netw.* **142**, 142–153 (2018). <https://doi.org/10.1016/j.comnet.2018.06.004>

87. K. Ouali, M. Kassar, T.M. Trang Nguyen, K. Sethom, B. Kervella, An efficient d2d handover management scheme for sdn-based 5g networks. In: 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), pp. 1–6 (2020). <https://doi.org/10.1109/CCNC46108.2020.9045534>
88. Z. HajiAkhondi-Meybodi, J. Abouei, M. Jassemuddin, A. Mohammadi, Mobility-aware femtocaching algorithm in d2d networks based on handover. *IEEE Trans. Veh. Technol.* **69**(9), 10188–10201 (2020). <https://doi.org/10.1109/TVT.2020.3003850>
89. L.-H. Shen, K.-T. Feng, Mobility-aware subband and beam resource allocation schemes for millimeter wave wireless networks. *IEEE Trans. Veh. Technol.* **69**(10), 11893–11908 (2020). <https://doi.org/10.1109/TVT.2020.3006320>
90. M.F. Özkoç, A. Koutsaftis, R. Kumar, P. Liu, S.S. Panwar, The impact of multi-connectivity and handover constraints on millimeter wave and terahertz cellular networks. *IEEE J. Sel. Areas Commun.* **39**(6), 1833–1853 (2021)
91. O. Semiari, W. Saad, M. Bennis, B. Maham, Caching meets millimeter wave communications for enhanced mobility management in 5G networks. *IEEE Trans. Wireless Commun.* **17**(2), 779–793 (2018). <https://doi.org/10.1109/TWC.2017.2771419>
92. L. Jiao, P. Wang, A. Alipour-Fanid, H. Zeng, K. Zeng, Enabling efficient blockage-aware handover in ris-assisted mmwave cellular networks. *IEEE Transactions on Wireless Communications*, 1–1 (2021). <https://doi.org/10.1109/TWC.2021.3110522>
93. M. Chiputa, M. Zhang, G.M.N. Ali, P.H.J. Chong, H. Sabit, A. Kumar, H. Li, Enhancing handover for 5g mmwave mobile networks using jump Markov linear system and deep reinforcement learning. *Sensors* **22**(3), 746 (2022)
94. A. Bhattacharyya, B. Sardar, D. Saha, Effect of mode-switching on tcp short flows during d2d communication in lte-a networks. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6 (2017). IEEE
95. P.J. Mateo, C. Fiandrino, J. Widmer, Analysis of tcp performance in 5g mm-wave mobile networks. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–7 (2019). IEEE
96. D. SreeArthi, S. Malini, M.J.A. Jude, V. Diniesh, Micro level analysis of TCP congestion control algorithm in multi-hop wireless networks. In: 2017 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5 (2017). IEEE
97. K.G. Tsiknas, K.E. Zoiros, T.D. Lagkas, Performance analysis of high-speed TCP protocols in LTE X2 handover under realistic operational conditions. *Telecommun. Syst.* **77**, 655–669 (2021)
98. M. Zhang, M. Polese, M. Mezzavilla, J. Zhu, S. Rangan, S. Panwar, M. Zorzi, Will TCP work in mmwave 5G cellular networks? *IEEE Commun. Mag.* **57**(1), 65–71 (2019)
99. C. Paasch, S. Barré, G. Detal, et al.: Multipath TCP in the Linux kernel (2013)
100. D. Zhu, C. Xu, J. Qin, Z. Zhou, J. Guan, Mobility-aware multimedia data transfer using multipath tcp in vehicular network. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1041–1046 (2017). IEEE
101. M. Karimzadeh, L. Valtulina, H. van den Berg, A. Pras, P.G. Ortiz, R. Sadre, Multipath tcp to support user's mobility in future lte network. In: 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC), pp. 1–8 (2017). IEEE
102. Q. De Coninck, O. Bonaventure, Tuning multipath tcp for interactive applications on smartphones. In: 2018 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 1–9 (2018). IEEE
103. A. Abdrabou, M. Prakash, A.S. AlShehi, S.-E. Ahmed, M. Darwish, An experimental study on energy consumption of wireless multipath TCP connections. In: 2019 Wireless Telecommunications Symposium (WTS), pp. 1–7 (2019). IEEE
104. D. Perdana, S.M. Paranaditha, D. Sulistyowati, J.J.P.C. Rodrigues, Evaluation of hmipv6 algorithm in 5g mmwave single and dual connectivity handover network. *IEEE Syst. J.* 1–7 (2021). <https://doi.org/10.1109/JSYST.2021.3087516>
105. H. Tong, T. Wang, Y. Zhu, X. Liu, S. Wang, C. Yin, Mobility-aware seamless handover with MPTCP in software-defined hetnets. *IEEE Trans. Netw. Serv. Manage.* **18**(1), 498–510 (2021)
106. Z. Pan, M. Saito, J. Liu, S. Shimamoto, p -persistent energy-aware handover decisions employing rf fingerprint for adaptive-sized heterogeneous cellular networks. *IEEE Access* **7**, 52929–52944 (2019)
107. H. He, X. Li, Z. Feng, J. Hao, X. Wang, H. Zhang, An adaptive handover trigger strategy for 5g c/u plane split heterogeneous network. In: 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 476–480 (2017). IEEE
108. J. Kim, P.V. Astillo, I. You, DMM-SEP: Secure and efficient protocol for distributed mobility management based on 5G networks. *IEEE Access* **8**, 76028–76042 (2020). <https://doi.org/10.1109/ACCESS.2020.2985448>
109. J. Lee, Y. Yoo, Handover cell selection using user mobility information in a 5G SDN-based network. In: 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 697–702 (2017). IEEE
110. J. Rizkallah, N. Akkari, SDN-based vertical handover decision scheme for 5G networks. In: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), pp. 1–6 (2018). IEEE
111. P. Zhao, X. Yang, W. Yu, J. Lin, D. Meng, Context-aware multi-criteria handover with fuzzy inference in software defined 5G hetnets. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018). IEEE
112. J. Cao, M. Ma, Y. Fu, H. Li, Y. Zhang, Cppha: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G hetnets. *IEEE Transactions on Dependable and Secure Computing* (2019)
113. F.B. Mismar, B.L. Evans, Partially blind handovers for mmwave new radio aided by sub-6 ghz lte signaling. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–5 (2018). IEEE
114. D. Moltchanov, A. Ometov, Y. Koucheryavy, Analytical characterization of the blockage process in 3gpp new radio systems with trilateral mobility and multi-connectivity. *Comput. Commun.* **146**, 110–120 (2019). <https://doi.org/10.1016/j.comcom.2019.07.010>
115. H. Zhang, W. Huang, Y. Liu, Handover probability analysis of anchor-based multi-connectivity in 5G user-centric network. *IEEE Wireless Commun. Lett.* **8**(2), 396–399 (2018)
116. S. Mondal, S. Al-Rubaye, A. Tsourdos, Handover prediction for aircraft dual connectivity using model predictive control. *IEEE Access* **9**, 44463–44475 (2021). <https://doi.org/10.1109/ACCESS.2021.3066554>

117. F. Zhao, H. Tian, G. Nie, H. Wu, Received signal strength prediction based multi-connectivity handover scheme for ultra-dense networks. In: 2018 24th Asia-Pacific Conference on Communications (APCC), pp. 233–238 (2018). IEEE
118. K. Ouali, M. Kassar, T.M.T. Nguyen, K. Sethom, B. Kervella, Modeling d2d handover management in 5G cellular networks. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 196–201 (2017). IEEE
119. S. Zang, W. Bao, P.L. Yeoh, B. Vucetic, Y. Li, Managing vertical handovers in millimeter wave heterogeneous networks. *IEEE Trans. Commun.* **67**(2), 1629–1644 (2018)
120. F. Du, G. Chen, L. Qiu, The analysis of mobility performance in mmwave-μ wave heterogeneous networks. In: 2019 IEEE/CIC International Conference on Communications in China (ICCC), pp. 908–913 (2019). IEEE
121. S.S. Kalamkar, F. Baccelli, F.M. Abinader, A.S. Marcano Fani, L.G. Uzeda Garcia, Beam management in 5G: a stochastic geometry analysis. *IEEE Transactions on Wireless Communications*, 1–1 (2021). <https://doi.org/10.1109/TWC.2021.3110785>
122. I.K. Jain, R. Kumar, S.S. Panwar, The impact of mobile blockers on millimeter wave cellular systems. *IEEE J. Sel. Areas Commun.* **37**(4), 854–868 (2019)
123. Y.-J. Chen, T. Hsu, L.-C. Wang, Improving handover performance in 5g mm-wave hetnets. In: GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–6 (2017). IEEE
124. M. Giordani, M. Zorzi, Improved user tracking in 5g millimeter wave mobile networks via refinement operations. In: 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), pp. 1–8 (2017). IEEE
125. J. Bao, T. Shu, H. Li, Handover prediction based on geometry method in mmwave communications-a sensing approach. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6 (2018). IEEE
126. M. Huang, X. Zhang, Big data analysis on beam spectrum for handover optimization in massive-mimo cellular systems. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2018). IEEE
127. G. Noh, J. Kim, S. Choi, N. Lee, H. Chung, I. Kim, Feasibility validation of a 5G-enabled mmwave vehicular communication system on a highway. *IEEE Access* **9**, 36535–36546 (2021). <https://doi.org/10.1109/ACCESS.2021.3062907>
128. A. Papoulis, S. Pilla, *Probability, Random Variables, and Stochastic Processes* (McGraw-Hill, New York, 1965), p.583
129. R.A. Paropkari, C. Beard, A. Van De Liefvoort, Handover performance prioritization for public safety and emergency networks. In: 2017 IEEE 38th Sarnoff Symposium, pp. 1–6 (2017). IEEE
130. E.M.O. Fafolahan, S. Pierre, A seamless mobility management protocol in 5g locator identifier split dense small cells. *IEEE Transactions on Mobile Computing* (2019)
131. A.M. Andrew, Reinforcement learning: An introduction by richard s. sutton and andrew g. barto, adaptive computation and machine learning series, mit press (bradford book), cambridge, mass., 1998, xviii+ 322 pp, isbn 0-262-19398-1,(hardback,£ 31.95). *Robotica* **17**(2), 229–235 (1999)
132. M. Erel-Özçevik, B. Canberk, Road to 5G reduced-latency: a software defined handover model for EMBB services. *IEEE Trans. Veh. Technol.* **68**(8), 8133–8144 (2019)
133. A. Hadachi, O. Batrashev, A. Lind, G. Singer, E. Vainikko, Cell phone subscribers mobility prediction using enhanced markov chain algorithm. In: 2014 IEEE Intelligent Vehicles Symposium Proceedings, pp. 1049–1054 (2014). IEEE
134. M. Franzese, A. Iuliano, Hidden Markov models (2019)
135. Q. Lv, Y. Qiao, N. Ansari, J. Liu, J. Yang, Big data driven hidden Markov model based individual mobility prediction at points of interest. *IEEE Trans. Veh. Technol.* **66**(6), 5204–5216 (2016)
136. K.-L. Yap, Y.-W. Chong, Optimized access point selection with mobility prediction using hidden markov model for wireless network. In: 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 38–42 (2017). IEEE
137. K. Vasudeva, M. Simsek, D. López-Pérez, I. Güvenç, Analysis of handover failures in heterogeneous networks with fading. *IEEE Trans. Veh. Technol.* **66**(7), 6060–6074 (2016)
138. C. Suarez-Rodriguez, Y. He, E. Dutkiewicz, Theoretical analysis of rem-based handover algorithm for heterogeneous networks. *IEEE Access* **7**, 96719–96731 (2019)
139. R. Arshad, H. ElSawy, S. Sorour, T.Y. Al-Naffouri, M.-S. Alouini, Velocity-aware handover management in two-tier cellular networks. *IEEE Trans. Wireless Commun.* **16**(3), 1851–1867 (2017)
140. M.-T. Nguyen, S. Kwon, Geometry-based analysis of optimal handover parameters for self-organizing networks. *IEEE Trans. Wireless Commun.* **19**(4), 2670–2683 (2020). <https://doi.org/10.1109/TWC.2020.2967668>
141. I. Shayea, M. Ergen, A. Azizan, M. Ismail, Y.I. Daradkeh, Individualistic dynamic handover parameter self-optimization algorithm for 5G networks based on automatic weight function. *IEEE Access* **8**, 214392–214412 (2020). <https://doi.org/10.1109/ACCESS.2020.3037048>
142. R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, J.C. Zhang, Artificial intelligence-enabled cellular networks: a critical path to beyond-5G and 6G. *IEEE Wirel. Commun.* **27**(2), 212–217 (2020)
143. S. Zhao, Q. Wang, A contextual awareness-learning approach to multi-objective mobility management. In: 2017 12th International Conference on Computer Science and Education (ICCSE), pp. 277–282 (2017). IEEE
144. T. Zhang, L. Feng, P. Yu, S. Guo, W. Li, X. Qiu, A handover statistics based approach for cell outage detection in self-organized heterogeneous networks. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 628–631 (2017). IEEE
145. A. Alhammedi, M. Roslee, M.Y. Alias, I. Shayea, S. Alraih, Dynamic handover control parameters for LTE-A/5G mobile communications. In: 2018 Advances in Wireless and Optical Communications (RTUWO), pp. 39–44 (2018). IEEE
146. Q. Liu, C.F. Kwong, S. Zhou, T. Ye, L. Li, S.P. Ardakani, Autonomous mobility management for 5G ultra-dense het-nets via reinforcement learning with tile coding function approximation. *IEEE Access* **9**, 97942–97952 (2021). <https://doi.org/10.1109/ACCESS.2021.3095555>
147. C. Wang, J. Yang, H. He, R. Zhou, S. Chen, X. Jiang, Neighbor cell list optimization in handover management using cascading bandits algorithm. *IEEE Access* **8**, 134137–134150 (2020). <https://doi.org/10.1109/ACCESS.2020.3011015>

148. S.-C. Wang, Artificial neural network, in *Interdisciplinary Computing in Java Programming*. (Springer, Cham, 2003), pp.81–100
149. A.B. Zineb, M. Ayadi, S. Tabbane, Qoe-based vertical handover decision management for cognitive networks using ann. In: 2017 Sixth International Conference on Communications and Networking (ComNet), pp. 1–7 (2017). IEEE
150. D. Cheelu, M.R. Babu, P.V. Krishna, A study of vertical handoff decision strategies in heterogeneous wireless networks. *Int. J. Eng. Technol.* **5**(3), 2541–2554 (2013)
151. J. Schmidhuber, Deep learning in neural networks: an overview. *Neural Netw.* **61**, 85–117 (2015)
152. D.S. Wickramasuriya, C.A. Perumalla, K. Davaslioglu, R.D. Gitlin, Base station prediction and proactive mobility management in virtual cells using recurrent neural networks. In: 2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON), pp. 1–6 (2017). IEEE
153. I. Labriji, F. Meneghello, D. Cecchinato, S. Sesia, E. Perraud, E.C. Strinati, M. Rossi, Mobility aware and dynamic migration of MEC services for the internet of vehicles. *IEEE Trans. Netw. Serv. Manage.* **18**(1), 570–584 (2021). <https://doi.org/10.1109/TNSM.2021.3052808>
154. Y. LeCun, Y. Bengio, G. Hinton, Deep learning. *Nature* **521**(7553), 436–444 (2015)
155. J. Wang, J. Tang, Z. Xu, Y. Wang, G. Xue, X. Zhang, D. Yang, Spatiotemporal modeling and prediction in cellular networks: A big data enabled deep learning approach. In: IEEE INFOCOM 2017-IEEE Conference on Computer Communications, pp. 1–9 (2017). IEEE
156. S. Khunteta, A.K.R. Chavva, Deep learning based link failure mitigation. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 806–811 (2017). IEEE
157. B. Shubyn, T. Maksymyuk, Intelligent handover management in 5G mobile networks based on recurrent neural networks. In: 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 348–351 (2019). IEEE
158. M.Elkourdi, A. Mazin, R.D. Gitlin, Performance analysis for virtual-cell based comp 5g networks using deep recurrent neural nets. In: 2019 Wireless Telecommunications Symposium (WTS), pp. 1–6 (2019). IEEE
159. Z. Ali, M. Miozzo, L. Giupponi, P. Dini, S. Denic, S. Vassaki, Recurrent neural networks for handover management in next-generation self-organized networks. arXiv preprint [arXiv:2006.06526](https://arxiv.org/abs/2006.06526) (2020)
160. Z. Wang, L. Li, Y. Xu, H. Tian, S. Cui, Handover optimization via asynchronous multi-user deep reinforcement learning. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018). IEEE
161. R. Klus, L. Klus, D. Solomitckii, M. Valkama, J. Talvitie, Deep learning based localization and ho optimization in 5g nr networks. In: 2020 International Conference on Localization and GNSS (ICL-GNSS), pp. 1–6 (2020). IEEE
162. L.A. Zadeh, Fuzzy logic. *Computer* **21**(4), 83–93 (1988)
163. P. Hájek, *Metamathematics of Fuzzy Logic*, vol. 4 (Springer, Cham, 2013)
164. E. Cardoso, K. Silva, R. Francés, Intelligent handover procedure for heterogeneous lte networks using fuzzy logic. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 2163–2168 (2017). IEEE
165. M. Liu, Y. Huan, Q. Zhang, W. Lu, W. Li, T.A. Gulliver, Multiple attribute handover in 5g hetnets based on an intuitionistic trapezoidal fuzzy algorithm. In: 2018 IEEE/CIC International Conference on Communications in China (ICCC Workshops), pp. 261–266 (2018). IEEE
166. A. Alhammadi, M. Roslee, M.Y. Alias, I. Shayea, S. Alriah, A.B. Abas, Advanced handover self-optimization approach for 4g/5g hetnets using weighted fuzzy logic control. In: 2019 15th International Conference on Telecommunications (ConTEL), pp. 1–6 (2019). IEEE
167. O. Semenova, A. Semenov, O. Voitsekhovska, Neuro-fuzzy controller for handover operation in 5g heterogeneous networks. In: 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 382–386 (2019). IEEE
168. F. Gong, Z. Sun, X. Xu, Z. Sun, X. Tang, Cross-tier handover decision optimization with stochastic based analytical results for 5g heterogeneous ultra-dense networks. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6 (2018). IEEE
169. R.T. Rodoshi, T. Kim, W. Choi, Fuzzy logic and accelerated reinforcement learning-based user association for dense c-RANs. *IEEE Access* **9**, 117910–117924 (2021). <https://doi.org/10.1109/ACCESS.2021.3107325>
170. E. Rasmusen, *Games and Information: An Introduction to Game Theory* (Blackwell, Oxford, 1989)
171. S.B. Peddi, S.R. Patil, Game theory based vertical handoff decision model for media independent handover in heterogeneous wireless networks. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 719–724 (2016). IEEE
172. S. Goudarzi, M.H. Anisi, D. Ciuonzo, S.A. Soleymani, A. Pescape, Employing unmanned aerial vehicles for improving handoff using cooperative game theory. *IEEE Transactions on Aerospace and Electronic Systems* (2020)
173. V. Marx, The big challenges of big data. *Nature* **498**(7453), 255–260 (2013)
174. M. Dalla Cia, F. Mason, D. Peron, F. Chiariotti, M. Polese, T. Mahmoodi, M. Zorzi, A. Zanella, Mobility-aware handover strategies in smart cities. In: 2017 International Symposium on Wireless Communication Systems (ISWCS), pp. 438–443 (2017). IEEE
175. Y. Sueda, A. Koike, On dynamics of handover trajectories in LTE cellular network system. In: 2018 7th International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 835–840 (2018). IEEE
176. M. Alhabo, L. Zhang, N. Nawaz, Gra-based handover for dense small cells heterogeneous networks. *IET Commun.* **13**(13), 1928–1935 (2019)
177. I.A. Alablani, M.A. Arafah, An adaptive cell selection scheme for 5G heterogeneous ultra-dense networks. *IEEE Access* **9**, 64224–64240 (2021). <https://doi.org/10.1109/ACCESS.2021.3075324>
178. H.-S. Park, Y. Lee, T.-J. Kim, B.-C. Kim, J.-Y. Lee, Faster recovery from radio link failure during handover. *IEEE Commun. Lett.* **24**(8), 1835–1839 (2020). <https://doi.org/10.1109/LCOMM.2020.2994989>
179. N. Malm, L. Zhou, E. Menta, K. Ruttik, R. Jäntti, O. Tirkkonen, M. Costa, K. Leppänen, User localization enabled ultra-dense network testbed. In: 2018 IEEE 5G World Forum (5GWF), pp. 405–409 (2018). IEEE

180. A. Parichehreh, R. Moosavi, P. Ramachandra, S. Alfredsson, A. Brunstrom, LTE as a road toward 5G: Qos analysis in mobility scenario using the monroe platform. In: 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–7 (2019). IEEE
181. S. Ahmadi, *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards* (Elsevier Science, New York, 2019). <https://books.google.com/books?id=N0hgtAEACAAJ>
182. Y. Xiao, Y. Pan, *Security in Distributed and Networking Systems* (World Scientific, Singapore, 2007). <https://doi.org/10.1142/6513>
183. 3GPP: Security related network functions. Technical Specification (TS) 43.020, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
184. 3GPP: 3G security; security architecture. Technical Specification (TS) 33.102, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
185. 3GPP: 3gpp system architecture evolution (SAE); security aspects of non-3gpp accesses. Technical Specification (TS) 33.402, 3rd Generation Partnership Project (3GPP) (2020). Version 16.0.0
186. R. Ma, J. Cao, D. Feng, H. Li, S. He, FTGPHA: Fixed-trajectory group pre-handover authentication mechanism for mobile relays in 5G high-speed rail networks. *IEEE Trans. Veh. Technol.* **69**(2), 2126–2140 (2020). <https://doi.org/10.1109/TVT.2019.2960313>
187. J. Cao, M. Ma, H. Li, Y. Fu, X. Liu, EGHR: Efficient group-based handover authentication protocols for MMTC in 5G wireless networks. *J. Netw. Comput. Appl.* **102**, 1–16 (2018). <https://doi.org/10.1016/j.jnca.2017.11.009>
188. A. Ozhelvaci, M. Ma, Secure and efficient vertical handover authentication for 5g hetnets. In: 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), pp. 27–32 (2018). IEEE
189. W. Haddar, S.B. Ameer, F. Zarai, Securing fast pmipv6 protocol in case of vertical handover in 5g network. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 1037–1042 (2019). IEEE
190. G. Chopra, S. Jain, R.K. Jha, Possible security attack modeling in ultradense networks using high-speed handover management. *IEEE Trans. Veh. Technol.* **67**(3), 2178–2192 (2017)
191. G. Chopra, R.K. Jha, S. Jain, Security issues in ultra dense network for 5g scenario. In: 2018 10th International Conference on Communication Systems & Networks (COMSNETS), pp. 510–512 (2018). IEEE
192. S. Taha, M. Alhassany, X. Shen, Lightweight handover authentication scheme for 5g-based v2x communications. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2018). <https://doi.org/10.1109/GLOCOM.2018.8648020>
193. S. Sodagari, T.C. Clancy, On singularity attacks in mimo channels. *Trans. Emerg. Telecommun. Technol.* **26**(3), 482–490 (2015)
194. V. Sharma, J. Guan, J. Kim, S. Kwon, I. You, F. Palmieri, M. Collotta, MIH-SPFP: MIH-based secure cross-layer handover protocol for fast proxy mobile IPv6-IoT networks. *J. Netw. Comput. Appl.* **125**, 67–81 (2019). <https://doi.org/10.1016/j.jnca.2018.09.002>
195. Y. Zhang, R. Deng, E. Bertino, D. Zheng, Robust and universal seamless handover authentication in 5G hetnets. *IEEE Transactions on Dependable and Secure Computing* (2019)
196. C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, J. Lee, Rehand: secure region-based fast handover with user anonymity for small cell networks in mobile communications. *IEEE Trans. Inf. Forensics Secur.* **15**, 927–942 (2020). <https://doi.org/10.1109/TIFS.2019.2931076>
197. X. Yan, M. Ma, A lightweight and secure handover authentication scheme for 5G network using neighbour base stations. *J. Netw. Comput. Appl.* **193**, 103204 (2021). <https://doi.org/10.1016/j.jnca.2021.103204>
198. X. Yan, M. Ma, Nseha: A neighbor-based secure and efficient handover authentication mechanism for 5g networks. In: 2021 9th International Conference on Communications and Broadband Networking, pp. 209–216 (2021)
199. D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, Y. Jeon, Design of secure handover authentication scheme for urban air mobility environments. *IEEE Access* **10**, 42529–42541 (2022)
200. A. Shaik, R. Borgaonkar, S. Park, J.-P. Seifert, New vulnerabilities in 4g and 5g cellular access network protocols: exposing device capabilities. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 221–231 (2019)
201. 3GPP: Study on 5g security enhancements against false base stations (fbs). Technical report (TR) 33.809, 3rd Generation Partnership Project (3GPP) (September 2021). Version 0.16.0
202. S. Park, A. Shaik, R. Borgaonkar, J.-P. Seifert, Anatomy of commercial imsi catchers and detectors. In: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society, pp. 74–86 (2019)
203. D. Strobel, Imsi catcher. *Chair for Communication Security, Ruhr-Universität Bochum* **14** (2007)
204. 3GPP: Evolved universal terrestrial radio access (e-utra); requirements for support of radio resource management. Technical specification (TS) 36.133, 3rd Generation Partnership Project (3GPP) (September 2013). Version 8.23.0
205. S. Gupta, B.L. Parne, N.S. Chaudhari, Security vulnerabilities in handover authentication mechanism of 5g network. In: 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), pp. 369–374 (2018). IEEE
206. A. Shaik, R. Borgaonkar, S. Park, J.-P. Seifert, On the impact of rogue base stations in 4g/lte self organizing networks. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 75–86 (2018)
207. M. Saedi, A. Moore, P. Perry, M. Shojafar, H. Ullah, J. Synnott, R. Brown, I. Herwono, Generation of realistic signal strength measurements for a 5g rogue base station attack scenario. In: 2020 IEEE Conference on Communications and Network Security (CNS), pp. 1–7 (2020). IEEE
208. H. Lee, M. Ma, Blockchain-based mobility management for lte and beyond. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 36–49 (2019). Springer
209. J. Jin, C. Lian, M. Xu, Rogue base station detection using a machine learning approach. In: 2019 28th Wireless and Optical Communications Conference (WOCC), pp. 1–5 (2019). IEEE

210. V.O. Nyangaresi, S.O. Abeka, A.J. Rodrigues, GUTI-based multi-factor authentication protocol for de-synchronization attack prevention in LTE handovers. *Int. J. Cyber-Secur. Digit. Forensics* **9**(1), 1–12 (2020)
211. P.K. Nakarmi, M.A. Ersoy, E.U. Soykan, K. Norrman, Murat: Multi-rat false base station detector. arXiv preprint [arXiv: 2102.08780](https://arxiv.org/abs/2102.08780) (2021)
212. Y. Aydin, G.K. Kurt, E. Ozdemir, H. Yanikomeroglu, Group handover for drone base stations. *IEEE Internet Things J.* **8**(18), 13876–13887 (2021). <https://doi.org/10.1109/JIOT.2021.3068297>
213. A. Rawat, S. Sharma, R. Sushil, Vanet: security attacks and its possible solutions. *J. Inf. Oper. Manag.* **3**(1), 301 (2012)
214. M.J. Alam, M. Ma, Dc and comp authentication in LTE-advanced 5G hetnet. In: *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6 (2017). IEEE
215. G. Singh, D. Shrimankar, Secure & efficient intra-MME handovers via mobile relays within the LTE-A and future 5G high-speed train networks. *Peer-to-Peer Network. Appl.* **13**(3), 762–779 (2020)
216. R.P. Jover, G. De Los Reyes, Cryptographically signing an access point device broadcast message. Google Patents. US Patent 9,860,067 (2018)
217. V.O. Nyangaresi, A.J. Rodrigues, S.O. Abeka, Neuro-fuzzy based handover authentication protocol for ultra dense 5g networks. In: *2020 2nd Global Power, Energy and Communication Conference (GPECOM)*, pp. 339–344 (2020). IEEE
218. Y. Arjoune, S. Faruque, Smart jamming attacks in 5g new radio: A review. In: *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1010–1015 (2020). IEEE
219. W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks. In: *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 46–57 (2005)
220. T. Erpek, Y.E. Sagduyu, Y. Shi, Deep learning for launching and mitigating wireless jamming attacks. *IEEE Trans. Cogn. Commun. Netw.* **5**(1), 2–14 (2018)
221. 3GPP: Evolved universal terrestrial radio access (e-utra); physical channels and modulation. Technical specification (TS) 36.211, 3rd Generation Partnership Project (3GPP) (2009). Version 8.9.0
222. R. Krenz, S. Brahma, Jamming LTE signals. In: *2015 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 72–76 (2015). IEEE
223. M. Lichtman, J.H. Reed, T.C. Clancy, M. Norton, Vulnerability of lte to hostile interference. In: *2013 IEEE Global Conference on Signal and Information Processing*, pp. 285–288 (2013). IEEE
224. M. Lichtman, R.P. Jover, M. Labib, R. Rao, V. Marojevic, J.H. Reed, LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Commun. Mag.* **54**(4), 54–61 (2016)
225. F.M. Aziz, J.S. Shamma, G.L. Stüber, Resilience of lte networks against smart jamming attacks: Wideband model. In: *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1344–1348 (2015). IEEE
226. S. Sodagari, T.C. Clancy, Efficient jamming attacks on mimo channels. In: *2012 IEEE International Conference on Communications (ICC)*, pp. 852–856 (2012). IEEE
227. G. Schreiber, M. Tavares, 5g new radio physical random access preamble design. In: *2018 IEEE 5G World Forum (5GWF)*, pp. 215–220 (2018). IEEE
228. F.M. Aziz, J.S. Shamma, G.L. Stüber, Resilience of lte networks against smart jamming attacks. In: *2014 IEEE Global Communications Conference*, pp. 734–739 (2014). IEEE
229. S. Mavoungou, G. Kaddoum, M. Taha, G. Matar, Survey on threats and attacks on mobile networks. *IEEE Access* **4**, 4543–4572 (2016)
230. F.V. Jensen, T.D. Nielsen, *Bayesian Networks and Decision Graphs*, 2nd edn. (Springer, Cham, 2007)
231. Y. Zhang, J. Hu, J. Dong, Y. Yuan, J. Zhou, J. Shi, Location prediction model based on bayesian network theory. In: *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–6 (2009). <https://doi.org/10.1109/GLOCOM.2009.5425444>
232. F. Soma, C. Adjih, I.E. Korbi, L.A. Saidane, A bayesian model for mobility prediction in wireless sensor networks. In: *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pp. 1–7 (2016). <https://doi.org/10.1109/PEMWN.2016.7842898>
233. Y. Cui, Q. Li, Z. Dong, Structural 3D reconstruction of indoor space for 5G signal simulation with mobile laser scanning point clouds. *Remote Sens.* **11**(19), 2262 (2019)
234. S. Ohta, T. Nishio, R. Kudo, K. Takahashi, H. Nagata, Point cloud-based proactive link quality prediction for millimeter-wave communications. arXiv preprint [arXiv:2301.00752](https://arxiv.org/abs/2301.00752) (2023)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.