IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 14, 2018, accepted November 25, 2018, date of publication December 17, 2018,
date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2887146

A Comprehensive Review of Enhancements and Prospects of Fast Handovers for Mobile IPv6 Protocol

MUHAMMAD MOHTASIM SAJJAD[1], (Member, IEEE), DHAMMIKA JAYALATH[1], (Senior Member, IEEE), AND CARLOS J. BERNARDOS[2]

[1]School of Electrical Engineering and Computer Science, Science and Engineering Faculty, Queensland University of Technology, Brisbane, QLD 4001, Australia
[2]School of Engineering, Universidad Carlos III de Madrid, 30 E-28911 Leganes, Spain

Corresponding author: Muhammad Mohtasim Sajjad (m.sajjad@qut.edu.au)

ABSTRACT The emerging mobility management schemes for the fifth generation (5G) of mobile networks mostly follow the network-based protocol principles, which do not involve the mobile node (MN) in their operation. Such solutions have not been able to meet the ultra-low handover latency requirement in complex mobility scenarios in 5G. These objectives can be potentially achieved through increased involvement of MN in the handover operation, which can now be conveniently effectuated through virtualization technologies. In this regard, the classical host-based Fast Handovers for Mobile IPv6 (FMIPv6) protocol has the potential to offer several benefits due to its distinctive features, such as link-layer assistance for handover preparation, in-advance new care-of address formulation, and buffering services. Several enhancements to the FMIPv6 protocol have also been proposed, which improve its handover performance. Many of these enhancements focus on the baseline FMIPv6 specification, while others aim to enhance its operation by adding support features, such as mobile multicast, vertical handovers, quality of service assurance, as well as security support. Moreover, several enhancements to the access-technology-specific solutions for FMIPv6 have also been proposed. This paper aims to provide a systematic review of FMIPv6 enhancements in order to gain insight into its advantages as well as its shortcomings. Based on the review, this paper also discusses the evolution prospects of FMIPv6 toward 5G. Finally, some of its potential limitations along with possible research directions in the context of 5G are also indicated.

INDEX TERMS 5G, handover optimization, mobile IPv6, mobility management, ultra-low latency, virtualization.

I. INTRODUCTION

The 5G mobile networks impose stringent mobility management challenges owing to the deployment of small cells, high traffic loads, and highly diverse services, applications and use cases. Most of these services, applications and use cases are latency critical and require ultra-low latency as the MN roams across different domains and networks. However, the emerging mobility management schemes, which are predominantly based on network-based protocol principles [1], [2], have been shown to incur very high latencies, among several other shortcomings [3]–[5]. Such discrepancies can potentially be addressed by exploiting the mobility-related intelligence available from the MN side.

In general, the mobility management protocols for 5G are required to evolve from the existing IP-based mobility management mechanisms. This is because the 5G networks are expected to evolve from the existing all-IP networks [6]. The Internet Engineering Task Force (IETF) has standardized the Mobile IPv6 (MIPv6) protocol [7] for handling mobility in the IP-based networks. The IETF has also specified several enhancements to MIPv6 which include Fast Handover for Mobile IPv6 (FMIPv6) [8], Hierarchical Mobile IPv6 (HMIPv6) [9] and Proxy Mobile IPv6 (PMIPv6) [10]. Among these, the FMIPv6 [8], which primarily aims to reduce the handover latency in MIPv6, has attracted a lot of attention. The IETF has further enhanced FMIPv6 by coupling it to PMIPv6 [10] to produce Fast handovers for

NOMENCLATURE

3G/4G/5G	3rd/4th/5th Generation Networks
AAA	Authentication, Authorization and Accounting
ACK	ACKnowledgement (TCP)
AP/AR	Access Point/Access Router
ASCONF	Address Configuration Change Chunk (SCTP)
BBU	Baseband Unit
BU/BAck	Binding Update/Acknowledgement
cAR	*candidate* Access Router
CARD	Candidate Access Router Discovery
CGA	Cryptographically Generated Address
CN	Correspondent Node
CoA/nCoA	Care-of Address/new CoA
CoT/CoTI	Care-of Test/Init Message
CTD	Context Transfer Data
CXTP	Context Transfer Protocol
DAD	Duplicate Address Detection
DiffServ	Differentiated Services
DMM	Distributed Mobility Management
DoS	Denial of Service
FBU/FBAck	Fast Binding Update/Acknowledgement
FMIPv6	Fast Handovers for Mobile IPv6
FNA/UNA	Fast/Unsolicited Neighbour Advertisement
GK	Group Key
HA	Home Agent
HI/HAck	Handover Initiate/Acknowledge
HK/HIK/HMK	Handover (Integrity/Master) Key
HKS	Handover Key Server
HMAC	Hash-based *MAC*
HMIPv6	Hierarchical Mobile IPv6
HoT/HoTI	Home Test/Init Message
HS/RS	Home/Remote Subscription
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security Protocol
IPv6	Internet Protocol version 6
IS	(MIH) Information Server
L2/L3/L4	Layer 2/3/4
LGD	Link Going Down
LMA	Local Mobility Anchor (PMIPv6)
MAC	Media Access Control
MAC	Message Authentication Code
MAP/nMAP	Mobility Anchor Point/new MAP
MIPv6	Mobile IPv6
MIH	Media Independent Handover/Function
MLD	Multicast Listener Discovery protocol
MN/MR	Mobile Node/Router
NAR/PAR	New AR/Previous AR
nCoA/pCoA	new/previous CoA
NFV	Network Functions Virtualization
OWHC	One-way Hash Chain
PIM	Protocol Independent Multicast protocol
PMIPv6	Proxy Mobile IPv6
PoA/nPoA	Point of Attachment/new PoA
PrRtAdv	Proxy Router Advertisement
QoS	Quality of Service
RA	Router Advertisement
RAN	Radio Access Network
RO	Route Optimization
RR	Return Routability
RRH	Remote Radio Header
RSS/RSSI	Received Signal Strength/ RSS Indication
RSVP	Resource Reservation Protocol
RTO	Retransmission Timeout
RtSolPr	Router Solicitation for Proxy Advertisement
RTT	Round Trip Time
s/t-BS	serving/target Base Station
SCTP	Stream Control Transmission Protocol
SDN	Software-Defined Networking
SEND	Secure Neighbour Discovery Protocol
SIP	Session Initiation Protocol
SNR	Signal-to-Noise Ratio
STA	STAtion (IEEE 802.11)
TCP	Transmission Control Protocol
VHO	Vertical Handovers
WiFi	Wireless Fidelty
WiMAX	Wireless Interoperability for Microwave Access
WLAN	Wireless Local Area Network

PMIPv6 (FPMIPv6) [11]. Several studies have shown that both FMIPv6 and FPMIPv6 outperform MIPv6 and its other IETF enhancements and can achieve up to 88.63% reduction in handover latency compared to MIPv6 [12], up to 82.14% compared HMIPv6 [12] and up to 77.94% compared PMIPv6 [13] under different scenarios and topology considerations.[1]

However, the fast handover solutions still suffer performance bottlenecks under certain scenarios such as, for real-time applications and high mobility. As a result, several enhancements in their standard protocol operation have been proposed. Some recent works have provided detailed surveys on MIPv6-based enhancements along with their key functional characteristics [19]–[21]. They also discuss FPMIPv6 and its enhancements. However, no comprehensive review on the baseline FMIPv6 protocol enhancements can be found in the open literature. Thus, this paper surveys the existing literature on the enhancements in the FMIPv6 protocol operation. As we discuss later in this paper, FMIPv6 along with its enhancements, capitalizing on the virtualization technologies can potentially address several key mobility management challenges in 5G mobility environment.

The enhancements in FMIPv6 are broadly organized into five major categories to provide a systematic and comprehensive survey. These categories are based on the key design features of these enhancements and are termed as *fundamental* enhancements, *complementary* enhancements, *supplementary* enhancements, *security-specific* enhancements and *access technology-specific* enhancements. Figure 1 shows the proposed taxonomy of these enhancements. Several subcategories for each type of enhancement are also shown in Figure 1.

The *fundamental* enhancements are primarily aimed at optimizing the handover sub-processes involved in the FMIPv6 protocol operation. By optimizing the individual sub-processes, the *fundamental* enhancements aim at improving the overall handover performance of FMIPv6. The handover sub-processes involved in the standard FMIPv6 operation include movement detection and neighbor discovery, link-layer assistance, nCoA acquisition, duplicate

[1]Interested readers may refer to the studies [12]–[19] for detailed comparisons of FMIPv6 and FPMIPv6 with other MIPv6-based solutions based on handover performance metrics such as handover latency, packet loss, signalling costs, packet delivery costs, tunnelling costs and handover blocking probabilities etc. These evaluations have been done through mathematical models, simulators as well as testbeds.

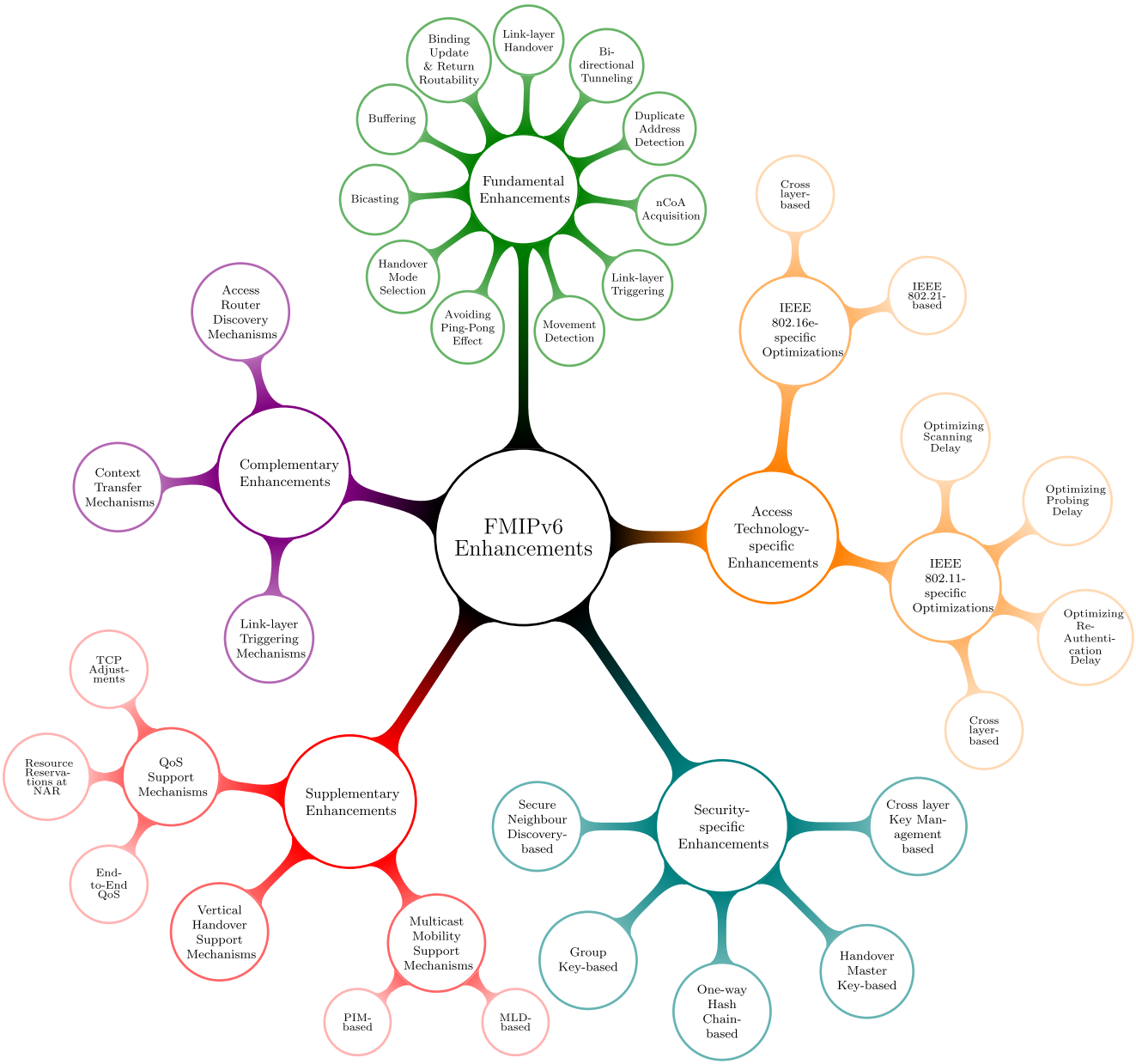

FIGURE 1. Taxonomy for FMIPv6 Protocol Enhancements.

address detection (DAD), bidirectional tunnel establishment, link-layer handover, binding update and return routability, and buffering. Bicasting is another sub-process utilized in some *fundamental* enhancements though it is not part of the baseline FMIPv6 standard. Other important aspects of the FMIPv6 operation which include the execution of suitable mode of operation, either predictive or reactive, as well as addressing the critical ping-pong effect have also been addressed through some *fundamental* enhancements.

The FMIPv6 operation has key dependencies on mechanisms such as link-layer assistance and neighbor discovery. However, its standard specification does not describe the exact operation of these mechanisms due to its limited scope. Thus several enhancements with the primary objective to incorporate these mechanisms in its operation are proposed. Such enhancements are termed as *complementary* enhancements of FMIPv6.

The *supplementary* enhancements, on the other hand, have the main objective to incorporate *additional* functionalities in FMIPv6 operation. The FMIPv6 protocol can thus support advanced mobility features such as multicast mobility, vertical handovers, and QoS assurances. The majority of these enhancements integrate the operation of FMIPv6 with other network protocols. For example, the enhancements to support multicast mobility utilize the Protocol Independent Multicast (PIM) [22], [23] and Multicast Listener Discovery (MLD) [24], [25] protocols. Similarly, for vertical handovers,

IEEE 802.21 [26], and for QoS-assurance, protocols such as Transmission Control Protocol (TCP) [27] interwork with the FMIPv6 protocol operation.

Several enhancements in FMIPv6 also focus on ensuring its secure operation, since the signaling exchange among its different protocol entities is prone to several security threats. These *security-specific* enhancements could potentially be categorized under *complementary* or *supplementary* enhancements, the fact that security is a relatively broader subject, it is discussed under a dedicated category for the sake of convenience.

The FMIPv6 protocol, like other MIPv6 based standards, is access-technology independent – it can operate with any underlying access technology. However, since it incorporates the L2 handover within its protocol operation, the successful execution of FMIPv6 operation relies on timely completion of the L2 handover. The IETF has thus also specified *access technology-specific* protocols for FMIPv6, for prominent access technologies such as IEEE 802.11 [28] and IEEE 802.16e [29]. Both these specifications have also been enhanced further by the research community. The respective enhancements, categorized as *access technology-specific* enhancements, mainly focus on cross-layer approaches, such as integrating the signaling from L2 (IEEE 802.11/IEEE 802.16e) and L3 (FMIPv6).

Challenges in achieving efficient FMIPv6 operation, along with relevant solutions which essentially utilize various approaches are also highlighted in this review. The rest of this paper is organized as follows: Section II describes the FMIPv6 protocol operation and discusses the *fundamental* enhancements. The *complementary* and *supplementary* enhancements are discussed in Section III and Section IV respectively. Section V presents the *security-specific* enhancements, while Section VI discusses the *access-technology specific* enhancements in FMIPv6. Section VII discusses major benefits which can be achieved in FMIPv6 operation through these enhancements. The prospective evolution of FMIPv6 principles towards 5G, along with some limitations and research directions are also discussed in Section VII. Finally, Section VIII summarizes and presents the conclusions of the paper.

II. FMIPv6 SPECIFICATION AND FUNDAMENTAL ENHANCEMENTS

The FMIPv6 protocol is primarily designed to operate in the predictive mode. The reactive mode is executed only in case the predictive mode fails. In each mode, the protocol undergoes certain phases (or sub-processes) to accomplish the handover process. The FMIPv6 performance can be significantly improved if these handover sub-processes are efficiently executed. The protocol entities in FMIPv6 are shown in Figure 2, while the signaling exchange among these entities during predictive and reactive mode is shown in Figures 3a and 3b respectively.

The FMIPv6 operation in predictive mode starts with *movement detection* as the MN detects its mobility towards

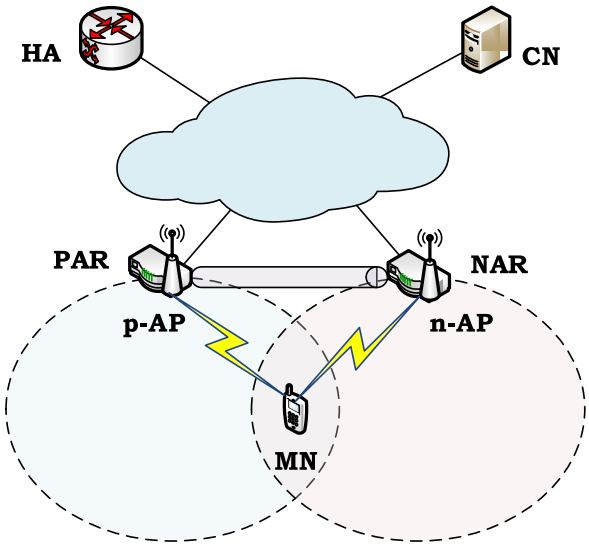

FIGURE 2. FMIPv6 Protocol Entities.

a new subnet. It then sends the Router Solicitation for Proxy Advertisement (RtSolPr) message to PAR, which contains information about the new network detected by the MN (e.g. the Access Point Identifier (AP-ID)). The PAR in response sends the Proxy Router Advertisement (PrRtAdv) message, which contains a network prefix for the new subnet. The MN uses this network prefix for *nCoA formulation* using the stateless address autoconfiguration [30] mechanism while still connected to the PAR. The MN then waits for *link-layer triggering* which indicates that the link quality with current subnet has deteriorated, and handover to a new subnet is required. Based on this trigger, the MN sends the Fast Binding Update (FBU) message to PAR, prior to the L2 link switch. The FBU message indicates the MN's imminent disconnection from PAR's link. The MN also shares the formulated nCoA with PAR through FBU. It then expects the Fast Binding Acknowledgement (FBAck) message in return which would indicate that the nCoA is verified by NAR, and thus can be used to resume communications at the new subnet after the handover.

Concurrently, at the network side, the PAR shares the nCoA with NAR via Handover Initiate (HI) message, which in turn checks its validity. This nCoA validation process is called *Duplicate Address Detection (DAD)*. If found valid, the NAR responds PAR with the Handover Acknowledgement (HAck) message. The HI/HAck exchange also results in the *Bidirectional Tunnel* establishment between PAR and NAR. The PAR, at this stage, sends FBAck message to MN over its current (PAR's) link, as well as over its prospective new link through NAR. The packets of any ongoing sessions of MN received at NAR for the MN which are forwarded from PAR through the tunnel, are buffered until the MN announces its presence at NAR. *Buffering* also earlier takes place at PAR, as it receives the FBU message from MN.

Finally, after the successful link-layer handover, the MN announces its presence at NAR by sending the Unsolicited Neighbor Advertisement (UNA)[2] message. The nCoA of MN has to be communicated to its Home Agent (HA) and the Correspondent Node (CN) through the process of Binding Update, which involves the exchange of Binding Update (BU) and Binding Acknowledgement (BAck) messages. The BU/BAck exchange updates the new location of MN with its Home Agent (HA) and the Correspondent Node (CN). The HA resides in the MN's home network, and normally forwards traffic to MN when it moves out of the home network into any foreign network. The CN, on the other hand, is the node with which the MN currently has an active session. The *Binding Update* process with CN however, first requires an additional *Return Routability (RR)* process to be completed, in order to ensure that the BU is received from an authentic MN. Essentially, the RR procedure establishes the mutual authentication between the MN and CN. The RR process involves the exchange of HoTI/HoT and CoTI/CoT messages between MN and the CN through which the MN receives two *tokens*. These *tokens* are used by MN to formulate a valid BU message to be sent to the CN. The successful completion of the RR procedure means that the MN (at its new location) and the CN are mutually authenticated, and thus direct communication between them is now possible via NAR, without requiring any packet forwarding from PAR or HA.

The reactive mode of FMIPv6 is triggered if the MN fails to send the FBU message at PAR's link as it receives the link-layer trigger. This may, for example, happen due to the fast speed of MN. As a result, the nCoA cannot be shared proactively with PAR and NAR. The HI/HAck exchange or tunnel establishment also cannot take place before the L2 handover. Moreover, both PAR and NAR do not initiate buffering, as neither receives any indications about MN's handover. Consequently, the order of execution for some phases changes in the reactive mode which also impacts the order of its handover signaling. The FMIPv6 signaling in the reactive mode is shown in Figure 3b.

The proposed *fundamental* enhancements in FMIPv6 usually involve modifications in any of these phases (or subprocesses). Below subsections provide discussion on optimizations proposed in each of these subprocesses. Unless explicitly mentioned, the discussion in these subsections is based on the principles of the predictive mode of FMIPv6 operation.

A. MOVEMENT DETECTION

Apart from the traditional movement detection schemes [31], which are generally too costly in MIPv6 environment, certain novel schemes have also been proposed.

[2]The earlier FMIPv6 specifications used the terminology of Fast Neighbor Advertisement (FNA) for this message. Different FMIPv6 enhancements also use either of these terminologies. Thus, in this paper, both UNA and FNA are used interchangeably

The movement detection in FMIPv6 can be considerably optimized if its new location can be predicted. In [20], a *pattern learning module* is used to store the MN's mobility pattern that helps to predict the destination cell where the MN will move to at the next handover event. Similarly, a *Global Positioning System (GPS)* based scheme is introduced in [32] in which every MN, using a GPS receiver, periodically sends its coordinates to a network entity named *Mobility Controller (MC)*. The MC can timely inform the MN about its next AP based on its movement pattern. In [33], the *Radio Frequency identification (RFID)* technology is considered for movement detection, where the *passive tags* are deployed throughout the area under consideration. This process totally eliminates the need for router solicitation/advertisement messages and thus avoids the relative time and bandwidth consumptions.

Recently, a group mobility management scheme, based on *hitch-and-ride* concept is introduced [34], in which a group of MNs with same movement pattern, moving into another network around the same interval, joins a MN which has already initiated the handover signaling with PAR. The group of MNs receives a broadcast-RtSolPr (B-RtSolPr) message from the MN and if suitable, subsequently joins the MN in its handover process. The rest of the handover signaling messages such as PrRtAdv, FBU and FBAck, are also broadcasted by MN and PAR. Such an approach can provide benefits such as session resumption for multiple MNs through a single link-layer scanning mechanism and a single nCoA configuration, while the BU process for all MNs can also be carried out in parallel [35].

B. LINK-LAYER TRIGGERING

The efficiency of FMIPv6 protocol operation depends largely on link-layer (L2) triggering. The timing as well as the criteria upon which such triggers are generated directly impacts the performance of FMIPv6 [36], [37]. If generated too early, it causes higher probability of wrong handover prediction while, if generated too late, the MN may go into the reactive mode, thus incurring high packet losses. An analytical study in [38] shows that the early triggering also increases the signaling costs and would require more buffer space.

For timely L2 trigger generation, an RSS prediction scheme is proposed in [39], which is based on the combination of *Empirical Model Decomposition* and *Support Vector Regression.* Another approach aimed at timely trigger generation is to adjust an appropriate RSS threshold. In [40], an adaptive RSS threshold mechanism is utilized for trigger generation in which the RSS threshold is adaptively adjusted according to the MN's velocity, and the handover takes place as soon as the current RSS approaches the adaptive RSS threshold. Another approach in [41] computes the RSS-threshold considering parameters such as the antenna gain and cell radius, in addition to the MN's velocity. The proposed approach pre-computes the RSS which is expected to be observed at the boundary of the current cell. This ensures that the handover is triggered only when the MN is indeed at the

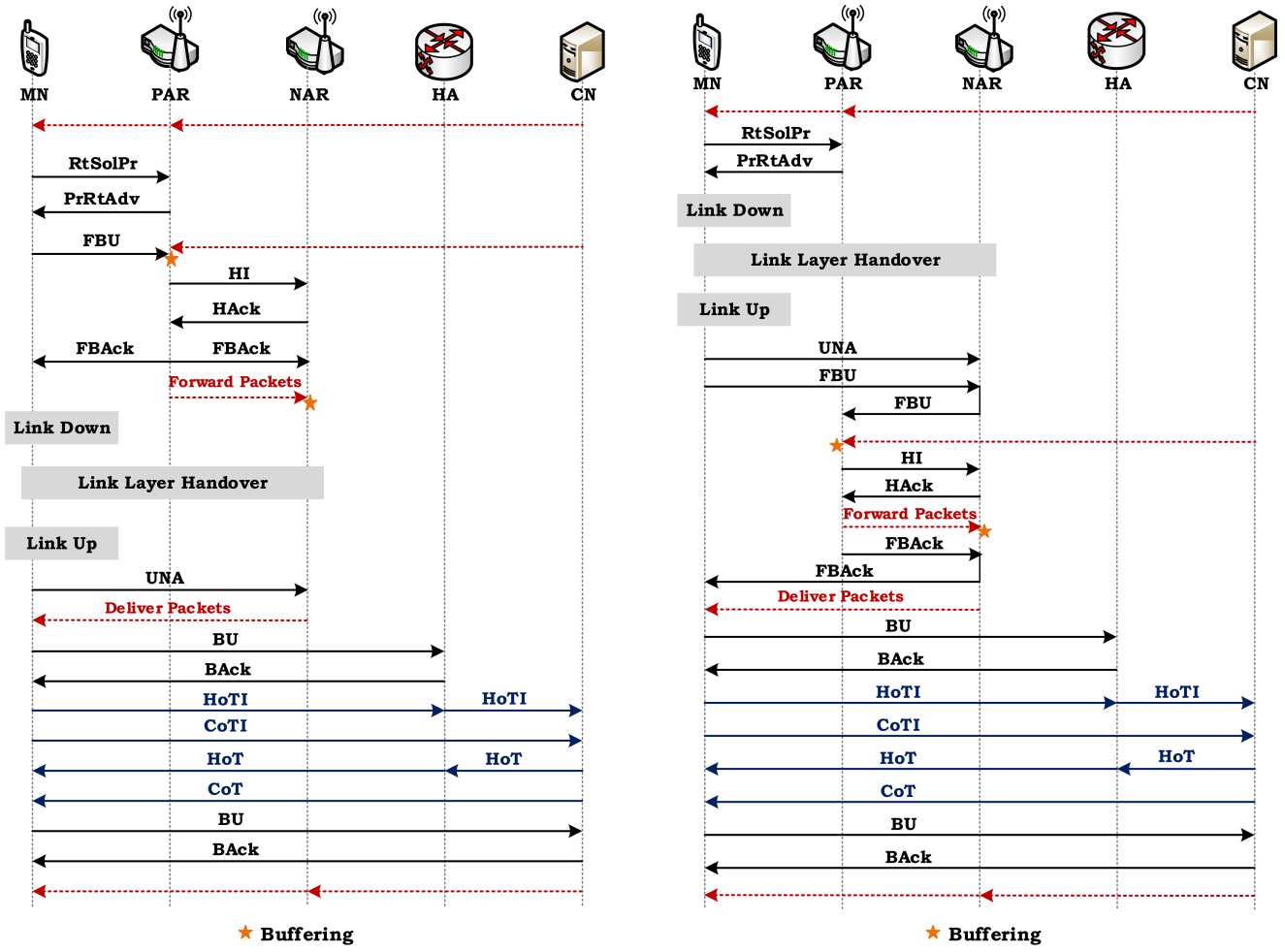

FIGURE 3. Signaling Sequence for FMIPv6. (a) Predictive Mode. (b) Reactive Mode.

boundary of the current attachment point, thus avoiding any false handover initiations.

The variations in wireless link quality can be of such an extent that it is very much likely for the RSSI to get stronger even after the L2 trigger. It is, therefore, worthwhile to evaluate the probability of the L2 trigger generation in the near future. In [42], based on the movement direction of MN, the probability of L2 trigger is assessed. Accordingly, the L2 trigger is either generated or ceased.

In a dynamic wireless environment, it is not always effective to generate triggers based solely on the RSS criteria [43] as factors such as signal fluctuations, moving speeds of MN, and diverse coverage areas of APs can cause wrong handover predictions. In literature, various schemes suggest using the criterion such as *Signal-to-Noise Ratio (SNR)* [44], *remaining link lifetime* [45], *signal decay* [43], and *movement pattern* [42], [46] etc.

A proposal in [47] suggests to completely replace the L2 triggers for handover anticipation with a *Prediction Algorithm* which is based on *data mining* algorithms and exploits the mobility history of the user. Based on this information, the algorithm predicts the next ARs the MN may move into. On similar principles, a Media Independent Handover[3] (MIH)-based Information Server [26] evaluates the *Possible Moving Area* for an MN based on specific parameters such as velocity, acceleration, coordinate values and movement detection which are conveyed to it on a constant basis.

In practical scenarios, the L2 trigger may not correspond to the handover process, in which case it is called *False Alarm*. The MN will have to perform all the handover procedures to re-attach with PAR including the nCoA formulation and DAD. In order to counter this, [48] proposes that the MN should re-access the PAR if it keeps receiving RAs from it. It is also suggested that the pCoA and its corresponding bindings with CN/HA should not be dropped right after the nCoA formulation or L2 trigger generation for a specified time. This is to ensure that the MN may re-access PAR

[3]The IEEE 802.21 Media Independent Handover (MIH) is discussed in detail in Section III-C

without CoA re-formulation and DAD. An enhancement of this proposal for vehicular environments is presented in [49]. In this scheme, in addition to reserving the pCoA and its bindings for a specific interval, the BU process at the new network is postponed to further reduce the impact of false alarm.

C. NCOA ACQUISITION

The nCoA acquisition process is reconsidered by several schemes with an aim to reduce the delays associated with it. Unlike [30], there can be other methods to create the nCoA as well. For example, [50] and [51] suggest formulating the nCoA through *pseudo-code* and the *International Mobile Subscriber Identity (IMSI)* respectively. Also, instead of MN, other protocol entities can also be delegated the responsibility of formulating the nCoA, like NAR [52], [53] and PAR [54] respectively.

In [55], a new routing policy is designed, according to which the MN can temporarily use its pCoA at NAR's link. The NAR also does not drop any packets received for the topologically incorrect address without verification. If it is able to verify the MN's previous association with PAR, it buffers the MN's traffic until its attachment. Similar schemes are proposed in [56] and [57] in which the MN uses a temporary CoA (usually the pCoA) during handover, while a proposal in [58] suggests using *anycast* address during handover. In [59], however, the NAR provides the validated and unique addresses from its pool which are to be used on a permanent basis. This scheme thus does not require nCoA formulation by MN or its subsequent verification through DAD.

D. DUPLICATE ADDRESS DETECTION (DAD)

The DAD process may become a major source of service degradation if it is not completed in a timely fashion. Few schemes propose to carry out this process in advance i.e. before the FBU message is sent [60], and thus completely eliminate the latency associated with it.

The proposal in [61], introduces the *Optimistic* IPv6 address concept which can be used by an MN for handover but has not yet completed the DAD process. According to the *Optimistic* DAD specification, the *Optimistic* IPv6 address should only be used if another suitable address is not available. The specification argues that the *Optimistic* DAD is useful because in most cases, the DAD process has much higher chances to be successful than to fail. Clearly, this proposal is only beneficial if the address collision probability is low.

An important issue that the DAD procedure can encounter is the looped back DAD messages, which needs to be suppressed. Certain techniques to counter this problem are discussed in [62].

E. BIDIRECTIONAL TUNNELLING

A bidirectional tunnel between PAR and NAR is established to forward packets from PAR to NAR in order to resume the MN's ongoing traffic at NAR's link, even before the MN initiates the binding update process. The tunnel establishment and maintenance, however, causes overheads associated to the packets tunneling/de-tunneling, link utilization as well as securing the tunnel [63]. As highlighted in [64], such issues aggravate with increasing number of handovers and volume of traffic to be tunneled. However, these issues can be partially addressed by carrying out the tunnel establishment process sufficiently in-advance i.e. even before the MN initiates the handover. An in-advanced tunnel establishment scheme in [65], proposes a *tunneling protocol module* which resides in each AR and establishes tunnels with neighboring ARs beforehand. It also takes care of the signaling required to establish tunnels, as well as deciding and negotiating the desired tunnel characteristics, which include security and encryption methods between the two tunnel endpoints.

The dependency on tunnels can also be minimized by pre-empting the handover functions like binding updates as discussed in Section II-G.

F. LINK LAYER HANDOVER

The FMIPv6 being the network layer mobility management protocol, does not directly discuss the L2 handovers. However, the successful completion of L2 handovers is necessary to accomplish the already initiated FMIPv6 operation. Any improvements in the L2 handover performance directly optimize the FMIPv6 handover as well.

As earlier discussed, the IETF has proposed the FMIPv6 specifications for technologies such as IEEE 802.11 [28], and IEEE 802.16e [29]. Several optimized solutions to enhance [28] and [29] have also been suggested which are discussed in detail in *access technology-specific* enhancements in Section VI.

G. BINDING UPDATE AND RETURN ROUTABILITY

Several optimizations have been proposed in the Binding Update and the Return Routability (RR) procedures in FMIPv6. These procedures carried out with CN achieve Route Optimization (RO). After RO, the NAR directly receives traffic from CN, instead of being tunneled from PAR. Thus, if carried out efficiently, these procedures can optimize the costs associated with the tunneling process.

The *Proactive Bindings for FMIPv6* approach is proposed in [66], in which the NAR carries out the binding update procedure on behalf of MN as soon as it receives the HI message from PAR. This approach proves to be an efficient scheme as the NAR knows the nCoA of MN much before the MN actually announces its presence on NAR. There are higher chances that by the time the MN connects to NAR, the NAR would have already completed the binding update process, hence the MN will be able to directly receive traffic from the CN right away. Similarly, [53] suggests that the CoTI message be sent to NAR by encapsulating it in the FBU and HI messages, which ultimately forwards it to the CN. Likewise, [67] suggests to carry out the Care-of

Test (CoTI/CoT messages exchange) proactively, while the *Enhanced Route Optimization* [68] scheme proposes the early home address test (HoTI/HoT messages exchange) prior to handoff. Another proposal in [52] suggests the BU to be carried out by the NAR, while in [69], PAR is responsible to carry out this process.

The *Proactive Route Optimization for FMIPv6 (PRO-FMIPv6)* [70] proposes that in addition to formulating the nCoA, the MN also formulates two tokens, *t1* and *t2*. Both these tokens traverse to the CN via different paths: *t1* is sent via HA and *t2* is sent via NAR. The respective binding update messages carrying each token are forwarded by HA and NAR which act as a proxy for each of these tokens. The CN checks the nCoA using both these tokens and subsequently sends the Binding Acknowledgement (BA) message to NAR.

Various route optimization schemes propose to utilize an intermediate *cross-over* router which can redirect the MN's traffic from the old location towards its new location at the time of handoff. This approach is similar in principle to the HMIPv6 protocol which relies on a local HA named Mobility Anchor Point (MAP), and essentially plays the role similar to the *cross-over* router. The *Optimal Crossover Router Discovery (OCRD)* [71], the *Crossover Router Pre-Discovery (CRPD)* [72], and the *Flow-based Fast Handover for Mobile IPv6 (FFHMIPv6)* [73] schemes are the examples of such an approach.

The BU process can also be carried out through other protocols which are not responsible for mobility management at the IP layer. In [74], the binding update information is sent through newly defined RSVP[4] (Resource Reservation Protocol [75]) objects: the *BU object* and the *BAck object*. Similarly, proposals in [76] and [77] use mSCTP[5] *chunks* to convey the new CoA to the CN beforehand and thus eliminate the binding update procedure at the network layer. Likewise, FMIPv6 and SIP[6] procedures are combined in [81] and [82] in which the MN sends the SIP RE-INVITE message to the CN as it acquires the new IP address. The CN, on session re-establishment, thus directs all ongoing sessions to the MN's new IP address directly.

[4]The RSVP Protocol reserves resources at new network. It is discussed further in Section IV-A3

[5]SCTP [78] supports transmission of multiple streams of data concurrently. It also supports multi-homing which allows an MN to have more than one IP address. Due to these features, it has been utilized for providing efficiency in mobility support. An extension to SCTP is described in [79] that allows SCTP to dynamically add or delete an IP address from an SCTP association. Through this extension, a primary address can also be set that could be used by a peer for sending to an endpoint. This specification defines two new chunk types, the *Address Configuration Change Chunk (ASCONF)* and the *Address Configuration Acknowledgement (ASCONF-ACK)*.

[6]SIP [80], being a multimedia signaling protocol is used to establish a voice or any multimedia session between endpoints. In SIP, a typical session starts when a user sends an INVITE message to a peer. The actual data flow begins after the recipient accepts this request. When a mobile node (User Agent or UA in SIP) moves into new IP domain and obtains an IP address, it has to carry out an update procedure with CN which is done by sending RE-INVITE message to it. The RE-INVITE message contains the new IP address as well as an updated Session Description Protocol (SDP). The ongoing session of the UA can therefore be resumed in the new network by the sending the RE-INVITE message to the CN.

Certain *unconventional* schemes for optimizing the BU have also been proposed. For example, in [83], the MN requests the CN to divert its traffic to its nCoA after a specific sequence number *N*. This scheme also suggests that the MN, instead of contacting NAR through PAR, should contact NAR directly through the internet. A *reverse binding update* scheme in [84] proposes that the PAR sends the FBU message to HA, in response to which the HA sends the *Reverse Packet Binding Update* to NAR. This would enable NAR to perform BU with CN well in advance.

The BU and RR procedures have certain security vulnerabilities as well, which also result is several inefficiencies. These are further discussed in *security-specific* enhancements of FMIPv6 in Section V.

H. BUFFERING

The buffering process in FMIPv6 aims to greatly reduce the packet losses during handover. However, there are certain factors which can affect its performance —the major being the handoff latency. If it is too high, the buffers cannot avoid packet losses due to their limited capacity. Secondly, the QoS is also impacted if the buffer containing sensitive packets is emptied abruptly since the limited bandwidth of the NAR's link could not appropriately handle them.

In order to counter the limited buffer space issues, [85] suggests that the routers should define the network load they can absorb and set a respective *price* according to a defined pricing strategy. This *price* information of the NAR is sent to the MN via PrRtAdv message. In case the MN accepts the *price*, it proceeds with the handoff process with NAR. The proposal in [63] also suggests the explicit allocation of buffer space for the MN's traffic at NAR before it receives any traffic from it. The required buffer size is shown to be dependent upon the interval of communication interruption in [86]. A proposal in [87] suggests adjusting the transmission rate between MN and AR according to RSSI for a better buffer management. In [88], the packet buffering is suggested to be done according to three QoS classes which are defined based on *per-hop behavior (PHB)* in the DiffServ (Differentiated Services) domain [89].

Some protocols suggest buffering to take place at entities other than PAR and NAR. In [90], it is proposed that the HA buffers the packets while the MN undergoes L2 handoff, while in [91], buffering at CN is proposed.

I. BICASTING

In standard FMIPv6 protocol operation, the PAR stops sending traffic to MN over its link as soon as it receives the FBU message from MN. All the incoming traffic of MN is instead buffered. However, in practical scenarios, the MN might be able to maintain the link with PAR for a significant period of time even after sending the FBU message. This scenario can result in significant handover latency. In order to counter this issue, the *Bicasting* mechanism is introduced [92]. In this approach, the PAR not only buffers the incoming traffic of MN, but also sends a copy of each packet to MN over its

wireless link, even after receiving the FBU message. The packets, instead of being buffered at PAR, may also be tunneled towards NAR if the tunnel is established.

The *Bicasting* however, can result in *packet duplication* as well as *out-of-sequence* arrivals at MN. To address these issues, the *FMIPv6 Bicasting with Selective Delivery (FMIPv6-BSD)* protocol [93] introduces a *counter* value, which is added to all incoming packets of MN after the FBU is received. This allows the MN to keep track of packets it received at PAR's link due to bicasting. After completing handover, the MN sends a list of received bicasted messages to MN in the UNA message. The NAR thus only delivers packets from its buffer to MN which it did not receive at the previous link.

J. OPERATIONAL MODE SELECTION

The FMIPv6 protocol is designed to primarily operate in the predictive mode in normal conditions. It switches to the reactive mode in case of predictive mode failure which generally happens due to rapidly deteriorating link conditions or fast movement of MN. It has been experimentally shown that the connection loss time (of an ongoing connection) in reactive mode can be up to more than 30 times than that of the predictive mode [94], resulting in high packet losses. In terms of cost analysis, while the reactive mode incurs slightly lower signaling costs compared to the predictive mode (approximately 2-3% only [12], [95]), the packet delivery costs, tunneling costs and the overall costs are the same in both modes [95]. However, the reactive mode may have better performance if the MN locates closer to the AR [96]. If the handover anticipation time is lower with the AR at closer vicinity, the packet losses will be lower too [96].

The effectiveness of predictive mode of operation depends on the reliability of the handover prediction. A study in [97] has shown that only about 50% of the total handover predictions are generally reliable. For analysis of both modes of operation, it is thus also essential to look into the factors and the probability of failure of the predictive mode. According to [98], the probability of predictive mode failure is dependent on several factors which include the radius of a cell, the velocity of the MN and the timing of the L2 trigger generation.

Since the reactive mode causes heavy packet losses, it is recommended to find solutions to minimize the chances of its occurrence. Boutabia and Afifi [99] suggest that in routine, the FBAck message should only be sent via new link instead of the old one, to increase the chances of successful predictive mode operation. A *Candidate CoA (CCoA)* approach is proposed in [100], in which a *CCoA* is configured by an AR and shared with its neighboring ARs beforehand. Whenever any MN requests information from it with MAC address of an associated AP, *CCoA* is provided to it right away and the time consuming DAD process and the involved signaling is eliminated. Thus the chances that the protocol will operate in predictive mode also increase. Various other approaches optimizing the nCoA acquisition and DAD procedure which can drive the protocol to operate in the predictive mode have been discussed in Sections II-C and II-D.

According to [40], the drawbacks of the reactive mode can be reduced, if the network, on learning about the MN's intention to handover, can itself drive the protocol into the reactive mode. The current subnet maintaining the ID's of all neighboring subnets can predict the new network and can trigger the reactive mode of operation by initiating procedures like tunnel establishment which are generally carried out after the MN attaches to new network during the reactive mode. A similar solution in [101] triggers reactive mode at PAR if the MN is having a real-time session, and the estimated handover latency of the reactive mode is less than a predefined threshold.

K. AVOIDING THE PING-PONG EFFECT

A scenario that completely nullifies the advantages of the FMIPv6 features such as in-advanced nCoA formulation, DAD and tunnel establishment, is the ping-pong effect. In this situation, the MN roams at the boundary of PAR and NAR, and constantly attaches/detaches to their links. Thus, the PAR and NAR have to constantly establish and withdraw the tunnel, repeatedly formulate CoAs and run the DAD process.

Few schemes in literature are proposed to handle this problem. According to [102], the PAR would not cancel the bidirectional tunnel with NAR immediately but would wait for a *wake-up* signal. If the MN returns to PAR, the NAR sends the *wake-up* signal to PAR, which would reactivate the two-way tunnel between them. Similarly, in [103], the PAR keeps the binding cache for MN active for a certain interval as instructed by the *Decision Engine (DE)*. In [104], the ongoing sessions are multicast to all the candidate networks at the time of handover to circumvent the ping-pong effect.

III. COMPLEMENTARY ENHANCEMENTS

The FMIPv6 protocol operation particularly relies on the effectiveness of (i) link-layer assistance, (ii) new AR/AP discovery, and (iii) (smooth) resumption of MN's traffic at NAR. However, the FMIPv6 specification, due to its limited scope, does not explicitly describe any of these operations. Therefore, certain enhancements which can complement the FMIPv6 operation with these mechanisms have been proposed. These enhancements essentially incorporate the signaling exchange of other protocols to underpin the FMIPv6 operation. These protocols prominently include IEEE 802.21 [26], Access router and access network discovery mechanisms [105], and context transfers protocol (CXTP) [106], respectively. These are briefly discussed in below subsections.

A. CANDIDATE ACCESS ROUTER/NETWORK DISCOVERY

The IETF has proposed the *Candidate Access Router Discovery (CARD)* [105] protocol which supports *MN-AR* and *AR-AR* communication to discover the candidate ARs (cARs) along with their capabilities. A combination of CARD and FMIPv6 has been proposed in [107] for efficient network

discovery. Due to CARD protocol, the MN may request information about its prospective cAR(s) as soon as it attaches to an AR. This enables the MN to formulate nCoA(s) for a respective cAR(s), as it receives the *reply* message. In the proposed scheme, the *MN-AR CARD request/reply* messages replace the RtSolPr and PrRtAdv messages respectively. And since this messages exchange can take place much before the L2 trigger, the probability that the protocol will function in the predictive mode increases. Moreover, since these messages also provide the L2 information with respect to the cAR under consideration, the MN performs scanning of the already known channels only, thereby reducing the overall scanning delay. Other optimizations based on CARD include [108] and [109].

The CARD protocol may provide L2 IDs of any APs associated with candidate ARs to the MN, however, it does not discuss the access network discovery process at L2. Therefore, in [110] an *Access Router Information Protocol (ARIP)* is proposed which performs both functions i.e. candidate access router discovery as well as the radio access network discovery within a unified protocol suite. In the *i-ARD* protocol [111], an AR in the FMIPv6 domain obtains information about its neighboring ARs and stores it in its cache. However, unlike CARD, the address resolution process is performed at the current AR of the MN.

B. CONTEXT TRANSFERS

The FMIPv6 operation can be further complemented if the context information of the MN is shared with NAR. The context information mainly includes (a). the authentication, authorization and accounting (AAA), (b). header compression, (c) QoS information [112]. Such a set of information is required to re-establish MN's ongoing traffic at NAR, and may result in a considerably slow resumption of traffic if it is not timely available.

The context transfers in FMIPv6 can be performed through IETF's Context Transfer Protocol (CXTP) [106]. Through CXTP, it is possible to transfer the context of an MN from PAR to NAR during or before the handover process. According to CXTP, the context transfer can be initiated by MN or by ARs. In [113], the MN initiated context transfer signaling has been combined with FMIPv6 signaling, thereby transferring the context to NAR in advance. Another example utilizing the CXTP can be found in [114], in which the context information such as user profile and service parameters are communicated to the new network during the handover preparation. The service parameters include QoS requirements of the ongoing service, and the user profile contains the information regarding user authentication with the new network.

C. IEEE 802.21 BASED LINK-LAYER TRIGGERING

The IEEE 802.21 standard has popularly been used for providing L2 triggering in FMIPv6 schemes. Although aimed at providing mobility support in heterogeneous networks by proposing a generic framework to the underlying access technologies, the IEEE 802.21 concepts intuitively apply to horizontal handover scenarios as well.

The IEEE 802.21 introduces an intermediate layer which resides between the link-layer and the upper layers, and is called Media Independent Handover Function (MIHF). The MIHF provides services which include Media Independent Event Service (MIES), Media Independent Command Service (MICS), and Media Independent Information Service (MIIS). The information associated with these services is exchanged between MIHF and the upper and lower layers through a set of *primitives*. For example, *Link_Detected* primitive communicates an event to the MIHF from link-layer that it has detected a new link. The MIHF can then provide this event information to an upper layer protocol like FMIPv6 through *MIH_Link_Detected* primitive. A generic representation of the IEEE 802.21 framework is shown in Figure 4.

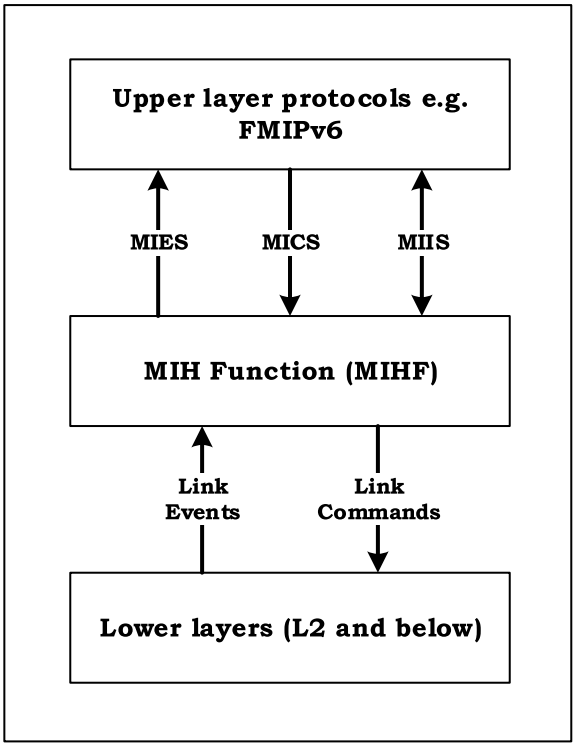

FIGURE 4. A Generic Framework for IEEE 802.21 specification [26].

Since the FMIPv6 specification does not describe any particular anticipation mechanism from the link-layer to perform its network layer operations, incorporating the MIH framework provides a suitable solution for providing anticipation to FMIPv6. Thus several solutions optimize FMIPv6 protocol through MIH primitives. Many of these solutions adopt the standard primitives, while others either extend them or propose the new ones. Through MIH framework, these solutions are not only able to reduce the L3 signaling loads, but are also able to counter the standard handover latency and packet losses as well. Many solutions also promise reduced handover anticipation time which increases chances for the protocol to

operate in predictive mode. Moreover, it helps in avoiding complications associated with uncertainty in the handover anticipation time e.g. the timing of L2 trigger generation.

A FMIPv6 optimization in [115] uses a subset of existing IEEE 802.21 primitives, along with a newly defined *Heterogeneous Network Information (HNI)* report which carries the subnet prefix of neighboring ARs, L2 information of their associated PoAs, their MAC address, channel range, and other parameters such as data rates etc. The *HNI report* is contained in the MIH Information Server and can be delivered to MN through *MIH_Get_Information request/reply* service primitives. The MN saves this report in the proposed *Neighboring Network Report (NNR)* cache.

As the link conditions become weak, the MIH Function (MIHF) generates the *MIH_Link_Going_Down* trigger to L3 (i.e. to the MIH user at L3, which is FMIPv6 in this case). The MN selects an appropriate PoA based on the information it has saved in its *NNR* cache without requiring to go through the scanning process. The L3 of MN next generates the command to L2 indicating it to switch the link using *MIH_Link_Switch* primitive. After the successful completion of L2 handover procedures, the L2 generates the *MIH_Link_Up* notification to L3 indicating the successful link establishment with the new PoA. Immediately after this, the FNA/UNA message is sent to the NAR and after the MN starts receiving traffic on the new link, the MIHF sends the *MIH_Link_Switch* response to L3.

A similar proposal is also proposed in [116] in which the MN gets information about the suitable AP and AR through the MIH Information Server. The scheme in [117], however, suggests to avoid using the MIH Information servers for such purposes as they incur additional delays. In [118], new MIH primitives and their parameters are defined. For example, the prefix information is provided through a newly defined primitive named *MIH-PrefixInfo*.

Another scheme on similar principles is proposed in [119], which promises the active delivery of packets to the MN until the *physical disconnection* of its link with current PoA (even after the FBU message has been received at PAR). This is in contrast to the existing FMIPv6 process in which traffic delivery to the MN from the previous link is stopped as soon as the PAR receives the FBU message. The proposed mechanism is achieved through efficient utilization of MIH services. The MIHF of the current PoA subscribes to the *Link_Going_Down* event of the MN. This enables the current PoA to notify the *Link_Down* event to the PAR as soon as it learns about it. The PoA can learn about the MN's link disconnection either after having explicitly performed the *disassociation* procedure with MN, or after the successive acknowledgement time-outs. On similar principles, the NAR subscribes to the *Link_Up* event of the MN with the MIHF of nPoA. This enables NAR to start delivering packets to the MN even before receiving the FNA message from it.

Other MIH-based FMIPv6 optimizations can be found in [120]–[122].

IV. SUPPLEMENTARY ENHANCEMENTS

Certain enhancements in FMIPv6 aim to support *advanced* handover services, which include (a) QoS support during handovers, (b) Multicast mobility support, and (c) Vertical handovers support. Adding these features to FMIPv6 provides a richer mobility experience to MNs [21] within a unified protocol framework. Since such enhancements supplement the baseline FMIPv6 protocol operation, these are referred to as *supplementary* enhancements in this paper.

A. QOS SUPPORT IN FMIPv6

For an accomplished FMIPv6 handover operation, it is desirable that the QoS is ensured for MN during its handover i.e. when it initiates and executes handover, and when it attaches to the new network after handover. The QoS in the context of FMIPv6 handovers can thus have different meanings i.e. (i) the transmission parameters (e.g. the TCP parameters) of ongoing sessions between MN and the CN are appropriately re-adjusted during the handover initiation, execution and traffic resumption at NAR, (ii) the appropriate resources to resume the MN's ongoing sessions are available and reserved at the new network to which the MN hands over to, and (iii) appropriate resources are available/reserved along the path between an intermediate/gateway node and NAR. Thus, the QoS specific enhancements in FMIPv6 are accordingly categorized into further three categories as follows.

1) TCP PROTOCOL ADJUSTMENT

The QoS during handover can be supported if the transmission parameters at the transport layer are readjusted during handover. Several studies on FMIPv6 performance enhancement have focused on adjusting certain standard TCP parameters such as *RTO* (*Retransmission Timeout*), *cwnd* (*Congestion Window*), *ssthresh (Slow-start Threshold)*, *RTT (Round Trip Time)* as well as timers such as *Retransmit* timer and *Persist* timer to improve QoS during handover.

In FMIPv6, one of the reasons of poor performance of TCP is the *out-of-sequence* problem which occurs when a MN receives packets from NAR which are tunneled from PAR, as well as those which are sent directly to MN from the CN. The second major issue is that any packet losses during the transmission in TCP are considered to have occurred due to network congestion. The TCP sender consequently drops its transmission window. If those losses were occurred in reality due to the handover process, such actions of the TCP sender would degrade the ongoing session.

The *out-of-sequence* problem in TCP during handovers is discussed in [123], according to which the packet sequence number is checked before the packet is buffered at NAR. This helps in delivering the buffered packets in their correct order.

In [124], a *FREEZE* phase is introduced at the time of handover during which the CN freezes the *retransmit* timers. During this phase, back-to-back measuring packets are sent

from the CN which are used by the receiver to estimate the bandwidth of the link. The MN estimates the available bandwidth and conveys it to the CN through a *TCP bandwidth option* in the TCP header within the ACK message. The CN adjusts the TCP parameters such as *RTO*, *cwnd*, *ssthresh* according to the new link conditions.

In a similar scheme in [79], the CN freezes the *RTT* and cancels the *Persist* timer so that no probes are sent. The CN for this purpose, receives handover indication through the *Handover Start Notification* message, and later resumes the normal TCP operation when it receives the *Handover Finish Notification* message. Likewise, in [125], a cross-layer based interaction between MIPv6 and TCP is proposed, in which the TCP parameters such as *RTO*, *cwnd*, *ssthresh*, *RTT* etc. are re-adjusted based on the handover initiation and termination indications received from MIPv6.

Similarly in [126], a *path-over* scheme in FMIPv6 networks is proposed, according to which the MN constantly sends a *QoS-Measurement-Chunk* (an mSCTP chunk) to CN reporting its currently degrading wireless conditions. The CN, in turn, varies the *cwnd* and *ssthresh* parameters while sending traffic to MN.

2) RESOURCE RESERVATION AT NAR

The FMIPv6 protocol can enable the transport of MN's QoS context to NAR before the MN attaches to it. The QoS context can be conveyed to NAR through HI/HAck messages from PAR. Consequently, the NAR having received the context information of MN in advance, is able to manage and allocate its resources for the handover flows of MN. A dynamic allocator is introduced in [127] and [128] which performs adaptive resource management in order to improve the network utilization. A similar scheme [129] relies on a central network entity named *Domain Resource Manager (DRM)* which is responsible for managing resources in a particular administrative domain. The MN at handoff has to coordinate with DRM to request any resources it requires at the new network. Similarly, a *QoS Broker* is introduced in [130] for resource management for MNs undergoing handover.

3) END-TO-END QOS

Unlike various QoS handover protocols which usually discuss QoS assurances at NAR (e.g. by reserving or managing its resources for MN), some enhancements in FMIPv6 focus on the *end-to-end* QoS guarantees over the new path towards NAR. The CXTP protocol is optimized in [131] in order to achieve this goal. It is argued that the baseline CXTP specification by the IETF cannot meet such an objective because contexts are transferred only between ARs. Thus, in the proposed scheme, the *Context Transfer Data (CTD)* message is enhanced through the addition of a *Hop-by-Hop extension* header. This message is sent from PAR to NAR via an intermediate node. All network entities along the new path, i.e. from the intermediate node to NAR, reserve resources for MN's active sessions accordingly. Similarly, another scheme is proposed in [132] which also establishes a new route between a gateway node and NAR, that can assure the desired QoS for the MN. Unlike [133], which used enhanced CXTP messages, this scheme utilizes the RSVP signaling to create the new QoS path between MAP and NAR. Another RSVP based scheme is proposed in [134] in which an intermediate node reserves resources for the MN in both uplink and downlink directions during handover.

A QoS support solution named *Differentiated Dynamic QoS Provisioning (DDQP)* for QoS provisioning in SUPANET architecture [135], is integrated with FMIPv6 protocol in [136]. Three types of pre-established *virtual* tunnels (VTs) are defined for constant and variable bit rate time critical data flows as well as for non-time critical data flows respectively. The ARs are also responsible to dedicate certain amount of timeslots for each kind of VT. At the time of handoff, two timeslot request (*TS_Req*) messages, *TS_Req-To_PAR* and *TS_Req-To_NAR* are encapsulated in the FBU message to request timeslots from PAR and NAR respectively.

A QoS signaling framework proposed by IETF, named *Next Steps in Signaling (NSIS)*, is believed to have better performance in terms of flexibility and scalability when compared to other popular QoS protocols like RSVP. In [137], a combination of QoS *NSIS Signaling Layer Protocol* with FMIPv6 is proposed. This approach also reserves resources along the path towards NAR in advance (i.e. before the MN attaches to it).

B. VERTICAL HANDOVERS SUPPORT IN FMIPv6

The IP layer, being the common convergence layer for disparate access technologies, can provide support for vertical handovers (VHOs) in heterogeneous environments. Several enhancements in FMIPv6 have been proposed to add support for vertical handovers in its operation.

The IEEE 802.21 specification has popularly been utilized in majority of these solutions since it provides a generic framework for handover-related information exchange among heterogeneous networks. Several FMIPv6 enhancements providing vertical handover support through IEEE 802.21 have already been discussed in Section III-C. This section overviews other IEEE 802.21-based schemes as well some other approaches for vertical handover support in FMIPv6.

In vertical handoffs, the process of handover decision is of primary importance. Unlike the horizontal handovers which are triggered normally due to deteriorating wireless link characteristics, the vertical handover decision is taken based on a number of parameters which include, for example, the monetary cost of the candidate network, user preferences, bandwidth availability, security and reliability etc. [138]. A plethora of vertical handoff decision algorithms based on these decision parameters have been proposed [138], and can be applied to FMIPv6 for providing the handover trigger in heterogeneous networks [60].

In case of vertical handoffs, the packet loss issue can exacerbate due to varying characteristics of the involved

heterogeneous networks. In [139], a FMIPv6-based *SafetyNet* protocol is proposed which multicasts packets to all the candidate AR(s) in the heterogeneous environment. The protocol also proposes a selective delivery approach in order to minimize the overhead for the wireless link data transmission, and ensures that only the missing packets are selectively delivered to the MN when it joins the new network.

A WiMAX to WLAN handover scenario is presented in [140], which utilizes the MIH framework and FMIPv6 signaling. In the considered scenario, the MN constantly seeks information about the alternative opportunities for connectivity from the MIH Information Server. When it receives any beacon frame from the neighboring WiFi APs, it can request information about networks they are associated to, from the MIH Information Server. This information may include information about the monetary cost, security, available bandwidth etc. For this purpose, the MN exchanges the *MIH_MN_HO_Get_Information Request/Response* messages with the Information Server. Figure 5 shows the detailed handover procedure of the proposed scheme. A similar solution which focuses on vertical handovers between 3GPP and non-3GPP networks is proposed in [141].

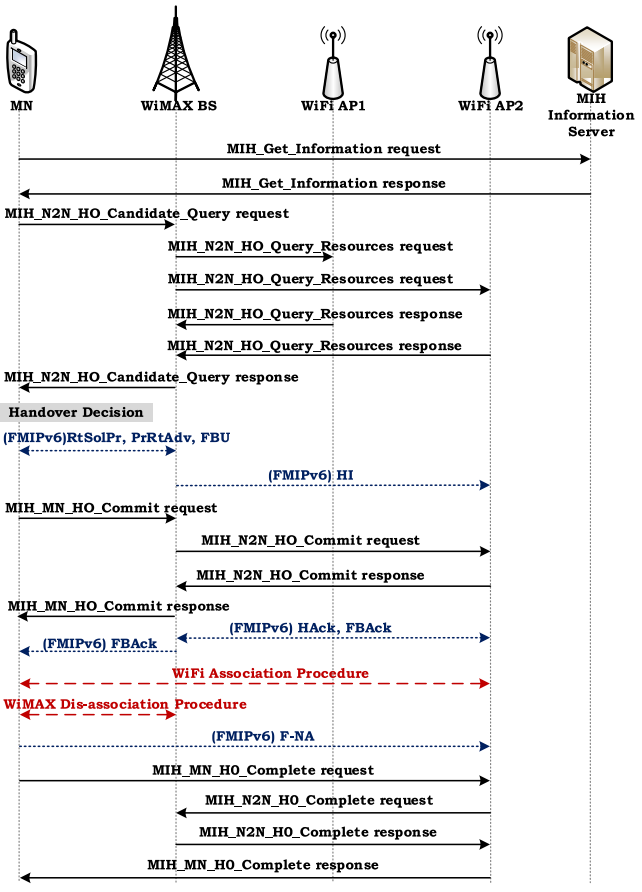

FIGURE 5. WiMAX to WiFi Handover Scenario with MIH Support proposed in [140].

In [142], another FMIPv6-based VHO scheme is proposed which utilizes the IEEE 802.21 primitives. Unlike the standard FMIPv6 protocol in which the MN will not receive any packets after sending the FBU message, the PAR only stops sending packets to MN when it receives a remote *Link_Down* indication from the MN's PoA (which is also capable of detecting the *Link_Down* event). After the successful layer 2 handoff, the MN updates its ongoing SIP session by sending the *SIP RE-INVITE* message to the CN. Until the MN receives the corresponding *SIP 200 OK* message, it uses its old IP address as source address for sending packets to the CN.

C. MULTICAST MOBILITY SUPPORT IN FMIPv6

The primary focus of the baseline FMIPv6 specification is resuming the *unicast* sessions of MN at NAR. Thus, it needs to be enhanced in order to the support the *multicast* traffic resumption after handover.

In order to realize the multicast services in a mobile environment, it is essential to have the supportive multicast routing and group management protocols, which can interwork with the handover management protocols. The group management protocols (e.g. Multicast Listener Discovery (MLD) [24], [25]) enable a mobile user to join or leave a particular multicast group, while the multicast routing protocols (e.g. Protocol Independent Multicast (PIM) [22], [23]) are required for the construction of distribution trees for delivering the multicast traffic from source to the receivers.

The IETF has recently put forward an experimental protocol specification for multicast mobility support in FMIPv6 [143]. The PrRtAdv message in this specification is extended to include an *M* bit which indicates that the current AR supports multicast services. When submitting the FBU message, the MN attaches *mobility options* which contain the multicast groups information the MN currently subscribes to. The HI message is similarly extended to carry these multicast context options. The NAR, if able to support each requested multicast group, responds with multicast acknowledgement within the HAck message. This acknowledgement is then also added to the FBAck message by PAR. The NAR implements the MLD Proxy [144] towards PAR to perform the MLD host-part function. It signals particular groups that it is willing to receive multicast traffic through the tunnel by sending the MLD report. The NAR meanwhile subscribes to the required multicast groups for the MN as well.

Prior to this, the M-FMIPv6 protocol [145] had also been proposed which also utilized the same approaches for multicast handover support. Two new types of options – the *Mobility Header (MH) multicast option* and the *ICMPv6 Multicast Address option* – were defined. The *MH Multicast Option* is added to the FBU message which contains the multicast address(es) that the MN currently subscribes to. The HI/HAck messages exchange takes place between PAR and NAR with an *ICMPv6 Multicast Option* carrying similar information as that in the *MH Multicast Option*.

The multicast routing and group management protocols have previously been utilized for several multicast-extensions in FMIPv6. Table 1 summarizes their major features. It is worth noting that the proposed FMIPv6 multicast enhancements involve the principles of the generic Home

TABLE 1. Summary of primary features of FMIPv6 enhancements of multicast mobility support.

Proposed Protocol	Design Principles			Integrated Unicast/ Multicast Support	Protocol Dependency		Node Mobility	
	HS-based	RS-based	MA-based		MLD	PIM	Source	Listener
M-FMIPv6 [145]	×	✓	×	✓	×	✓	×	✓
FTJ-FMIP-RS [147]	×	✓	×	✓	×	✓	×	✓
Zhang et al.'s Proposal [148]	×	×	✓	×	✓	✓	×	✓
MC-MIPv6 [149]	✓	✓	✓	✓	✓	✓	×	✓
Yoo et al.'s Proposal [150]	✓	✓	×	✓	✓	✓	×	✓
FMIPv6 for ETM [151]	×	✓	×	×	×	✓	✓	×
Kwon et al.'s Proposal [152]	×	✓	✓	✓	✓	✓	×	✓
LMM for FMIPv6 [153]	✓	×	×	✓	✓	×	×	✓
M-FMIPv6/FTB [154]	×	✓	×	✓	✓	✓	×	✓

Subscription (HS), Remote Subscription (RS) and Multicast Agent (MA) based approaches [146]. In HS (also known as Bi-directional tunneling) approach, the MN subscribes to the multicast tree through its HA which forwards multicast traffic to MN at its existing location. In RS, the NAR joins the multicast tree to resume the multicast traffic of MN. In MA-based approaches, a multicast agent joins the multicast tree and forwards traffic to MN at its current location.

1) PROTOCOL INDEPENDENT MULTICAST BASED ENHANCEMENTS

As an MN moves into a new network with active multicast session(s), the NAR has to be associated with the respective multicast trees, to be able to receive and deliver the multicast flows to the MN. The Protocol Independent Multicast (PIM) is used in several schemes for this purpose. The NAR has to associate itself directly to the multicast tree or to the PIM's *Rendezvous Point (RP)* which is a network node already part of the multicast tree.

The RS approach is preferred over the HS for most of the optimizations presented herein, since it ensures optimal routing (Table 1). However, there is a possibility for the tree joining operation taking a longer time during which a significant data may be lost (e.g. due to buffer overflow at PAR). The RS-based *Fast Tree Join* mechanism for FMIPv6 Multicast Handover *(FTJ-FMIP-RS)* scheme [147] discusses the unpredictability/uncertainty associated with the multicast tree expansion latency. Thus, in the proposed scheme, the NAR starts the multicast subscription as soon as it detects the multicast handover event by receiving HI message from PAR.

In [148] and [149], the multicast communication is resumed at the new network through an RP. In [148], the MPLS (Multi-Protocol Label Switching) crossed Label Switch Router (CLSR) is the supposed convergence point, while in MC-MIPv6 (Multicast Convergence based MIPv6) [149], the RPs have particular domains in which they handle the multicast communications. The NAR, in this case, subscribes to the RP of its respective domain to resume the ongoing communications for the MN.

Another solution in [150] attempts to provide a pragmatic approach supporting various possible multicast service subscription methods by NAR. The four possible methods for the provision of multicast service at NAR include (i) path extension, (ii) HS, (iii) RS, (iv) NAR already on the respective distribution tree. The NAR selects the method using information in HI-M (a multicast extension of HI) message, as well as the hop count values among the multicast source, HA, PAR and NAR.

The mobile multicast support mechanisms described above are used for multicast receiver's mobility, and do not address the mobility of the multicast source. An *Enhanced Tree Morphing (ETM)* scheme in [151] relies on the address duality concept i.e. two addresses are used by the mobile multicast source when it is away from its home network. It uses its CoA at the network layer but HoA at the application layer to send data to the multicast tree. After handover, as the mobile source announces its attachment on NAR, the data will be distributed to the previous distribution tree via NAR-to-PAR reverse tunnel; thus benefiting various receivers associated with the previous distribution tree.

2) MULTICAST LISTENER DISCOVERY BASED ENHANCEMENTS

The MN can initiate joining a multicast group by sending the *MLD report* message. The *MLD report* message carries the multicast addresses that the MN currently subscribes to. The MLD signaling between the PAR and NAR also takes place when PAR, on learning the MN's prospective handover, requests the NAR to join a particular multicast tree for MN.

An MLD-based FMIPv6 enhancement proposed in [152] requires the tunneling of the multicast traffic from PAR until the NAR completes subscription with the desired multicast groups. For this purpose, the PAR first sends *MLD Query* messages towards MN to learn the multicast groups it has active subscriptions with. The MN, in response, sends the *MLD Report* messages to PAR. This multicast information is conveyed to NAR, which initiates the *Join* process for MN. When the *Join* process completes, the MN is required to tunnel *MLD Done* messages to PAR. If the MN does not send the *MLD Report* message, or the PAR receives the *MLD Done* message from it, packet forwarding to MN from PAR stops, as PAR assumes that the NAR has successfully joined the multicast groups.

A *Light-weight Mobile Multicast (LMM)* protocol in [153] for FMIPv6 is designed by simplifying the MLD Proxying [144] which functions only through *join* and

leave messages. For protocol operation, the simplified MLD proxy function is implemented at HA, in such a way that the upstream interfaces connect to the multicast router, while the downstream interfaces connect to the multicast subscriber. Accordingly, the upstream and the downstream interfaces perform the MLD host part and the MLD router part functions respectively. The MN sends an unsolicited *MLD report* message to HA every time it detects a change in its address. When it moves out of its home network towards PAR, it establishes a bidirectional tunnel with HA through BU/BA messages. The *MLD report* is then tunneled to the HA which, in turn, tunnels back the multicast data. When the MN moves from PAR to NAR, it performs FMIPv6 handover during which the PAR forwards multicast packets to NAR through the established tunnel among them. The NAR buffers these packets until it hears the FNA (or UNA) message. After this, the MN again sends the BU message to HA which then starts packet transmission to MN directly via NAR.

The Multicast Fast MIPv6 with *Flow Tunneling and Buffering (M-FMIPv6/FTB)* [154] scheme relies on conditional tunneling of multicast traffic on a *per flow* basis instead of *per mobile node* basis. It also makes the NAR capable of receiving multicast traffic in advance before the MN's attachment with it. After the nCoA formulation, the MN sends the FBU containing the *multicast membership information* inserted in specially defined ICMPv6 options, identical to those of M-FMIPv6 [145]. Similarly, the HI message carries ICMPv6 option for multicast membership control information which triggers NAR to configure its interface to make it supportive for the multicast transmission. As shown in Figure 6, the multicast routing signaling follows this interface configuration. Next, after sending HAck, the NAR also tunnels an *MLD Multicast Listener Report* whose reception at PAR actually triggers the multicast traffic tunneling instead of HAck message reception. This procedure also allows NAR to request tunneling of traffic for only those groups which it has not yet subscribed with, thus realizing the *conditional* tunneling approach.

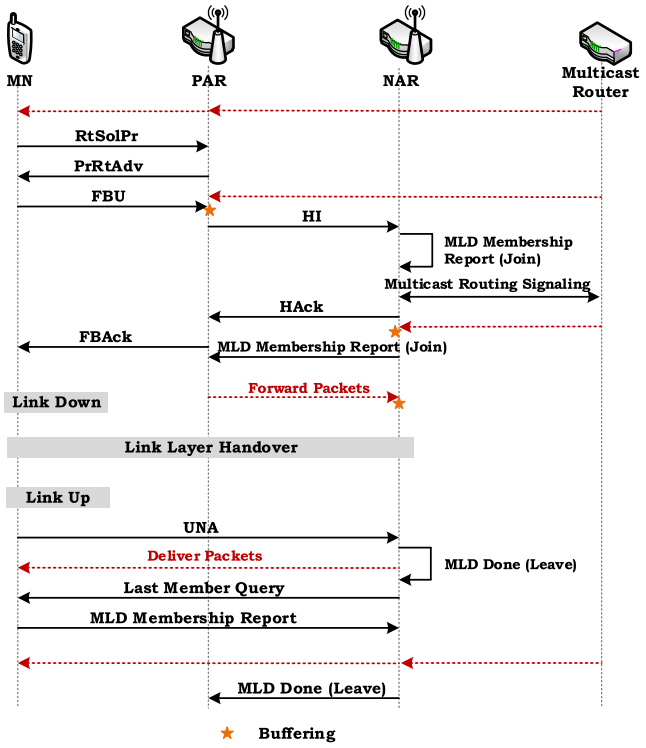

FIGURE 6. Protocol Operation for M-FMIPv6/FTB Scheme [154].

V. SECURITY-SPECIFIC ENHANCEMENTS

The FMIPv6, being the extension of MIPv6, not only faces security challenges it inherits from MIPv6, but also certain additional security threats due to its distinctive operational features. Several protocols aimed at securing MIPv6 are thus applicable to FMIPv6, since it relies on the BU/RO/RR procedures of MIPv6 [155], [156]. However, this section mainly focuses on security challenges, as well as their solutions, within the FMIPv6 protocol operation. In this regard, the possible security threats to FMIPv6 as indicated in the literature are first highlighted.

A. SECURITY THREATS TO FMIPv6

Following are the key security threats which FMIPv6 faces.

- *DoS Attack:* In *Denial-of-Service* (or *DoS* attack), the services or resources of a network node (e.g. a CN) are made unavailable to the legitimate users of the network [155].
- *Session Hijacking:* In *Session Hijacking*, the MN redirects traffic of a victim node towards itself [157].
- *Malicious Mobile Node Flooding:* In the *Malicious Mobile Node Flooding* attack, a valid MN redirects its traffic to a victim node [157].
- *Man-in-the-Middle:* In *Man-in-the-Middle* attacks, an attacker inserts itself in the communication path between two communicating nodes (e.g. a MN and a CN), possibly modifying the signaling exchanges between them or causing session hijacking [155].
- *Replay Attacks:* In *Replay* attacks, an attacker who can itself be the source of data or man-in-the-middle entity, repeats the data transmission (or a signaling message) towards a victim node (e.g a MN or CN) [155].

Here, the *Session Hijacking* and *Malicious Mobile Node Flooding* attacks are the categories of *Redirection* attacks [157]. Some other possible security threats which FMIPv6 protocol may face include,

- *Return-to-PAR Spoofing Attack:* In *Return-to-PAR Spoofing* attack, an attacker may pretend to be a MN returning to PAR. The PAR thus may stop packet forwarding towards NAR and instead divert all its traffic to the attacker node. This is also a form of *Session Hijacking* attack.
- *Man-on-the-side attack:* In *Man-on-the-side* attack, the attacker may only read or insert new traffic for any ongoing session among two entities (e.g. a MN or CN). It is also a form of *Man-in-the-Middle* attack.

- *Relay attack:* In *Relay* attack, the attacker acts as a relay and may request connection simultaneously to two nodes (e.g. a MN and CN) while masquerading as the other node. Thus, an unwanted communication session (or unwanted traffic exchange) can be established among two victim nodes.

There could be different possible scenarios in which these attacks can be launched in FMIPv6, essentially exploiting the FMIPv6 signaling. Some of such scenarios are described below:

- *RtSolPr/PrRtAdv:* The RtSolPr message can be intercepted by an attacker which can reply MN with a false PrRtAdv message. This could cause the MN to handover to a *rogue* router [8]. Likewise, an unsolicited network-initiated PrRtAdv message sent to the MN by an attacker may also cause it to handover to a *rogue* router [8]. In this case, the MN may send FBU to PAR which would then start forwarding MN's traffic to the target AR resulting in the MN's *Session Hijacking* by the target AR [157].
- *FBU:* The FBU message can be used to launch a variety of different attacks, e.g., an attacker may send a fake FBU to PAR with wrongful information about MN's imminent handover to an NAR. The PAR exchanges HI/HAck messages with NAR with a DAD process also taking place at NAR. If the number of these fake FBU messages increases, both PAR and NAR get overloaded – the PAR processing HI and NAR processing HAck messages along with DAD. This may result in simultaneous service degradation of both entities. Various other attacks which include *Malicious Mobile Node Flooding, Session Hijacking* etc. can also be launched by mis-using the unsecured FBU message [157].
- *UNA:* In the network re-attachment phase, the UNA message can also be exploited just like the FBU message. An example scenario is the *Man-in-the-Middle* attack where an attacker comes between the MN and the NAR, and intercepts the UNA message [157]. It obtains the nCoA and the L2 address information of MN and masquerading as NAR, sends a fake *Neighbor Advertisement Acknowledgement (NAACK)* message to MN. Through NAACK, the attacker may indicate the MN that the nCoA communicated through the UNA message is invalid and may communicate it a bogus nCoA to use at NAR's link. On the other hand, the attacker may also communicate with NAR showing itself as a valid MN which had already sent its details through PAR. It may thus consequently intercept the MN's traffic sent to it from NAR [157].

It is to be noted that the BU-related signaling (i.e. BU/BAck, CoT/CoTI, and HoT/HoTI) can also be exploited to launch the aforementioned attacks. For example, *DoS* attack can be initiated by an attacker by sending a false BU message to CN, falsely indicating it that the MN has moved to another location, where actually a victim node resides. The CN can thus divert heavy traffic volumes to the victim node, potentially resulting in exhaustion of the victim's resources. Likewise, an attacker can replay a previous BU message towards CN, thus hijacking the ongoing session of MN.

Other attacks such as *Malicious Mobile Node Flooding*, *Man-in-the-Middle*, *Return-to-Home Spoofing* attacks etc. can also be launched through BU-related messages. All these attacks, the corresponding scenarios in which they can be launched, and several solutions to prevent them, have been discussed in detail in [155] and [156]. Some other related studies include [158]–[162].

B. SECURITY SERVICES

In order to address the above mentioned threats, certain security services have been used in the proposed solutions to secure the FMIPv6 signaling. These include:

- *Confidentiality:* Confidentiality means that a message exchanged between two nodes is encrypted (e.g. through a shared key), and is thus unintelligible to any other network node [172]. A special kind of *session key* termed as the *handover key* is used by several FMIPv6 enhancements for this purpose.
- *Integrity:* Integrity means that a message arrives at the intended receiver exactly as it was sent by the sender node, without any information being altered accidentally or maliciously [172]. The integrity of a message can be preserved by creating a *digest* of the message through a hash function. The *digest* needs to be sent separately and secretly to the receiver. The receiver also derives the *digest* using the same hash function, and compares it with the *digest* it received along the message. If both *digests* are the same, the integrity of the message is verified. Otherwise, it is assumed that the message has been modified [172].
- *Authentication:* Authentication of a message means validating that the sender of the message is a legitimate and valid node [172]. The authentication of a message can be ensured by using the *Message Authentication Code* (*MAC*). The *MAC*, like the *digest*, is derived through a hash function and a symmetric key between the sender and the receiver. The receiver re-computes the *MAC* over the received message. If the re-computed *MAC* is found to be the same as the one received with the message, the message is considered to be originated from an authentic source [172].
- *Nonrepudiation:* Nonrepudiation ensures that the sender of the message cannot deny a message which was in fact sent by it [172]. *Digital signature* is a popular technique to ensure non-repudiation. A *digital signature* can be generated through a private key at the sender and public key at the receiver (or verifier). Often, a *digital signature* is an encrypted message *digest*. Just like the *digest*, the *digital signature* also needs to be sent separately with the data (or a control signal). Note that the *digital signature* can also be used for other security services such as message authentication and integrity [172].

C. SECURITY ENHANCEMENTS TO FMIPv6

Many of the security challenges highlighted in Section V-A can be solved if the FMIPv6 signaling messages are secured. Some of the prominent enhancements in FMIPv6, aimed at securing its signaling messages, are discussed in this section. The key approaches used in these enhancements include the Secure Neighbor Discovery (SEND)-based approach, the Group-key based approaches, the One-way hash chain based approach, the Handover Key Server based approaches, and the Cross-layer based approaches. These solutions, as summarized in Table 2, have different features and are aimed at mitigating different threats.

Some of these solutions are infrastructure-based meaning that they rely on some sort of security infrastructure such as AAA Infrastructure or *Handover Key Server* [169]. Infrastructure-less solutions do not require such infrastructure to provide security services. Some solutions proposed for FMIPv6 rely on security infrastructure only when they initially enter a new domain, and do not require any such infrastructure during subsequent handovers. We define such solutions as Partially Infrastructure-based solutions. As noted in Table 2, the Infrastructure-based and Partially Infrastructure-based solutions mostly rely on the widely deployed AAA infrastructure. On the other hand, the Infrastructure-less solutions can function entirely by enhancing the FMIPv6 signaling, and do not require any additional signaling or security protocols.

1) SEND-BASED ENHANCEMENTS

The FMIPv6 protocol operation initiates with Neighbor/Router discovery operations as discussed in Sections II and III-A. However, the default neighbor discovery protocol [173] is prone to certain security threats [8] as it requires manual configurations for security association between nodes [174]. Thus, aimed at securing the neighbor discovery, SEND protocol is proposed, which functions on zero-configuration mechanism. The SEND protocol uses Cryptographically Generated Addresses (CGAs) to make sure that the claimed source address by the sender of the Neighbor Discovery (ND) message is indeed the owner of that address. Moreover, the public key signatures are also used to protect the integrity of the messages.

The *SEND* protocol is used in [163] in order to secure the FBU message. The FBU message sent by the MN is effectively responsible to redirect its traffic towards the nCoA, and can be easily misused to initiate various attacks as discussed in Section V-A.

The SEND protocol, although considered as security standard for FMIPv6 due to the above mentioned features, still suffers from expensive computational costs. Moreover, other security attacks which may be launched by exploiting the RtSolPr/PrRtAdv and UNA messages which are not secured through SEND. Aimed at securing these messages, another SEND-based scheme is proposed in [164]. The concept of *handover key* is introduced in this scheme for securing these

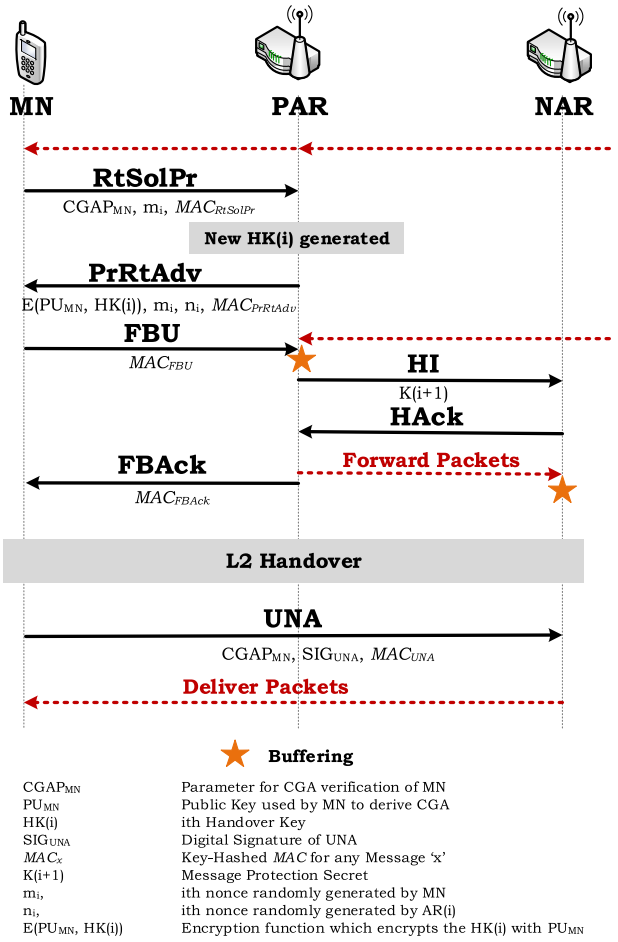

FIGURE 7. SEND-based Secure FMIPv6 Scheme [164], [175].

messages between MN and ARs. As shown in Figure 7, the PAR is responsible for the *handover key* generation, which is then communicated to the MN through PrRtAdv message. A *message protection secret, K(i)* is also derived from the *handover key*, which is then used by both MN and PAR for generating *HMAC* (Keyed-Hashed *MAC*, e.g. $MAC_{RtSolPr}$ in Figure 7) values. *HMAC* is a type of *MAC* which is generated through a hash function and a cryptographic key, which in this case is $K(i)$. Each involved entity i.e. MN, PAR and NAR on receiving a signaling message, first verifies the *HMAC* value before performing its public key operation.

The concept of *handover key* is used in other proposals as well, which are discussed next. For each of these solutions, the management of the *handover key* is of vital importance. In general, the MN moving across domains is required to obtain a new *handover key* for each visited domain. This is to ensure that even if the *handover key* is compromised in one domain, it is not used for any attacks as the MN moves into another domain. Moreover, the *freshness* of the *handover key* is also important to ensure that threats such as replay attacks can be prevented.

TABLE 2. Summary of key features of *security-specific* enhancements for FMIPv6.

Proposed Solution	Major Approach for Security	Target Security Threats	Security Services Provisioned	Security Infrastructure Consideration	Potential Drawbacks	FMIPv6 Messages Protection						Deployment Considerations
						RtSolPr	PrRtAdv	FBU	FBAck	HI	HAck	UNA	
[163]	CGA	Redirection, Replay, DoS	Integrity, Signalling Authentication	Infrastructure-less	Secures FBU message only	×	×	✓	×	×	×	×	Standard-oriented. Based on FMIPv6 signalling
[164]	Digital Signature, Hashed MAC, CGA	Redirection, DoS, Replay	Integrity, Signalling authentication	Infrastructure-based	Higher computational costs	✓	✓	✓	✓	×	×	✓	Based on AAA Infrastructure
[165]	Group key, MAC	Redirection, DoS, Replay	Signalling authentication	Partially Infrastructure-based	Prone to flooding, replay, DoS, Man-in-the-Middle attacks [166]	✓	✓	✓	✓	✓	✓	✓	Based on AAA Infrastructure
[167]	Light-weight approach of OWHC	DoS, Flooding, Replay, Session Hijacking	Signalling Authentication	Infrastructure-less	Handover key highly vulnerable to exposure. DoS, Redirection attacks [168]	×	×	✓	✓	×	×	×	Based on FMIPv6 signalling
[169]	HO Master key	Threats based on unprotected FBU	Integrity, Signalling authentication, Confidentiality	Infrastructure-based	High computation overhead. Protection for FBU only	×	×	✓	×	×	×	×	Based on *Handover Key Server*
[170]	Integrated L2/L3 Authentication, HO Master key	Threats based on unprotected FBU	Integrity, Signalling authentication, Confidentiality	Infrastructure-based	High computation overhead. Protection for FBU only	×	×	✓	×	×	×	✓	Based on AAA Infrastructure
[171]	Integrated L2/L3 Authentication	Replay, Redirection, Man-in-the-Middle	Integrity, Signalling Authentication, Confidentiality	Partially Infrastructure-based	High computation overhead	✓	✓	✓	✓	✓	×	✓	Based on AAA Infrastructure

2) GROUP KEY BASED ENHANCEMENTS

A group key management scheme in [165] relies on a *Group Key (GK)* which is distributed among all protocol entities involved in the handover protocol operation. An MN, when enters into a new domain, obtains an *Authentication Ticket* ($Ticket_{MN}$) after it successfully registers in the domain. The MN can derive a session key *sK* as well as the *GK* from it. Here, *sK* is used for securing both the fast handover as well

as the BU signaling. So, at router discovery, the MN includes the $Ticket_{MN}$ and $MAC(sK)$ in the RtSolPr message to PAR. The PAR verifies the $MAC(sK)$ since the GK has already been shared with it. Other FMIPv6 signaling messages also carry the $MAC(sK)$ which is verified at the receiving node.

This scheme, however, has several shortcomings as identified in [166]. These include: (i) Each AR with the *GK* can retrieve and even manipulate messages between any other communicating nodes in its domain. (ii) The scheme does not ensure that the MN is actually present at its currently claimed CoA. The *Mobile Node Flooding* attack is thus possible in this case. (iv). Since there is no concept of *freshness* in case of RtSolPr and PrRtAdv messages, these can be replayed to launch *Replay* or *DoS* attacks.

3) ONE-WAY HASH CHAIN-BASED ENHANCEMENT

The aforementioned security solutions for FMIPv6 incur higher computational costs. Thus, a light-weight security solution based on *one-way hash chain (OWHC)* technique is proposed in [167]. The OWHC technique aims to authenticate the FMIPv6 signaling messages. In this method, the *handover key(s)* can be generated by the OWHC values, one at a time for each handover, instead of generating them through public keys. The one-way hash chain (V_0, ..., V_n), in this scheme, is a set of values such that each value is a one-way function for the next value. i.e. $V_i = H(V_i + 1)$. Before triggering the very first handoff, the MN generates the OWHC (e.g., 20 values, with a length of 128 bits each).

However, this scheme also has some drawbacks as highlighted in [168]. These include: (i). The protocol only proposes protection for the FBU and FBAck messages, and does not protect the RtSolPr, PrRtAdv, and UNA messages. (ii). The Access Routers (ARs) can easily compute the next handover key by *XOR*ing the current *handover key* with the respective *Handover Vector (HV)*. Therefore, it is highly likely that the next *handover keys* can be computed by an eavesdropper. (iii). The proposed scheme is still vulnerable to *DoS* attacks as it uses *SEND* protocol only during the first handover.

4) HANDOVER MASTER KEY BASED ENHANCEMENTS

In order to provide an enhanced set of security services during handovers, the concept of *Handover Master Key (HMK)* is introduced in [169]. The proposed scheme assumes that an *HMK* is pre-shared between the MN and a *Handover Key Server*, through which the *handover key* is derived. The *Handover Integrity Key (HIK)* is also derived from the *HMK*, which provides the integrity protection to the messages which are exchanged by the MN and the *Handover Key Server*. The *handover key* is used by the MN to secure the FBU message sent to the PAR. However, other than the FBU message, this scheme does not address the protection of any other FMIPv6 signaling message.

A similar solution is proposed in [170], in which an *Extended Handover Master Session Key (EMSK)* is established between the MN and the AAA server, after the initial authentication of MN in the new domain. The proposed solution aims at providing an integrated link-layer and network layer authentication solution. Similar to [169], several keys such as *Authentication Master Key (AMK)*, *Encryption Master Key (EMK)* can be derived from the *EMSK* at the network layer, while the *Integrity Key (IK)* and *Encryption Key (EK)* are derived from the *Session Master Key (SMK)* at the link-layer. The *SMK* itself had been earlier derived from the *handover key*. With *IK* and *EK* shared between the MN and AP, the AP only processes authenticated packets which it receives from the MN. However, this process is also based on assumptions such as that the *EMSK* is shared between MN and the AAA server, and that the *handover key* is shared between the MN and PAR.

Although, the solution provides an integrated L2 and L3 authentication to reduce the overhead of the authentication process at two layers, from the FMIPv6 signaling protection view, this solution also focuses on securing the FBU message only.

5) A CROSS-LAYER KEY MANAGEMENT-BASED ENHANCEMENTS

Since a MN first establishes communication at the link-layer (e.g. to an AP in the IEEE 802.11 domain), it would require a key at L2 for secure link-layer communications. Similar to [170], another cross-layer based key management scheme is proposed in [171], in which the L2 key is derived from a L3 key in an IEEE 802.11 network. In the proposed scheme, the *handover key*, which the MN would require at the NAR's subnet, is generated and shared proactively with NAR, while the MN is still connected to the PAR's link. The new *handover key* is shared with NAR through HI message. The MN also uses this key to derive the L2 key for establishing the security association with new AP at NAR's subnet.

The proposed scheme promises the protection of RtSolPr/PrRtAdv, FBU/FBAck as well as HI message through the previous/current *handover key*, while the UNA message is protected through the new *handover key*. The HAck message is however left unprotected. This scheme, thus, not only provides a secure FMIPv6 signaling and promises the MN's authentication at the new network, it also reduces the overhead associated with the L2 handover authentication process. However, this scheme is applicable only for FMIPv6 over IEEE 802.11 networks, and for any other access technology such as IEEE 802.16e, the respective L2 security procedures would need to be considered to devise a similar solution.

VI. ACCESS TECHNOLOGY-SPECIFIC ENHANCEMENTS

The FMIPv6 considers the link-layer handover within its protocol operation. Thus its handover performance varies with different underlying access technologies.

The proposals for FMIPv6 deployment in different access networks have been introduced. The IETF has provided primary specifications for FMIPv6 over IEEE 802.11 [28], CDMA2000 [176] and IEEE 802.16e [29] networks.

Numerous optimized solutions discussed in the previous sections can also be applied to these specifications; however, they also bring out certain challenges at their own as well. The FMIPv6 over IEEE 802.11 and IEEE 802.16e have been thoroughly explored by the research community, and various solutions have been put forward. The FMIPv6 over CDMA2000 [176] has also not received much attention from the research community, since no future technologies are planned to be based on it. Therefore, discussion on this protocol is omitted in this paper.

A. FMIPv6 OVER IEEE 802.11

The IETF specification for FMIPv6 over IEEE 802.11 considers the standard handover procedures of IEEE 802.11 such as scanning, authentication and association within the FMIPv6 operation. In predictive mode, the MN[7] performs scanning to find the available APs. It then exchanges RtSolPr/PrRtAdv messages with PAR to obtain AR(s) information about the scanned AP(s). The MN then sends the FBU message to PAR which exchanges HI/HAck messages and establishes a tunnel with NAR. It then sends the FBAck message to MN. At this point, the MN starts the L2 handover. The MN selects an AP and performs the *Join* process with it. It also sends *Authentication* as well as *Association* or *Re-association* requests to the new AP. The MN and AP also carry out the *802.1X EAP (Extensible Authentication Protocol)* [178] procedures for authenticating the association among them. After the successful completion of the L2 handover, the MN sends the FNA message to NAR.

The IETF specification for FMIPv6 over IEEE 802.11 networks have similar drawbacks in different scenarios as the standard FMIPv6 which include high handoff latency, packet losses etc. The research community has provided various proposals addressing these challenges. Majority of these optimizations primarily improve the standard IEEE 802.11 L2 handover operation. A special focus has been on reducing the scanning interval, as according to [94], it is the major cause of packet losses during the IEEE 802.11 handoffs. In addition, the IEEE 802.11 *Probing* and *Authentication* processes are also focused in some solutions. Certain cross-layer based solutions which integrate the L3 FMIPv6 handover process with L2 IEEE 802.11 handover process have also been proposed.

1) OPTIMIZING SCANNING DELAY

Various optimizations in IEEE 802.11 L2 handover operation use *selective*, *intermittent*, or *pre-scanning* approaches to optimize the FMIPv6 over IEEE 802.11. Some techniques, on the other hand, completely eliminate the scanning phase in the IEEE 802.11 link-layer handover operation.

A *pre-scanning* approach is proposed in [43] in which the MN starts scanning process beforehand as its current RSSI falls below a pre-adjusted *Roaming Threshold*. The MN would not thus require the scanning process again during the L2 handover. The *pre-scanning* approach may prove to be impractical in real scenarios since it is prone to omit a candidate AP due to rapidly varying mobility patterns. Therefore, instead of *pre-scanning*, a desirable approach is to focus on a solution which can promise the reduced scanning interval during handover.

An *iterative* scanning approach is proposed in [179], which, unlike the pre-scanning approach, carries out scanning during the actual handoff execution. The proposed scheme relies on an *iterative on-off* channel scanning, in which the channel discovery process is divided between channel scanning and data transmission periods. The proposed scheme not only utilizes the scan period for data transmission thereby reducing the overall disruption time, but also allows more accurate AP selection by effectuating the scanning process at the most appropriate time i.e. *during* the handoff.

Similarly, a *selective* scanning approach is proposed in [180] which uses *neighbor graphs* to identify and selectively scan the nearby APs of an MN. This approach also effectively reduces the scanning delay associated with the link-layer handoff.

Some schemes aim to completely eliminate the scanning process during the IEEE 802.11 handover. The concept of *shared* beacon is introduced in [181], in which the APs advertise the beacon on a dedicated standalone channel, while the MN can select a suitable AP based on the RSSI from each AP. The MN can keep an updated list of candidate APs by listening to the shared beacon channel, while still keeping the data exchange alive. Then, at the time of handoff, it selects one of them according to its handoff policy (which might include the RSSI), and initiates handoff with the selected AP by sending the *Authentication Request* frame to it right away. In this way, the scanning phase during handoffs is completely eliminated. Another scheme named *D-Scan (Scan in AP-Dense 802.11 networks)* in [182] argues that in an AP dense environment, it is very likely for an MN to obtain information about the neighboring APs through *eavesdropping* wireless traffic. The MN can capture certain management frames or data packets sent by APs, which might contain useful information of the MN's interest such as AP's MAC, SSID, and RSSI. Similarly in [183], the MN obtains the information about the neighboring channel conditions through a *Neighbor Access Channel Statement (NACS)* from a closely located MN. In this way, the scanning delay during the L2 handoff is completely eliminated.

2) OPTIMIZING PROBING DELAY

The MN probes the selected AP during scanning by exchanging the *Probe Request/Response* messages with it. A *Handoff with Null Dwell time (HaND)* scheme is proposed in [184] to optimize the probing delay. The proposed scheme uses the *zero-channel-dwell-time* approach, in which the MN, after sending the *Probe Request* frame to the APs on the new channel, immediately switches back to the current channel to resume its on-going session with the current AP.

[7] In IEEE 802.11 standard specifications, e.g. IEEE 802.11r [177], a MN is termed as mobile station (or mobile STA). In this paper, the term MN is used for the sake of consistency.

The *Probe Response* frames from each of those APs are sent to the currently serving AP of the MN, instead of directing them towards the MN on the same channel over which the *Probe Request* frame was received. In this way, the MN can obtain information about the neighboring APs without actually spending time on any channel other than its currently active channel for data transmission.

The *NACS* approach [183] discussed in the previous section also effectively reduces the probing delay. Other examples of optimizations associated to the probe delay include [185] and [186].

3) OPTIMIZING (RE-)AUTHENTICATION DELAY

The IEEE 802.11 *Authentication* or *re-Authentication* delay is another significant delay factor during IEEE 802.11 handover process. A dual-authentication scheme is proposed in [187] which consists of *Immediate Authentication* and *Full Authentication* phases. During the *Immediate Authentication*, the new AP allows MN to associate with it if it is able to provide some evidence of its association to an old AP. Since, this is a temporary authentication, the MN is allowed to access the network temporarily, and has to carry out *Full Authentication* i.e. IEEE 802.1X within the supposed time constraint. This scheme not only reduces the authentication delay significantly at handoff, but also does not risk sharing any security contexts to AP (as is done by certain inter-AP protocols that use the pre-authentication approaches). In [188], it is suggested that, at the time of handoff, instead of sending the *Probe Request* to all APs, the MN sends the *Authentication Request* to only the selected candidate APs. The current IEEE 802.11 specifications support authentication with multiple APs, so this step does not violate any standard procedures. In response, the MN receives the *Authentication Response* frame, and selects the final target AR based on the RSSI of the corresponding *Authentication Responses* it receives.

4) CROSS-LAYER BASED SOLUTIONS

Several IEEE 802.11 and FMIPv6 handover procedures can be combined together as cross-layer solutions to optimize the overall handover delay. The broadcast of the *Router Advertisement (RA)* message through the L2 beacon frames is proposed in [189]. According to this proposal, the AP associated to an AR receives the *RA* and stores it. Instead of waiting for the standard *Routing Advertisement Interval* to receive an RA, the MN can receive it 80% faster through the beacon frame, thus efficiently reducing the movement detection or network discovery time.

Similarly, in [190], the PrRtAdv message is extended by several ICMPv6 options containing various L2 connection parameters to be sent to the MN. In this way, it would not need to discover them through scanning. In [191], the proposed *Cell Information Exchange Protocol (CIEP)*, obtains the L2 and L3 information of the target network in one protocol suite. The *CIEP* essentially aims to replace the IEEE 802.11 *Inter Access Point Protocol (IAPP)* [192] and *CARD* [105] protocols, which are used for L2 and L3 information exchange between the subnets respectively.

B. FMIPv6 OVER IEEE 802.16e

Compared to the handover process in IEEE 802.11, the IEEE 802.16e handover mechanism [193] consists of some additional handover subprocesses since it also involves parameter adjustments. Like FMIPv6, the IEEE 802.16e standard also supports the coordination with the target network, and receiving information about it before the actual handoff. It supports *initial ranging* and *association* with the target BS during scanning and before selecting the target BS, due to which the service disruption and data losses can be reduced.

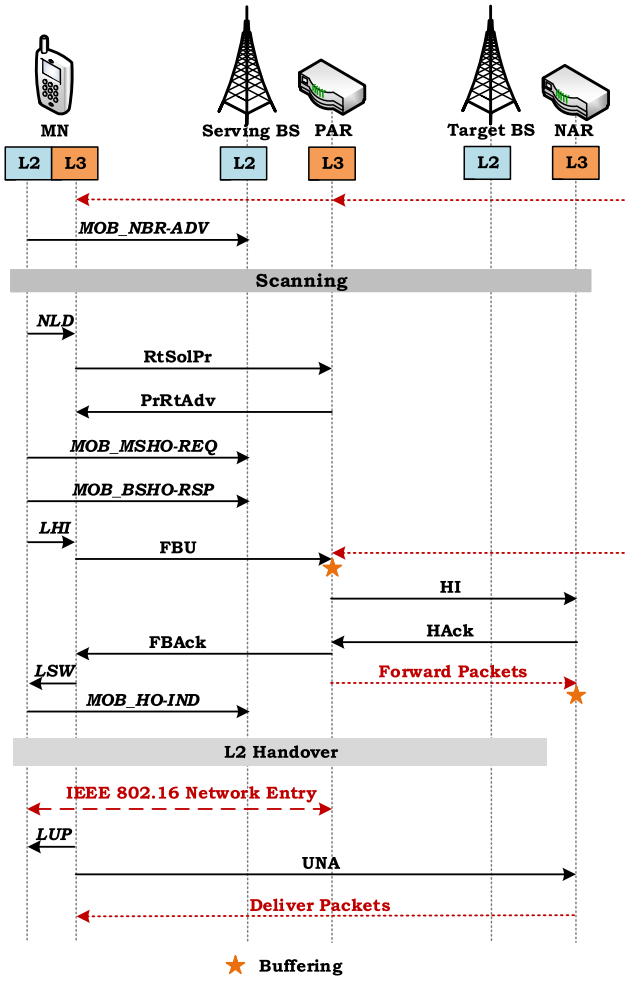

FIGURE 8. Signaling Sequence for FMIPv6 over IEEE 802.16e [29].

In the IETF specified FMIPv6 operation over IEEE 802.16e networks [29], a number of new primitives are introduced which include *NEW_LINK_DETECTED (NLD)*, *LINK_HANDOVER_IMPEND (LHI)*, *LINK_SWITCH (LSW)* and *LINK_UP (LUP)*. In the predictive mode of FMIPv6 over IEEE 802.16e, which is shown in Figure 8, the BS periodically broadcasts the *MOB_NBR-ADV* message which provides channel information of its neighboring BSs. The MN[8] can also search for neighboring BSs through scanning.

[8]In the IEEE 802.16e standard specification [194], the term mobile station is used. In this paper, we use the term MN for the sake of consistency.

The *MOB_NBR-ADV* message provides static information while more dynamic parameters can be obtained through scanning. During scanning, the MN may try to establish *association* with neighboring BSs to establish basic relationships such as *ranging* with them.

The MN has to relate the new BSs' BSIDs to their associated ARs by exchanging the RtSolPr/PrRtAdv messages with PAR. The handover process is initiated by MN by sending the *MOB_MSHO-REQ* message to the current BS, which responds with *MOB_BSHO-RSP* message. Alternatively, this process can also be initiated by the BS by sending the *MOB_BSHO-REQ* message to the MN.

As soon as the target BS is selected and the link-layer of MN knows that the L2 handover is imminent, it informs the network layer about it through *LHI* primitive. The network layer checks if the target BS belongs to a different subnet. If so, it sends an FBU message to the PAR, which then establishes a bidirectional tunnel with the NAR and sends the FBAck to the MN.

After receiving the FBAck, the MN is ready to start the L2 handover. The L3 of MN may issue a *LSW* command to L2 for this purpose, which in turn sends the *MOB_HO-IND* message to current BS indicating the imminent handover. The MN switches link to the target BS, and after synchronization, it completes the IEEE 802.16e *network (re-)entry* procedures. During the L2 handover phase, the *RNG-REQ/RSP* messages, among certain other messages, are exchanged between the MN and the target BS to perform *ranging* in order to obtain PHY channel information. As the L2 handover completes, the link-layer indicates this to the IP layer by the *LUP* primitive. The L3 then sends the UNA message to NAR, which in turn starts delivering buffered packets to the MN.

The mobility management in IEEE 802.16e also faces numerous challenges [195]. These are reflected in FMIPv6 over IEEE 802.16e performance as well, which like other FMIPv6 solutions by the IETF, is also not suitable enough for the real-time network applications [196]. Several optimizations specific to FMIPv6 in the WiMAX environment have thus been proposed. The cross-layer optimizations have been a popular approach. Also, since the proposed specification is based on primitives similar to the primitives in the IEEE 802.21 standard [26], several enhancements based on IEEE 802.21 have also been proposed. These enhancements have thus been organized into two subcategories as follows.

1) CROSS LAYER-BASED OPTIMIZATIONS

The integration and/or synchronization of FMIPv6 and IEEE 802.16e signaling messages has been done in various optimizations. Some schemes also define new messages for supporting their respective proposals.

In [197], the *MOB_NBR-ADV* message and the PrRtAdv message are integrated as *Pr-MOB_NBR-ADV* message which can simultaneously convey the information of the neighboring BSs as well as their corresponding ARs. On the other hand, the *RNG-REQ* message, which implies that the MN has moved into a new network, is integrated with FNA message which also has a similar functionality. This results in an integrated *FNA-RNG-REQ* message. Similarly, in [198], the *MOB_HO-IND* message is combined with FBU while the FNA is merged with *RNG-REQ* message. In addition, during the initial neighbor discovery process, the *MOB_NBR-ADV* and PrRtAdv messages are also integrated. In [199], the RtSolPr and PrRtAdv messages are omitted to be replaced by the *MOB_NBR-ADV* message, while the FNA is also omitted as the target BS sends the *HO-COMPLETE* message to the NAR.

In [200], three new messages are defined which are communicated from BSs to ARs to provide them various handover updates that they receive from the MNs. These are: *HO-NOTIF, HO-CONFIRM* and *HO-COMPLETE*. The usage of these messages eliminates the need of standard FMIPv6 messages such as RtSolPr, PrRtAdv, FBU, FBAck and FNA. When the BS receives *MOB_MSHO-REQ* message, it sends the *HO-NOTIF* message to PAR, to inform it about the impending L3 handover. As the MN finalizes the target BS, it sends the *MOB_HO-IND* message to its current BS, which in turn sends the *HO-CONFIRM* message to the PAR. The MN then starts the L2 handover, and as it completes the L2 handover procedures, the target BS sends the *HO-COMPLETE* message to the NAR. This also eliminates the need to send the UNA message.

Other examples that inter-operate FMIPv6 and IEEE 802.16e signaling include [201]–[204].

2) IEEE 802.21-BASED OPTIMIZATIONS

Due to similarities between the primitives defined by the FMIPv6 over IEEE 802.16e specification and the IEEE 802.21 MIH framework, both standards have been proposed to interoperate in several optimizations for FMIPv6 over IEEE 802.16e. An integrated protocol in [205], which incorporates FMIPv6, IEEE 802.16e, SIP and IEEE 802.21 has been designed. According to this scheme, as soon as the MN's L2 receives the *MOB_BSHO-RSP* or *MOB_BSHO-REQ* messages, its L2 sends the *MIH_Link_Going_Down (LGD)* trigger to the SIP application which in turn sends a *SIP RE-INVITE* message to the CN with nCoA before the link disconnection.

In [206], the MIH Information Server is assumed to be collocated with the ARs. In this proposal, as soon as the MN detects the neighboring BSs, it receives more information about them from the Information Server by exchanging the *MIH_Get_Information_Request/Response* messages. Next, the FBU is sent to PAR as the MAC layer generates the *Link_Going_Down* trigger. The MN informs PAR about the handover execution through *MIH_Link_Down* event. The PAR at this point starts forwarding the buffered packets towards NAR. The MN, on the other hand, after successful completion of the IEEE 802.16e *network re-entry* procedures, sends *MIH_Link_Up* indication to the NAR.

Similar solutions in [207] and [208] also utilize the IEEE 802.21 procedures to improve the fast handovers performance in IEEE 802.16e networks.

VII. PROSPECTS OF FMIPv6 IN 5G

In the previous sections, we have presented a comprehensive review of the enhancements to the FMIPv6 protocol. Based on these enhancements, in this section, we discuss the evolution prospects of FMIPv6 principles towards 5G. We discuss how an evolved solution based on fast handover principles can address some of the complex mobility management challenges in 5G. The standardization prospects of FMIPv6 framework as well as its deployment aspects in 5G are also discussed. Finally, some pertinent FMIPv6 limitations which would require further investigations in the context of 5G are also indicated.

A. 5G MOBILITY ENVIRONMENT AND FMIPv6 PROSPECTS

In this section, an overview of the mobility management requirements in 5G is first presented. Next, the prospects of FMIPv6 to meet these requirements are correspondingly discussed.

1) AN OVERVIEW OF MOBILITY MANAGEMENT REQUIREMENTS IN 5G

The 5G networks are envisioned to deliver revolutionary applications, services and use cases. The existing IP-based networks require significant architectural changes in order to evolve towards 5G. Unlike the centralized control and management of the existing networks, 5G requires decentralized network architectures in order to cope with the unprecedented traffic growth [209]. On the other hand, deployment of smaller cells is envisioned to increase the network capacity and effective spectrum utilization [210]. Moreover, in order to effectively support different use cases with often conflicting requirements, technologies such as software-defined networking (SDN) and network function virtualization (NFV) are seen as key building blocks in 5G networks [211].

The aforementioned architectural changes also require evolution of the existing network protocols for effective control and management in 5G systems. In particular, the protocols for mobility management in 5G are required to ensure stringent performance guarantees. The existing MIPv6-based protocols with their centralized architecture impose several bottlenecks to the mobility management process. These bottlenecks become more evident under the heavy traffic load conditions at the centralized node (e.g. HA in MIPv6 or Local Mobility Anchor (LMA) in PMIPv6).

The IETF has acknowledged such drawbacks and has already specified a preliminary decentralized mobility management framework termed as distributed mobility management (DMM) [1]. In DMM, the handover and the traffic management is performed at the first-hop access routers without any reliance on a centralized network node. The IETF has also specified certain requirements for DMM [6], the key among which include the need to evolve these solutions towards decentralization from the existing IPv6 mobility principles [6]. The IETF also requires these solutions to support services such as multicast mobility and security assurance [6].

The standardization process for DMM at IETF is still at very early stages. The current DMM solutions are mainly based on the network-based PMIPv6 protocol. However, several performance studies have shown considerable limitations in their performance [3]–[5]. These studies have shown that the current DMM solutions incur high handover latencies as well as signaling costs, as the MN undergoes frequent handovers with multiple or long-lasting sessions. Moreover, these solution have not been sufficiently explored to support services such as multicast mobility and secure handovers as specified by the IETF's requirements [6].

Nonetheless, the current trends of network softwarization and virtualization of 5G systems also introduce some additional challenges to the mobility management process. To ensure backward compatibility of the virtualized domains with the existing infrastructure, the mobility management protocols would require further evolution in accordance with SDN and NFV. Accordingly, the continuation of IPv6 mobility principles is seen as a key approach for such development as well [212].

Another key aspect in which the current mobility management mechanisms including DMM lag, is the lack of adaptable mobility support which is suitable for specific mobility profile or services of a mobile user. The DMM process, following the traditional mobility management protocols, generally provides the same mobility management support to all MNs regardless of their movement pattern or ongoing application requirements [213]. As noted earlier, due to diversity in emerging applications, services and use cases, providing same mobility support would be highly inefficient. Therefore, flexible mobility management mechanisms, which can change their execution principles according to MN's mobility and application requirements, are desired for the 5G networks [213].

The network virtualization and softwarization also introduce new security challenges to the mobility management process. For example, virtualization of Radio Access Network (RAN) simplifies the radio nodes such as Base Stations into Remote Radio Headers (RRHs) [214]. The RRHs are decoupled from the Baseband Unit (BBU) where the actual signal processing takes place. The BBUs in the virtualized RAN function as a separate entity, and are deployed usually in a remote data center or cloud [214]. This allows adversaries to deploy a malicious RRH into the network conveniently which may not only affect the 5G system security, but also the MN's communication session (e.g. through its false claims of being a legitimate RRH) [215].

In summary, the mobility management protocols for 5G would essentially need to be (a) decentralized (b) IPv6-based, (c) robust, (d) virtualizable, (e) flexible, (f) secure.

2) PROSPECTS OF FMIPv6 IN 5G MOBILITY ENVIRONMENT

The FMIPv6 principles and their enhancements discussed in the previous sections can potentially provide a suitable *scaffolding* for designing protocols to handle mobility in 5G networks. The FMIPv6-based solutions, as discussed below, have the potential to meet some of the complex mobility management requirements in a 5G environment. The key prospects of FMIPv6 in 5G can be summarized in the following points:

- **Decentralized:** The FMIPv6 protocol supports traffic resumption through forwarding traffic from previous network to the new network through a bidirectional tunnel. Effectively, the protocol does not need reliance on any centralized network node for traffic resumption as a result of handover. Thus, it can naturally evolve towards a decentralized mobility solution. The benefits of decentralization through the FMIPv6 principles can be maximized by several enhanced route optimization mechanisms as discussed in Section II-G. Such solutions can potentially counter the high latencies and tunneling costs [5] if the MN undergoes several handovers with long-lasting sessions.
- **IPv6-based:** Since FMIPv6 is based on the IPv6 principles, it can inherently support smooth evolution towards IPv6-based decentralization of the mobility management process. Thus, smooth mobility management could be supported in the subsequent IPv6-based hybrid centralized/distributed domains, which are expected to coexist in the real-world scenarios [3]. Similarly, preserving the IPv6 principles would also ensure further evolution towards softwarized domains [216]. This would also allow smooth mobility management in the ensuing hybrid SDN domains wherein SDN-based and non-SDN based domains would coexist [217], [218].
- **Robust:** Several FMIPv6 enhancements have shown that it can be easily enhanced to provide a unified solution which can support advanced mobility features such as vertical handovers, multicast mobility, QoS, and security. Thus, by providing a unified protocol framework, it can offer a robust mobility management solution which is highly desirable for a 5G mobility environment. Such an approach avoids the need to rely on additional protocols which not only result in computational overheads, but may also cause higher latencies during the time-critical handover event.
- **Secure:** Security in 5G is considered to be of paramount importance, with several new threats being identified [215], [219]–[221]. Several enhancements to the FMIPv6 protocol have shown that the basic handover security can be provided within its operational framework. The enhanced FMIPv6 framework can also provide the main security services such as confidentiality, signaling integrity as well as authentication, usually without relying on existing security infrastructure or additional security protocols. Thus, several security enhancements to FMIPv6 open avenues to effectively address some of the complex security challenges in a 5G mobile environment [215].
- **Virtualizable:** The FMIPv6 protocol framework comprises of an elaborate set of handover subprocesses. These subprocesses can be decoupled from each other and act as independent functions, which can be subsequently controlled through the control plane entities e.g. an SDN controller [216]. In fact, the feasibility of deploying (and controlling) such handover subprocesses at SDN controller as "*stand-alone modules*" has already been discussed in [212].
  Therefore, in a virtualized 5G environment, several FMIPv6 subprocesses such as movement detection, handover preparation, handover mode selection, handover triggering, nCoA formulation, duplicate address detection, route optimization, packet forwarding, buffering can be virtualized i.e. controlled and executed by the control plane. Moreover, other mobility support mechanisms such as in-advanced resource reservation at new network, vertical handover decisions, mobile multicast session management etc. can also be implemented as virtual functions.
- **Flexible:** The ability of FMIPv6 protocol to operate proactively, as well as adapting its operation to the reactive mode in case of predictive mode failure, represents an inherent flexibility feature of FMIPv6 – a feature that does not exist in other MIPv6-based protocols. With the evolution towards SDN and NFV in 5G, its operation can be made further flexible by controlling its mutually independent handover subprocesses from the central control entities [212].
  Based on the mobility requirements, the control plane may or may not decide to execute these subprocesses during handover. Furthermore, different versions of such handover subprocesses can also be defined, and the order of their execution may also be varied by the control plane, to best suit the mobility and application requirements of the MN.

B. STANDARDIZATION PROSPECTS

The standardization efforts for mobility management mechanisms in 5G are primarily focused on DMM. Utilizing FMIPv6 for DMM is among the recommendations of the IETF for improved handover performance [222]. However, FMIPv6 principles have not yet been considered in DMM standardization since these efforts are still in infancy.

The effectiveness of using FMIPv6 principles in DMM has also been substantiated by some recent works. It has been shown in [223] and [224] that extending DMM process through FMIPv6-based principles, such as proactive handover initiation, link-layer assistance, in-advanced new IP address formulation, buffering, and bidirectional tunneling, can outperform the popular PMIPv6-based DMM process. The study in [224] shows that fast handovers based DMM can achieve up to 74% reduction in handover latency compared to the PMIPv6-based DMM solution.

C. DEPLOYMENT CONSIDERATIONS

The user devices in 5G, in general, are expected to play a greater role in the 5G ecosystem compared to the previous generations of mobile networks [225]. The inadequacies of network-based DMM solutions motivate the need to explore an increased MN involvement in the mobility management process (e.g. through FMIPv6).

Recent advances in virtualization technologies have not only enabled functions and infrastructure virtualization at the network side, but also at the user's end as well [226]. A relevant virtualization technology is the operating system virtualization wherein several functions and processes are implemented in *containers*. *Containers* are a low-weight virtualization technology, which can function independently from each other. Such an architecture not only provides flexibility to rapidly update certain components in the operating system, but also allows convenient deployment of new services which may include novel control and management mechanisms.

These technologies are also capable of deploying sophisticated mobility management mechanisms aimed at diverse 5G mobility scenarios. Considering the service-oriented 5G architecture offering diverse services, the operational adjustments to FMIPv6 can also be conveniently made to best suit the requirements of a particular service. For example, a multicast-enhanced version of FMIPv6 can be used for managing an ongoing multicast session. Otherwise, only the baseline FMIPv6 operation would suffice. Likewise, in a heterogeneous environment, the enhanced FMIPv6 version with vertical handover support can be executed. Another example can be of a delay-sensitive or tactile application, for which a multi-homed version of FMIPv6 can be utilized. In case of a high mobility scenario, a simplified version of baseline FMIPv6 can be used e.g. [54].

Note that such an approach may not necessarily require multiple FMIPv6 deployments in a single user equipment. Instead an enhanced, flexible FMIPv6 solution can intelligently evaluate the requirements of a particular service and execute the necessary mobility management feature from within a unified framework.

D. POTENTIAL LIMITATIONS

Despite its invigorating prospects towards 5G, FMIPv6 principles still have some limitations which would become more pronounced in the context of 5G. Following are some key limitations which require considerable efforts to realize their full potential for the 5G mobility environment. Some possible approaches which can be explored further to address these limitations are also highlighted.

- **MN Involvement in handover operation:** Although involving MN in handover operation helps in intelligent handover management, an excessive dependence on MN would incur high power and computational overheads for battery constraint MNs. Moreover, as discussed in the Section VII-A1, such a mechanism would be vulnerable to more security threats.

  Therefore, it is important to explore mechanisms which could balance the trade-off between MN's participation in handover and the mobility-related intelligence acquired from it. In this regard, some example approaches include delegating certain handover operations to network nodes which are performed by the MN, such as BU, RO, RR and nCoA formulation as discussed in Sections II-C and II-G. Moreover, the FMIPv6 signaling which requires the MN's involvement such as RtSolPr, PrRtAdv, FBU, FBAck and UNA can interwork with access-technology specific messages, as discussed in Section VI.
- **Precision of Handover Prediction:** Among all components of the FMIPv6 framework, precision of handover prediction plays a pivotal role. However, devising an accurate in-advance handover prediction mechanism still requires considerable research efforts. This is especially critical in scenarios where the MN undergoes handovers frequently.

  In this regard, intelligent mechanisms can be designed by applying Machine Learning techniques. These techniques are nowadays being increasingly adopted for management, maintenance and optimization of networks [227]. Intelligent handover prediction algorithms can be developed through such techniques, not only at the MN but also at the network side.
- **Signaling Costs:** The FMIPv6 operation, although provides significant gains in terms of handover latency and packet loss reductions, incurs higher signaling costs [12]–[18]. The study combining FMIPv6 principles with DMM has also shown that although this approach significantly reduces the latency, it incurs higher signaling costs compared to the existing solution [224]. Assuming a prospective unified FMIPv6 framework in 5G, which would integrate QoS, VHO, mobile multicast and security within a single protocol framework, the signaling overheads would significantly increase.

  A number of different approaches can be pursued to address this challenge. These include (a) using lightweight signaling i.e. carrying fewer options in a FMIPv6 message, (b) integrating several FMIPv6 messages together e.g. [54], (c) integrating L2 and L3 messages through cross-layer mechanisms as discussed in Section VI-B1.
- **Emerging Security Challenges:** The emerging security challenges, with the advent of network virtualization, impose complex security requirements. These requirements in turn demand robust security solutions, which would most likely incur high computational costs and high resource consumptions.

  A potential approach to such challenges is to define several security levels for users with different service requirements (e.g. based on [228]). Again, this would require flexible design considerations for the mobility management protocol as discussed in Section VII-A1.

VIII. CONCLUSIONS

The FMIPv6 protocol in its primary or hybrid forms, like FPMIPv6, has been shown to have the most optimal handover performance among all MIPv6-based solutions. However, the baseline FMIPv6 protocol still experiences certain performance bottlenecks, which can be addressed by enhancing its protocol operation. A comprehensive study of the FMIPv6 protocol's operational features, their shortcomings, and the enhancements proposed to overcome them, is provided in this paper. A holistic approach is adopted in this study to bring together all such solutions under different categories based on their functional characteristics. These enhancements show that FMIPv6 principles can evolve towards robust mobility solutions, which may include advanced mobility features such as multicast mobility, vertical handovers, QoS-supported and secure handovers.

The IPv6-based mobility solutions, aimed at 5G networks are currently evolving towards the decentralized mobility protocols. Based on the requirements defined by the IETF, the decentralized mobility management solutions are expected to provide robust mobility standards for 5G. Several concepts introduced in the FMIPv6 enhancements open avenues to achieve such advanced mobility solutions. Consequently, the FMIPv6 protocol, with its unique operational features, and capitalizing on virtualization technologies, can potentially address some of the very complex mobility management challenges in 5G.

REFERENCES

[1] C. Bernardos, A. D. L. Oliva, F. Giust, J. Zuniga, and A. Mourad, *Proxy Mobile IPv6 Extensions for Distributed Mobility Management*, document Internet Draft draft-ietf-dmm-pmipv6-dlif-02 (work in progress), IETF, Aug. 2018.

[2] S. Jeon, S. Figueiredo, R. L. Aguiar, and H. Choo, "Distributed mobility management for the future mobile networks: A comprehensive analysis of key design options," *IEEE Access*, vol. 5, pp. 11423–11436, 2017.

[3] J. Carmona-Murillo, V. Friderikos, and J. González-Sánchez, "A hybrid DMM solution and trade-off analysis for future wireless networks," *Comput. Netw.*, vol. 133, pp. 17–32, Mar. 2018.

[4] J. Carmona-Murillo, I. Soto, F. J. Rodríguez-Pérez, D. Cortés-Polo, and J. L. González-Sánchez, "Performance evaluation of distributed mobility management protocols: Limitations and solutions for future mobile networks," *Mobile Inf. Syst.*, vol. 2017, Feb. 2017, Art. no. 2568983.

[5] L. Yi, H. Zhou, D. Huang, and H. Zhang, "An analytical study of distributed mobility management schemes with a flow duration based model," *J. Netw. Comput. Appl.*, vol. 41, pp. 351–357, May 2014.

[6] H. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen, *Requirements for Distributed Mobility Management*, document RFC 7333, IETF, Aug. 2014.

[7] C. Perkins, D. Johnson, and J. Arkko, *Mobility support in IPv6*, docuemtn RFC 6275, IETF, Jul. 2011.

[8] R. Koodli, *Mobile IPv6 Fast Handovers*, document RFC 5568, IETF, Jul. 2009.

[9] H. Soliman, C. Castelluccia, K. Elmalki, and L. Bellier, *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management*, document RFC 5380, IETF, Oct. 2008.

[10] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile IPv6*, document RFC 5213, IETF, Aug. 2008.

[11] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, *Fast Handovers for Proxy Mobile IPv6*, document RFC 5949, IETF, Sep. 2010.

[12] J. H. Lee, J. M. Bonnin, I. You, and T. M. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1077–1088, Mar. 2013.

[13] M.-S. Kim, S. Lee, D. Cypher, and N. Golmie, "Performance analysis of fast handover for proxy mobile IPv6," *Inf. Sci.*, vol. 219, pp. 208–224, Jan. 2013.

[14] S. Haseeb and A. F. Ismail, "Handoff latency analysis of mobile ipv6 protocol variations," *Comput. Commun.*, vol. 30, no. 4, pp. 849–855, 2007.

[15] C. Makaya and S. Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 972–983, Mar. 2008.

[16] K. N. Ashraf, V. Amarsinh, and D. Satish, "Survey and analysis of mobility management protocols for handover in wireless network," in *Proc. IEEE 3rd Int. Adv. Comput. Conf. (IACC)*, Feb. 2013, pp. 413–420.

[17] R. Hsieh, A. Seneviratne, H. Soliman, and K. El-Malki, "Performance analysis on hierarchical mobile IPv6 with fast-handoff over end-to-end TCP," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 3, Nov. 2002, pp. 2488–2492.

[18] X. Pérez-Costa, M. Torrent-Moreno, and H. Hartenstein, "A performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their combination," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 7, no. 4, pp. 5–19, Oct. 2003.

[19] A. Boukerche, A. Magnano, and N. Aljeri, "Mobile IP handover for vehicular networks: Methods, models, and classifications," *ACM Comput. Surv.*, vol. 49, no. 4, pp. 73:1–73:34, Feb. 2017.

[20] H. Modares, A. Moravejosharieh, J. Lloret, and R. B. Salleh, "A survey on proxy mobile IPv6 handover," *IEEE Syst. J.*, vol. 10, no. 1, pp. 208–217, Mar. 2016.

[21] A. J. Jabir, S. Shamala, Z. Zuriati, and N. Hamid, "A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol," *IEEE Syst. J.*, vol. 12, no. 1, pp. 1065–1081, Mar. 2018.

[22] A. Adams, J. Nicholas, and W. Siadak, *Protocol Independent Multicastdense Mode (PIM-DM): Protocol Specification (Revised)*, document RFC 3973, IETF, Jan. 2005.

[23] B. Fenner, M. Handley, I. Kouvelas, and H. Holbrook, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)*, document RFC 4601, IETF, Aug. 2006.

[24] W. C. Fenner, S. E. Deering, and B. Haberman, *Multicast Listener Discovery (MLD) for IPv6*, document RFC 2710, IETF, Oct. 1999.

[25] R. Vida and L. Costa, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*, docuemtn RFC 3810, IETF, Jun. 2004.

[26] *IEEE Standard for Local and Metropolitan Area Networks—Media Independent Handover Services*, IEEE Standard 802.21-2008, IEEE Computer Society, Jan. 2009.

[27] J. Postel, *Transmission Control Protocol*, docuemtn RFC 793, IETF, Sep. 1981.

[28] P. McCann, *Mobile IPv6 Fast Handovers for 802.11 Networks*, document RFC 4260, IETF, Nov. 2005.

[29] H.-J. Jang, Y.-H. Han, J. Cha, S. D. Park, and J. Jee, *Mobile IPv6 Fast Handovers Over IEEE 802.16e Networks*, docuemtn RFC 5270, IETF, Jun. 2008.

[30] S. Thomson, T. Narten, and T. Jinmei, *IPv6 Stateless Address Autoconfiguration*, docuemtn RFC 4862, IETF, Sep. 2007.

[31] J. C. Greg Daley, *Movement Detection Optimization in Mobile IPv6*, document Internet Draft draft-daley-mobileip-movedetect-01.txt (work in progress), IETF, May 2003.

[32] J. Montavont, E. Ivov, and T. Noel, "Analysis of mobile IPv6 handover optimizations and their impact on real-time communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 3244–3249.

[33] A. Papapostolou and H. Chaouchi, "Handoff with energy awareness for future pervasive environments," *J. Supercomput.*, vol. 64, no. 2, pp. 357–382, 2013.

[34] M.-S. Chiang, C.-M. Huang, and D. D. Tuan, "Fast handover control scheme for multi-node using the group-based approach," *IET Netw.*, vol. 4, no. 1, pp. 44–53, 2015.

[35] X. Wang, D. Wang, and S. Qi, "Mobility support for vehicular networks based on vehicle trees," *Comput. Standards Interfaces*, vol. 49, pp. 1–10, Jan. 2017.

[36] L. Dimopoulou, G. Leoleis, and I. O. Venieris, "Fast handover support in a WLAN environment: Challenges and perspectives," *IEEE Netw.*, vol. 19, no. 3, pp. 14–20, May 2005.

[37] Y.-S. Kim, D.-H. Kwon, and Y.-J. Suh, "Seamless handover support over heterogeneous networks using FMIPv6 with definitive L2 triggers," *Wireless Pers. Commun.*, vol. 43, no. 3, pp. 919–932, 2007.

[38] N. P. Singh and B. Singh, "Impact of L2 triggering time on handover performance for 4G wireless networks," *Wireless Pers. Commun.*, vol. 68, no. 3, pp. 727–746, 2013.
[39] M. Tao, F. Liu, and C. Qu, "Predictive timely trigger and performance optimization for deterministic handovers," *Int. J. Wireless Inf. Netw.*, vol. 22, no. 2, pp. 97–104, 2015.
[40] L. Zhang and Y.-C. Tian, "An enhanced fast handover triggering mechanism for Fast Proxy Mobile IPv6," *Wireless Netw.*, vol. 24, no. 2, pp. 513–522, Feb. 2018.
[41] M. Khan and K. Han, "An optimized network selection and handover triggering scheme for heterogeneous self-organized wireless networks," *Math. Problems Eng.*, vol. 2014, Jun. 2014, Art. no. 173068.
[42] M. Tao, H. Yuan, S. Dong, and H. Yu, "Initiative movement prediction assisted adaptive handover trigger scheme in fast MIPv6," *Comput. Commun.*, vol. 35, no. 10, pp. 1272–1282, 2012.
[43] X. Cheng and D. Bi, "Real-time adaptive link layer trigger based cross layer fast handoff mechanism in IEEE 802.11 WLANs," in *Proc. Int. Conf. Commun. Softw. Netw. (ICCSN)*, Feb. 2009, pp. 443–447.
[44] H. Lu, P. Hong, X. Zhou, and L. Liu, "Performance evaluation of link layer triggers for fast handovers in mobile IPv6," in *Proc. 1st Int. Conf. Commun. Netw. China*, Oct. 2006, pp. 1–5.
[45] M. Yang, K. Jung, A. Park, and S.-H. Kim, "Definitive link layer triggers for predictive handover optimization," in *Proc. Veh. Technol. Conf. (VTC Spring)*, May 2008, pp. 2326–2330.
[46] R. Rizk and H. Nashaat, "Smart prediction for seamless mobility in F-HMIPv6 based on location based services," *China Commun.*, vol. 15, no. 4, pp. 192–209, Apr. 2018.
[47] A. E. Bergh and N. Ventura, "PA-FMIP: A mobility prediction assisted fast handover protocol," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2006, pp. 1–7.
[48] M. Tao, H. Yuan, and W. Wei, "Effective performance compensation for the premature handoff trigger in FMIPv6 networks," *Int. J. Wireless Inf. Netw.*, vol. 20, no. 4, pp. 392–400, 2013.
[49] M. Tao, F. Liu, and C. Qu, "Optimizing unsatisfactory handover trigger in heterogeneous vehicular networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 4, p. 33, 2015.
[50] I. Aldmour, L. Siregar, and T. Al Dala'in, and R. Budiarto, "Enhancement of FMIPv6 by utilising concurent binding update process," *Elect. Eng. Comput. Sci. Inform.*, vol. 1, no. 1, pp. 183–185, 2014.
[51] I. Joe and H. Lee, "An efficient inter-domain handover scheme with minimized latency for PMIPv6," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2012, pp. 332–336.
[52] I. Joe and H. Yun, "An improved fast handover algorithm based on the enhanced access router (EAR-FMIPv6)," in *Proc. 4th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM)*, vol. 1, Sep. 2008, pp. 185–188.
[53] Y. Li, W. Chen, D. Jin, and L. Zeng, "Seamless handoff scheme for real-time application in the wireless IPv6 networking," in *Proc. 2nd Int. Conf. Anti-Counterfeiting, Secur. Identificat.*, Aug. 2008, pp. 136–139.
[54] N. Van Hanh, S. Ro, and J. Ryu, "Simplified fast handover in mobile IPv6 networks," *Comput. Commun.*, vol. 31, no. 15, pp. 3594–3603, 2008.
[55] L. J. Zhang, W. K. Chen, and S. Pierre, "Novel seamless mobility protocol for next generation wireless networks," in *Proc. Int. Conf. Artif. Intell. Ind. Eng. (AIIE)*. Phuket, Thailand: Atlantis Press, 2015, pp. 631–634.
[56] H. Oh, K. Yoo, C.-K. Kim, W.-J. Yang, T.-I. Kim, and H.-W. Jung, "An enhanced fast handover scheme with temporal reuse of CoAs and PBP in IPv6-based mobile networks," in *Proc. Int. Conf. Multimedia Ubiquitous Eng. (MUE)*, Apr. 2007, pp. 183–189.
[57] H. Oh, K. Yoo, J. Na, and C.-K. Kim, "A robust seamless handover scheme for the support of multimedia services in heterogeneous emerging wireless networks," *Wireless Pers. Commun.*, vol. 52, no. 3, pp. 593–613, 2010.
[58] C.-S. Shieh, "QoS provisioning in mobile wireless networks with improved handover and service migration," Ph.D. dissertation, Dept. Comput. Sci. Eng., National Sun Yat-Sen Univ., Kaohsiung, Taiwan, 2009.
[59] Y.-H. Han and S.-H. Hwang, "Care-of address provisioning for efficient IPv6 mobility support," *Comput. Commun.*, vol. 29, no. 9, pp. 1422–1432, 2006.
[60] M. Abbassi, S. Khan, and M. Rahman, "A distributed signaling fast mobile IPv6 scheme for next generation heterogeneous IP networks," in *Proc. Int. Conf. Res. Netw.* Berlin, Germany: Springer, 2012, pp. 43–51.
[61] N. Moore, *Optimistic Duplicate Address Detection (DAD) for IPv6*, document RFC 4429, IETF, Apr. 2006.
[62] R. Asati, H. Singh, W. Beebee, C. Pignataro, E. Dart, and W. George, *Enhanced Duplicate Address Detection*, document RFC 7527, IETF, Apr. 2015.
[63] L. J. Zhang, S. Pierre, and L. Marchand, "Optimization of handover performance for FMIPv6," in *Intelligence in Communication Systems*. Boston, MA, USA: Springer, 2005, pp. 169–178.
[64] F. Z. Yousaf, C. Wietfeld, and S. A. Mahmud, "Optimizing tunnel management in predictive handover protocols," *Comput. Netw.*, vol. 104, pp. 198–212, Jul. 2016.
[65] L. J. Zhang, W. K. Chen, Y. Zhang, A. Quintero, and S. Pierre, "Seamless mobility management schemes for IPv6-based wireless networks," *Mobile Netw. Appl.*, vol. 19, no. 6, pp. 745–757, Dec. 2014.
[66] F. Z. Yousaf and C. Wietfeld, *Proactive Bindings for FMIPv6*, document Internet Draft draft-yousaf-ietf-mipshop-pbfmipv6-01.txt (work in progress), IETF, Jul. 2008.
[67] J. Zhang and D. A. J. Pearce, "Proactive care-of address test for route optimization in FMIPv6," in *Proc. 3rd ACM Int. Workshop Wireless Mobile Appl. Services WLAN Hotspots*, 2005, pp. 92–95.
[68] J. Arkko, C. Vogt, and W. Haddad, *Enhanced Route Optimization for Mobile IPv6*, document RFC 4866, IETF, May 2007.
[69] R. M. Abdullah, A. Abdullah, N. A. W. A. Hamid, M. Othman, and S. Subramaniam, "The rapid vertical handover for efficient IPv6 mobility support in heterogeneous wireless networks," *Arabian J. Sci. Eng.*, vol. 39, no. 2, pp. 851–860, 2014.
[70] J. Espi, R. Atkinson, I. Andonovic, and J. Dunlop, "Proactive route optimization for fast mobile IPv6," in *Proc. IEEE 70th Veh. Technol. Conf. Fall (VTC-Fall)*, Sep. 2009, pp. 1–5.
[71] R. V. Ferre and J. P. Aspas, "Improving fast handovers for mobile IPv6: Optimal crossover discovery using geopaging routing tables," in *Proc. IEEE 61st Veh. Technol. Conf. (VTC-Spring)*, vol. 5, May 2005, pp. 2994–2998.
[72] D. H. Cuong, D. Guha, J. K. Choi, J. S. Park, and H. J. Kim, "An enhanced fast handover scheme with crossover router pre-discovery support in mobile IPv6," in *Proc. Joint Int. Conf. Opt. Internet Next Gener. Netw. (COIN-NGNCON)*, Jul. 2006, pp. 6–11.
[73] A. Viinikainen, J. Puttonen, M. Sulander, T. Hämäläinen, T. Ylönen, and H. Suutarinen, "Flow-based fast handover for mobile IPv6 environment—Implementation and analysis," *Comput. Commun.*, vol. 29, no. 16, pp. 3051–3065, 2006.
[74] A. Belhoul, Y. A. Şekercioğlu, and N. Mani, "Mobility-aware RSVP: A framework for improving the performance of multimedia services over wireless IP-based mobile networks," *Comput. Commun.*, vol. 32, no. 4, pp. 569–582, 2009.
[75] L. Zhang, S. Berson, S. Herzog, and S. Jamin, *Resource Reservation Protocol (RSVP)–Version 1 Functional Specification*, document RFC 2205, IETF, Sep. 1997.
[76] J.-M. Lee, H.-J. Lim, J.-H. Lee, and T.-M. Chung, "A scheme to reduce the handoff latency using mSCTP in fast mobile IPv6," in *Proc. 2nd Int. Conf. Syst. Netw. Commun. (ICSNC)*, Aug. 2007, p. 14.
[77] J. Liu, J. Dou, H. Zou, and Y. Gao, "Reducing signaling cost with simplifed mSCTP in fast mobile IPv6," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIHMSP)*, Aug. 2008, pp. 130–133.
[78] R. Stewart *et al.*, *Stream Control Transmission Protocol*, document RFC 4960, IETF, Sep. 2007.
[79] J. Espi, R. Atkinson, D. Harle, I. Andonovic, and C. Arthur, "Downlink TCP performance enhancement at handoff for FMIPv6-enabled nodes," in *Proc. 21st Annu. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2010, pp. 2266–2270.
[80] J. Rosenberg *et al.*, *SIP: Session Initiation Protocol*, document RFC 3261, IETF, Jun. 2002.
[81] D. S. Nursimloo, G. K. Kalebaila, and H. A. Chan, "A two-layered mobility architecture using fast mobile IPv6 and session initiation protocol," *EURASIP J. Wireless Commun. Netw.*, vol. 2008, Dec. 2007, Art. no. 348594.
[82] T. Al Mosawi, H. Shuaib, and A. H. Aghvami, "A fast handover scheme based on smart triggers and SIP," in *Proc. IEEE 70th Veh. Technol. Conf. Fall (VTC-Fall)*, Sep. 2009, pp. 1–5.
[83] Y.-S. Yen, L.-Y. Chen, T.-Y. Chi, and H.-C. Chao, "A novel predictive scheduling handover on mobile IPv6," *Telecommun. Syst.*, vol. 52, no. 2, pp. 461–473, 2013.
[84] S. Lee, R. S. Tolentino, and B. Park, "Fast location opposite update scheme for minimizing handover latency over wireless/mobile networks," in *Proc. 5th Int. Multi-Conf. Eng. Technol. Innov. (IMETI)*, 2012, pp. 50–54.

[85] X. Cai and F. Liu, "Optimizing fast handover for mobile IPv6 with dynamic price," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar./Apr. 2008, pp. 2828–2833.

[86] M. Tao and H. Yu, "A smooth handover scheme for fast-moving users in mobile IPv6 networks," *Wireless Pers. Commun.*, vol. 60, no. 4, pp. 649–664, 2011.

[87] S.-R. Tong and S.-H. Yang, "Buffer control to support a seamless stream handoff in a WLAN that employs simulcast streaming," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 260–268, Jan. 2008.

[88] K. M. Kim, S. J. Yong, B. S. Sim, H. Y. Youn, and O. Song, "Effective packet buffering for FMIPv6 protocol over DiffServ domain," in *Proc. Int. Conf. Inf. Netw.*, Feb. 2012, pp. 102–107.

[89] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, *An Architecture for Differentiated Services*, document RFC 2475, IETF, Dec. 1998.

[90] Y.-S. Yen, R.-S. Chang, and C.-Y. Wu, "A seamless handoff scheme for IEEE 802.11 wireless networks," *Wireless Commun. Mobile Comput.*, vol. 13, no. 2, pp. 157–169, 2013.

[91] S. Bonam and P. A. Kumari, "Fast and reliable handover in heterogeneous networks (mobile IPv6)," *Int. J. Adv. Res. Electr., Electron. Instrum. Eng.*, vol. 3, no. 11, pp. 12954–12961, Nov. 2014.

[92] K. Malki and H. Soliman, *Simultaneous Bindings for Mobile IPv6 Fast Handovers*, document Internet Draft draft-elmalki-mobileip-bicasting-v6-06 (work in progress), IETF, Jul. 2005.

[93] H. Petander, "Optimizing localized mobility management for make-before-break handoffs," in *Proc. NEWCOM-ACoRN Joint Workshop*, Sep. 2006, pp. 1–6.

[94] E. Ivov and T. Noel, "An experimental performance evaluation of the IETF FMIPv6 protocol over IEEE 802.11 WLANs," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, vol. 1, Apr. 2006, pp. 568–574.

[95] J. H. Lee, T. Ernst, and T. M. Chung, "Cost analysis of IP mobility management protocols for consumer mobile devices," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 1010–1017, May 2010.

[96] T. C. Schmidt and M. Wählisch, "Predictive versus reactive—Analysis of handover performance and its implications on IPv6 and multicast mobility," *Telecommun. Syst.*, vol. 30, no. 1, pp. 123–142, 2005.

[97] T. C. Schmidt and M. Wählisch, "Analysis of handover frequencies for predictive, reactive and proxy schemes and their implications on IPv6 and multicast mobility," in *Networking—ICN*. Berlin, Germany: Springer, 2005, pp. 1039–1046.

[98] S. Ryu, K. Lee, and Y. Mun, "Optimized fast handover scheme in mobile IPv6 networks to support mobile users for cloud computing," *J. Supercomput.*, vol. 59, no. 2, pp. 658–675, 2012.

[99] M. Boutabia and H. Afifi, "Maximizing predictive mode probability in fast handovers for mobile IP," in *Proc. 20th Int. Conf. Telecommun. (ICT)*, May 2013, pp. 1–5.

[100] A. Bagheri, "Enhancing fast mobile IPv6 (FMIPv6) handoff by eliminating reactive mode using candidate care-of address," Ph.D. dissertation, Univ. Malaya, Kuala Lumpur, Malaysia, 2010.

[101] B. Liu, P. Martins, and P. Bertin, "The operation mode selection in FMIPv6," in *Proc. IEEE Symp. Comput. Commun.*, Jul. 2008, pp. 742–749.

[102] J. Zongpu, W. Hongmei, X. Xiao, and J. Ziyu, "Analysis and optimization for handover performance of mobile IPv6 based ping-pong mode," in *Proc. 3rd Int. Conf. Pervasive Comput. Appl. (ICPCA)*, vol. 2, Oct. 2008, pp. 667–672.

[103] L. Zhuang, C. Wang, and Y. Zhang, "Research of an improved mobile IPv6 smooth handoff technology," in *Proc. Third Int. Symp. Electron. Commerce Secur. Workshops (ISECS)*, Guangzhou, China, 2010, pp. 347–350.

[104] M.-S. Chiang, C.-M. Huang, P. B. Chau, S. Xu, H. Zhou, and D. Ren, "A forward fast media independent handover control scheme for proxy mobile IPv6 (FFMIH-PMIPv6) over heterogeneous wireless mobile network," *Telecommun. Syst.*, vol. 65, no. 4, pp. 699–715, Aug. 2017.

[105] M. Liebsch, H. Chaskar, E. Shim, A. Singh, and D. Funato, *Candidate Access Router Discovery (CARD)*, document RFC 4066, IETF, Jul. 2005.

[106] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, *Context Transfer Protocol (CXTP)*, document RFC 4067, IETF, Jul. 2005.

[107] Y. Zhou, J. Yuan, Y. Wang, and P. Zhang, "Service-oriented FMIPv6 framework for efficient handovers in 4G networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2007, pp. 4478–4482.

[108] F. Z. Yousaf, C. Müller, and C. Wietfeld, "Multi-hop discovery of candidate access routers (MHD-CAR) for fast moving mobile nodes," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.

[109] D. Di Sorte, M. Femminella, L. Piacentini, and G. Reali, "Performance evaluation of the push-mode-multicast based candidate access router discovery (PMM CARD)," *Comput. Netw.*, vol. 50, no. 3, pp. 367–397, 2006.

[110] D.-H. Kwon, Y.-S. Kim, K.-J. Bae, and Y.-J. Suh, "Access router information protocol with FMIPv6 for efficient handovers and their implementations," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 6, Dec. 2005, p. 6.

[111] V. Solouk, B. M. Ali, S. Khatun, K. D. Wong, and M. A. Mahdi, "Layer-2 protocol adaptation method to improve fast handoff for mobile IPv6 vertical handoffs," *J. Commun.*, vol. 4, no. 6, pp. 396–403, 2009.

[112] J. Kempf, *Problem Description: Reasons for Performing Context Transfers Between Nodes in an IP Access Network*, docuemnt RFC 3374, Sep. 2002.

[113] R. Farahbakhsh, "Smooth handover by synchronizing context transfer protocol and fast mobile IPv6," in *Proc. IEEE Int. Conf. Internet Multimedia Services Archit. Appl. (IMSAA)*, Dec. 2009, pp. 1–5.

[114] W. B. Diab and S. Tohme, "Seamless handover and security solution for real-time services," in *Proc. 11th IEEE Int. Symp. Multimedia (ISM)*, Dec. 2009, pp. 363–368.

[115] Q. B. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized FMIPv6 using IEEE 802.21 MIH services in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, Nov. 2007, pp. 3397–3407.

[116] T.-Y. Wu, W. Chen, W.-T. Lee, and Y.-P. Huang, "Improving handoff efficiency by IS-FMIPv6 based on IEEE 802.21," *Concurrency Comput., Pract. Exper.*, vol. 24, no. 4, pp. 371–382, 2012.

[117] V. Solouk, B. M. Ali, S. Khatun, D. Wong, and M. A. Mahdi, "Layer-2 protocol adaptation method to improve fast handoff for mobile IPv6 vertical handoffs," in *Proc. 11th Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2008, pp. 492–497.

[118] Y. Y. An, B. H. Yae, K. W. Lee, Y. Z. Cho, and W. Y. Jung, "Reduction of handover latency using MIH services in MIPv6," in *Proc. 20th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, vol. 2, Apr. 2006, pp. 229–234.

[119] M. Boutabia and H. Afifi, "MIH-based FMIPv6 optimization for fast-moving mobiles," in *Proc. 3rd Int. Conf. Pervasive Comput. Appl. (ICPCA)*, vol. 2, Oct. 2008, pp. 616–620.

[120] M. Kim, T. W. Moon, and S. J. Cho, "Network-based seamless handover framework providing QoS in heterogeneous wireless networks," in *Proc. 9th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2009, pp. 254–258.

[121] A. Almeida, N. Lopes, and A. Santos, "Intelligent handover for vehicular networks," in *Proc. 22nd Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2014, pp. 298–304.

[122] J. Yuan, Y. Wang, F. Liu, and L. Zheng, "Optimized handover scheme using IEEE 802.21 MIH service in multi-service environment," in *Proc. IEEE 71st Veh. Technol. Conf. (VTC-Spring)*, May 2010, pp. 1–5.

[123] B. Park and H. Latchman, "Performance enhancement of fast handover for MIPv6 by reducing out-of-sequence packets," *Wireless Pers. Commun.*, vol. 47, no. 2, pp. 207–217, Mar. 2008.

[124] W. Yi-Zhi and L. Xing-Feng, "TCP performance analysis and improvement in FMIPv6," in *Proc. 10th Int. Conf. Adv. Commun. Technol. (ICACT)*, vol. 3, Feb. 2008, pp. 1539–1543.

[125] D. Le, X. Fu, and D. Hogrefe, "A cross-layer approach for improving TCP performance in mobile environments," *Wireless Pers. Commun.*, vol. 52, no. 3, pp. 669–692, 2010.

[126] J. Liu and L. Han, "QoS-satisfied pathover scheme in FMIPv6 environment," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 3, Dec. 2008, pp. 157–160.

[127] N. V. Lopes, M. J. Nicolau, and A. Santos, "A QoS-enable solution for mobile environments," in *Proc. Actas 10th Conf. Redes Comput. (CRC)*. Braga, Portugal: Univ. Minho, 2010, pp. 1–7.

[128] N. V. Lopes, M. J. Nicolau, and A. Santos, "A QoS-enabled resource management scheme for F-HMIPv6 micro mobility approach," *Telecommun. Syst.*, vol. 52, no. 1, pp. 341–357, 2013.

[129] R. Bless, J. Hillebrand, C. Prehofer, and M. Zitterbart, "A quality-of-service signaling architecture for seamless handover support in next generation, IP-based mobile networks," *Wireless Pers. Commun.*, vol. 43, no. 3, pp. 817–835, 2007.

[130] H. Lee, J.-Y. Choi, and J. Jeong, "On security-effective mobility-QoS management scheme in heterogeneous mobile networks," in *Proc. AFIN*, 2015, p. 62.

[131] C. Liu, D. Qian, Y. Liu, and K. Xiao, "A framework for end-to-end QoS context transfer in mobile IPv6," in *Proc. IFIP Int. Conf. Pers. Wireless Commun.* Springer, 2004, pp. 466–475.
[132] Q. Wang and M. A. Abu-Rgheff, "IPv6-based architecture for fast and cost-effective micro-mobility management," in *Proc. 6th IEEE Int. Conf. 3G Beyond*. Edison, NJ, USA: IET, 2005, pp. 1–5.
[133] T. Chen, G. Schafer, A. Wolisz, and M. Sortais, "A performance study of session state re-establishment schemes in IP-based micro-mobility scenarios," in *Proc. 12th Annu. Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst. (MASCOTS)*, Oct. 2004, pp. 159–166.
[134] S. Elleingand and S. Pierre, "FH-RSVP scheme for intra-site handover in hierarchical mobile IPv6 networks," *Comput. Commun.*, vol. 30, no. 2, pp. 416–427, 2007.
[135] J. Dou, H. Zeng, and H. Wang, "Single user-plane architecture network (SUPANET) and its QoS provisioning mechanisms in signaling and management (S&M) planes," in *Proc. 5th Int. Conf. Parallel Distrib. Comput., Appl. Technol. (PDCAT)*, Singapore. Berlin, Germany: Springer, 2005, pp. 429–440.
[136] Y. Gao, H. Zeng, and H. Wang, "Research on mobility management in DDQP mechanism of SUPANET," in *Proc. WRI Int. Conf. Commun. Mobile Comput. (CMC)*, vol. 3, Jan. 2009, pp. 216–221.
[137] J. Wang, M. Song, Y. Zhang, N. Liu, and Y. Man, "A mobility-aware scheme for next steps in signaling with resource reservation mechanism," in *Proc. IEEE Int. Conf. Commun. Technol. Appl. (ICCTA)*, Oct. 2009, pp. 796–800.
[138] X. Yan, Y. A. Şekercioğlu, and S. Narayanan, "A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks," *Comput. Netw.*, vol. 54, pp. 1848–1863, Feb. 2010.
[139] H. Petander, E. Perera, and A. Seneviratne, "Multicasting with selective delivery: A SafetyNet for vertical handoffs," *Wireless Pers. Commun.*, vol. 43, no. 3, pp. 945–958, 2007.
[140] A. B. Pontes, D. D. P. Silva, J. Jailton, O. Rodrigues, and K. L. Dias, "Handover management in integrated WLAN and mobile WiMAX networks," *IEEE Wireless Commun.*, vol. 15, no. 5, pp. 86–95, Oct. 2008.
[141] A. Michalas, A. Sgora, and D. D. Vergados, "An integrated MIH-FPMIPv6 mobility management approach for evolved-packet system architectures," *J. Netw. Comput. Appl.*, vol. 91, pp. 104–119, Aug. 2017.
[142] M. Boutabia, E. Abd-Elrahman, and H. Afifi, "A hybrid mobility mechanism for heterogeneous networks in IMS," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, Jul. 2010, pp. 1570–1575.
[143] T. Schmidt, M. Waehlisch, R. Koodli, G. Fairhurst, and D. Liu, *Multicast Listener Extensions for Mobile IPv6 (MIPv6) and Proxy Mobile IPv6 (PMIPv6) Fast Handovers*, document RFC 7411, IETF, Nov. 2014.
[144] B. Fenner, H. He, B. Haberman, and H. Sandick, *Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding (IGMP/MLD Proxying)*, document RFC 4605, IETF, Aug. 2006.
[145] K. Suh, D.-H. Kwon, Y.-J. Suh, and Y. Park, *Fast Multicast Protocol for Mobile IPv6 in the Fast Handovers Environments*, document Internet Draft draft-suh-mipshop-fmcast-mip6-00.txt (work in progress), IETF, Jan. 2004.
[146] C. Janneteau, Y. Tian, S. Csaba, T. Lohmar, H.-Y. Lach, and R. Tafazolli, "Comparison of three approaches towards mobile multicast," in *Proc. IST Mobile Summit*, 2003, pp. 15–18.
[147] M. Gohar, S. T. Kim, and S. J. Koh, "Fast tree join for seamless multicast handover in FMIPv6-based mobile networks," *Telecommun. Rev.*, vol. 20, no. 6, pp. 993–1003, 2010.
[148] H. Zhang, H. Zhou, H. Zhang, J. Guan, and W. Liu, "A novel seamless handoff mechanism for MPLS multicast," in *Proc. IET Int. Conf. Wireless, Mobile Multimedia Netw.*, 2006, pp. 1–4.
[149] M. O. Cherif, S.-M. Senouci, and B. Ducourthial, "MCMIPv6: Multicast configuration-based mobile IPv6 protocol," in *Proc. IFIP Wireless Days (WD)*, Oct. 2010, pp. 1–5.
[150] S.-J. Yoo and S.-J. Shin, "Fast handover mechanism for seamless multicasting services in mobile IPv6 wireless networks," *Wireless Pers. Commun.*, vol. 42, no. 4, pp. 509–526, 2007.
[151] T. C. Schmidt, M. Wählisch, and M. Wodarz, "Fast adaptive routing supporting mobile senders in source specific multicast," *Telecommun. Syst.*, vol. 43, no. 1, pp. 95–108, 2009.
[152] D.-H. Kwon, W.-J. Kim, and Y.-J. Suh, "An efficient mobile multicast mechanism for fast handovers: A study from design and implementation in experimental networks," *Comput. Commun.*, vol. 31, no. 10, pp. 2162–2177, 2008.
[153] J. Guan, H. Luo, H. Zhang, H.-C. Chao, and J. H. Park, "Design and implementation of light-weight mobile multicast for fast MIPv6," *Comput. Commun.*, vol. 32, no. 3, pp. 552–559, 2009.
[154] G. A. Leoleis and I. S. Venieris, "Fast MIPv6 extensions supporting seamless multicast handovers," *Comput. Netw.*, vol. 51, no. 9, pp. 2379–2396, 2007.
[155] H. Modares, A. Moravejosharieh, J. Lloret, and R. Salleh, "A survey of secure protocols in mobile IPv6," *J. Netw. Comput. Appl.*, vol. 39, pp. 351–368, Mar. 2014.
[156] O. Elshakankiry, N. Zhang, and A. Carpenter, "Securing home and correspondent registrations in mobile IPv6 networks," Ph.D. dissertation, School Comput. Sci., Univ. Manchester, Manchester, U.K., 2010.
[157] I. You, Y. Hori, and K. Sakurai, "State of art on security protocols for fast mobile IPv6," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 20, no. 3, pp. 121–134, 2010.
[158] K. Elgoarany and M. Eltoweissy, "Security in mobile IPv6: A survey," *Inf. Secur. Tech. Rep.*, vol. 12, no. 1, pp. 32–43, 2007.
[159] H. Sun, J. Song, and Z. Chen, "Survey of authentication in mobile IPv6 network," in *Proc. 7th IEEE Consum. Commun. Netw. Conf.*, Jan. 2010, pp. 1–4.
[160] J. Guan, I. You, C. Xu, H. Zhou, and H. Zhang, "Survey on route optimization schemes for proxy mobile IPv6," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2012, pp. 541–546.
[161] A. Moravejosharieh, H. Modares, and R. Salleh, "Overview of mobile IPv6 security," in *Proc. 3rd Int. Conf. Intell. Syst. Modeling Simulation*, Feb. 2012, pp. 584–587.
[162] T. Aura, "Mobile IPv6 security," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 2002, pp. 215–234.
[163] J. Kempf and R. Koodli, *Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using Secure Neighbor Discovery (SEND)*, document RFC 5269, IETF, Jun. 2008.
[164] I. You, K. Sakurai, and Y. HORI, "An enhanced security protocol for fast mobile IPv6," *IEICE Trans. Inf. Syst.*, vol. E92-D, no. 10, pp. 1979–1982, 2009.
[165] H.-S. Kang and C.-S. Park, "Authenticated fast handover scheme in the hierarchical mobile IPv6," in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, 2006, pp. 211–224.
[166] I. You, K. Sakurai, and Y. Hori, "Comments on kang-park's security scheme for fast handover in hierarchical mobile IPv6," in *Proc. 4th Int. Conf. Frontier Comput. Sci. Technol.*, Dec. 2009, pp. 351–355.
[167] W. Haddad and S. Krishnan, *Authenticating FMIPv6 Handovers*, document Internet-Draft draft-haddad-mipshop-fmipv6-auth-02 (work in progress), IETF, Sep. 2006.
[168] I. You and J.-H. Lee, "Comments on a one-way hash chain based authentication for FMIPv6," in *Proc. Int. Conf. Broadband, Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2010, pp. 293–296.
[169] V. Narayanan, *Establishing Handover Keys Using Shared Keys*, document Internet Draft draft-vidya-mipshop-handover-keys-aaa-04.txt (work in progress), IETF, Mar. 2007.
[170] J. Choi and S. Jung, "An integrated handover authentication for FMIPv6 over heterogeneous access link technologies," *Wireless Pers. Commun.*, vol. 71, no. 2, pp. 839–856, 2013.
[171] C.-S. Park, H.-S. Kang, and J. Jung, "A cross-layer key management scheme for MIPv6 fast handover over IEEE 802.11 wireless LAN," *Mobile Inf. Syst.*, vol. 2015, Oct. 2015, Art. no. 708064.
[172] B. A. Forouzan, "Network security," in *Data Communications and Networking*, 4th ed. New York, NY, USA: McGraw-Hill, 2007, pp. 961–994.
[173] T. Narten, E. Nordmark, and W. Simpson, *Neighbor Discovery for IP Version 6 (IPv6)*, document RFC 4861, IETF, Sep. 2007.
[174] J. Arkko, J. Kempf, B. Zill, and P. Nikander, *Secure Neighbor Discovery (SEND)*, document RFC 3971, IETF, Mar. 2005.
[175] I. You, Y. Hori, and K. Sakurai, "Enhancing SVO logic for mobile IPv6 security protocols," *J. Wireless Mobile Netw.*, vol. 2, no. 3, pp. 26–52, 2011.
[176] H. Yokota and G. Dommety, *Mobile IPv6 Fast Handovers for 3G CDMA Networks*, document RFC 5271, IETF, Jun. 2008.
[177] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition*, IEEE Standard 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008), Jul. 2008, pp. 1–126.

[178] *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*, IEEE Standard 802.1X-2010, Feb. 2010.

[179] F. Z. Yousaf and C. Wietfeld, "Optimizing throughput performance of FMIPv6 over legacy 802.11 networks using iterative scanning," *Comput. Netw.*, vol. 57, no. 3, pp. 762–781, 2013.

[180] P.-J. Huang, Y.-C. Tseng, and K.-C. Tsai, "A fast handoff mechanism for IEEE 802.11 and IAPP networks," in *Proc. IEEE 63rd Veh. Technol. Conf.*, vol. 2, May 2006, pp. 966–970.

[181] J. Ok, P. Morales, A. Darmawan, and H. Morikawa, "Using shared beacon channel for fast handoff in IEEE 802.11 wireless networks," in *Proc. IEEE 65th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2007, pp. 849–853.

[182] J. Teng, C. Xu, W. Jia, and D. Xuan, "D-scan: Enabling fast and smooth handoffs in AP-dense 802.11 wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 2616–2620.

[183] Y. Yan, Y. Qian, and R. Q. Hu, "A novel channel probing/scanning scheme for secure fast handoff in IEEE 802.11-based wireless networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–6.

[184] X. Chen and D. Qiao, "HaND: Fast handoff with null dwell time for IEEE 802.11 networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[185] S. H. Obay, H. S. Hasan, and S. Rosli, "Fast handoff for 802.11 wireless network," *Commun. Netw.*, vol. 3, no. 4, pp. 250–256, 2011.

[186] Y. S. Chen, M. C. Chuang, and C. K. Chen, "DeuceScan: Deuce-based fast handoff scheme in IEEE 802.11 wireless networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 2, pp. 1126–1141, Mar. 2008.

[187] S. Kim and S. Seo, "Dual authentications for fast handoff in IEEE 802.11 WLANs: A reactive approach," in *Proc. 1st Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol., Wireless VITAE*, May 2009, pp. 156–160.

[188] J. Ok, P. Morales, and H. Morikawa, "AuthScan: Enabling fast handoff across already deployed IEEE 802.11 wireless networks," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.

[189] B. Park, Y.-H. Han, and H. Latchman, "EAP: New fast handover scheme based on enhanced access point in mobile IPv6 networks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 9, pp. 69–75, 2006.

[190] J. Montavont, E. Ivov, T. Noel, and K. Guillouard, "Analysis of a geolocation-based FMIPv6 extension for next generation wireless LANs," *Ubiquitous Comput. Commun. J.*, vol. 2, no. 5, pp. 56–65, 2007.

[191] W.-J. Kim, D.-H. Kwon, and Y.-J. Suh, "Integrated handoff scheme of FMIPv6 and MAC protocol in 4th generation systems," in *Proc. 7th Int. Conf. Adv. Commun. Technol. (ICACT)*, vol. 2, 2005, pp. 971–976.

[192] *IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability Via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation*, IEEE Standard 802.11F-2003, 2003.

[193] *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society*, Standard 802.16e-2005 and IEEE Standard 802.16-2004/Cor1-2005, 2006.

[194] *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Standard 802.16e-2005 and IEEE Standard 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), 2006, pp. 1–822.

[195] S. K. Ray, K. Pawlikowski, and H. Sirisena, "Handover in mobile WiMAX networks: The state of art and research issues," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 3, pp. 376–399, 3rd Quart., 2010.

[196] H. Kim and M. Moh, "Performance of FMIPv6-based cross-layer handover for supporting mobile VoIP in WiMAX networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process.*, Aug. 2009, pp. 221–226.

[197] C.-H. Shih and Y.-C. Chen, "A FMIPv6 based handover scheme for real-time applications in mobile WiMAX," *J. Netw.*, vol. 5, no. 8, pp. 929–936, 2010.

[198] Y.-W. Chen and F.-Y. Hsieh, "A cross layer design for handoff in 802.16e network with IPv6 mobility," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 3844–3849.

[199] S. M. Seyyedoshohadaei, S. Khatun, B. M. Ali, M. Othman, and F. Anwar, "An integrated scheme to improve performance of fast mobile IPv6 handover in IEEE 802.16e network," in *Proc. IEEE 9th Malaysia Int. Conf. Commun. (MICC)*, Dec. 2009, pp. 840–845.

[200] J. Park, D.-H. Kwon, and Y.-J. Suh, "An integrated handover scheme for fast mobile IPv6 over IEEE 802.16e systems," in *Proc. IEEE Veh. Technol. Conf.*, Sep. 2006, pp. 1–5.

[201] J. Kim, J. Jeong, and H. Choo, "An efficient handover scheme with pre-configured tunneling in IEEE 802.16e systems," in *Proc. Australas. Telecommun. Netw. Appl. Conf. (ATNAC)*, Dec. 2007, pp. 408–413.

[202] K. Lee and Y. Mun, "Fast handover for mobile IPv6 over IEEE 802.16e networks," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, Jun./Jul. 2009, pp. 29–33.

[203] I. Khan and D. A. Karras, "An efficient cross layer intra and inter domain mobility solution for IEEE 802.16e mobile WiMAX," in *Proc. 16th Int. Conf. Syst., Signals Image Process.*, Jun. 2009, pp. 1–7.

[204] S. Pahal, B. Singh, and A. Arora, "Cross layer based fast handover for IEEE 802.16e networks," *Opt.-Int. J. Light Electron Opt.*, vol. 125, no. 15, pp. 4108–4112, 2014.

[205] H.-H. Huang, J.-S. Wu, and S.-F. Yang, "A multiple cross-layers explicit fast handover control using MIH in 802.16e networks," in *Proc. 5th IFIP Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, May 2008, pp. 1–5.

[206] G. A. Al-Suhail and H. J. Al-Hammedy, "Improving inter-domain fast handover using MIH services in mobile WiMAX," *Int. J. Commun., Netw. Syst. Sci.*, vol. 5, no. 11, pp. 743–752, 2012.

[207] J. Yuan, C. Bo, and Z. Chen, "An improved FHMIPv6 handover scheme for mobile WiMAX," in *Proc. 4th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Oct. 2008, pp. 1–4.

[208] H.-H. Huang and J.-S. Wu, "A Pre-binding update fast handover control using IEEE 802.21 MIH over 802.16e networks," in *Proc. WRI Int. Conf. Commun. Mobile Comput. (CMC)*, vol. 2, Jan. 2009, pp. 417–421.

[209] F. Giust, L. Cominardi, and C. J. Bernardos, "Distributed mobility management for future 5G networks: Overview and analysis of existing approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 142–149, Jan. 2015.

[210] Q. C. Li, H. Niu, A. T. Papathanassiou, and G. Wu, "5G network capacity: Key elements and technologies," *IEEE Veh. Technol. Mag.*, vol. 9, no. 1, pp. 71–78, Mar. 2014.

[211] I. F. Akyildiz, S. Nie, S.-C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Comput. Netw.*, vol. 106, pp. 17–48, Sep. 2016.

[212] L. Cominardi, F. Giust, C. J. Bernardos, and A. De La Oliva, "Distributed mobility management solutions for next mobile network architectures," *Comput. Netw.*, vol. 121, pp. 124–136, Jul. 2017.

[213] M. M. Sajjad, "A software-defined networking based adaptive multimode decentralized mobility architecture for 5G," M.S. thesis, Dept. Elect. Eng. Comput. Sci., Queensland Univ. Technol., Brisbane, QLD, Australia, 2018.

[214] D. Pliatsios, P. Sarigiannidis, S. Goudos, and G. K. Karagiannidis, "Realizing 5G vision through Cloud RAN: Technologies, challenges, and trends," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 136, May 2018.

[215] M. A. Ferrag, L. Maglars, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[216] X. Yin and L. Wang, "A fast handover scheme for SDN based vehicular network," in *Mobile Ad-hoc and Sensor Networks*. Singapore: Springer, 2018, pp. 293–302.

[217] Sandhya, Y. Sinha, and K. Haribabu, "A survey: Hybrid SDN," *J. Netw. Comput. Appl.*, vol. 100, pp. 35–55, Dec. 2017.

[218] R. Amin, M. Reisslein, and N. Shah, "Hybrid SDN networks: A survey of existing approaches," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3259–3306, 4th Quart., 2018.

[219] "5G and security," *Eur. 5G Annu. J.*, 5GPPP, Oct. 2016, p. 54. https://bscw.5gppp.eu/pub/bscw.cgi/d117642/Euro%205G%20Annual%20Journal%202016.pdf

[220] "5G PPP phase 1 security landscape," 5GPPP Secur. WG, White Paper, Jun. 2017. [Online]. Available: https://5g-ppp.eu/wpcontent/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[221] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.
[222] D. D. Liu, J. Zuniga, P. Seite, H. Chan, and C. Bernardos, *Distributed Mobility Management: Current Practices and Gap Analysis*, document RFC 7429, IETF, Jan. 2015.
[223] M. Balfaqih, M. Ismail, R. Nordin, A. A. Rahem, and Z. Balfaqih, "Fast handover solution for network-based distributed mobility management in intelligent transportation systems," *Telecommun. Syst.*, vol. 64, no. 2, pp. 325–346, 2017.
[224] M. Balfaqih, M. Ismail, R. Nordin, and Z. A. Balfaqih, "802.21-assisted distributed mobility management solution in vehicular networks," *IEEE Access*, vol. 5, pp. 9518–9532, 2017.
[225] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 90–96, Feb. 2014.
[226] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[227] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Commun. Surveys Tuts.*, to be published.
[228] S. Ben Hadj Said, K. Guillouard, and J.-M. Bonnin, "Towards adaptive security mechanisms in 3GPP EPS/LTE networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 1876–1881.

MUHAMMAD MOHTASIM SAJJAD received the M.Eng. degree from the Queensland University of Technology, Brisbane, Australia. He has spent three years in the industry, working on NGN technologies in different engineering roles including network operations and management. His research interests include 5G networks, mobile communications, software-defined networking, network slicing, and network virtualization. He is a member of the IEEE. He has served as a reviewer for several international conferences and journals.

DHAMMIKA JAYALATH received the B.Sc. degree in electronics and telecommunications engineering from the University of Moratuwa, Sri Lanka, the M.Eng. degree in telecommunications from the Asian Institute of Technology, Thailand, and the Ph.D. degree in wireless communications from Monash University, Australia, in 2002. He was a Fellow at the Australian National University and a Senior Researcher at the National ICT Australia. Since 2007, he has been an Academic with the School of Electrical Engineering and Computer Science, Queensland University of Technology. His research interests include the general areas of communications and signal processing. He has published significantly in these areas. His current research interests include cooperative communications, cognitive radios, statistical signal processing, and multiuser communications. He is a Senior Member of the IEEE.

CARLOS J. BERNARDOS received the degree in telecommunication engineering and the Ph.D. degree in telematics from the University Carlos III of Madrid (UC3M), in 2003 and 2006, respectively. His Ph.D. thesis focused on route optimization for mobile networks in IPv6 heterogeneous environments. From 2003 to 2008, he was a Research and Teaching Assistant with UC3M, where he has been an Associate Professor, since 2008. He has published over 50 scientific papers in prestigious international journals and conferences. He is an active contributor to the Internet Engineering Task Force. His current work focuses on vehicular networks and IP-based mobile communication protocols. He served as the TPC Chair for WEEDEV 2009 and the TPC Co-Chair for the Mobility Track of NTMS 2011. He has also served as a Guest Editor for the IEEE Network.