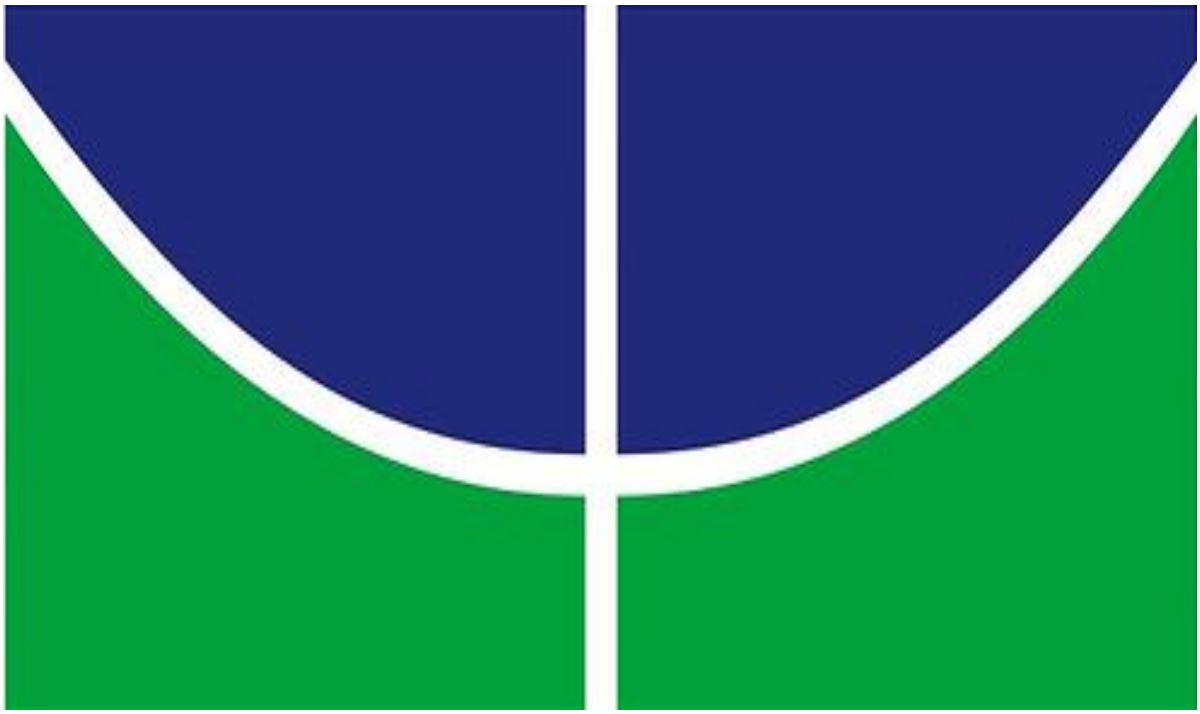

Avaliação de Desempenho de Protocolos de Autenticação para Redes Sem Fio Heterogêneas

JOSÉ BENÍCIO MENEZES TRINETO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AVALIAÇÃO DE DESEMPENHO DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES SEM FIO HETEROGÊNEAS

JOSÉ BENÍCIO MENEZES TRINETO

ORIENTADOR: PAULO ROBERTO DE LIRA GONDIM

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGE.DM - 624/2016
BRASÍLIA/DF: MARÇO - 2016

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AVALIAÇÃO DE DESEMPENHO DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES SEM FIO HETEROGÊNEAS

JOSÉ BENÍCIO MENEZES TRINETO

DISSERTAÇÃO DE MESTRADO SUBMETÍDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

PAULO ROBERTO DE LIRA GONDIM, Dr., ENE/UNB
(ORIENTADOR)

UGO SILVA DIAS, Dr., ENE/UNB
(EXAMINADOR INTERNO)

PRISCILA AMERICA SOLIS M. BARRETO, Dr., CIC/UNB
(EXAMINADOR EXTERNO)

Brasília, 02 de março de 2016.

FICHA CATALOGRÁFICA

TRINETO, JOSÉ BENÍCIO
Avaliação de Desempenho de Protocolos de Autenticação para Redes Sem Fio Heterogêneas [Distrito Federal] 2016.
xxii, 147p.,210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2016).
Dissertação de Mestrado – Universidade de Brasília.
Faculdade de Tecnologia.
Departamento de Engenheira Elétrica.
1.Redes Heterogêneas 2. Autenticação
3.Gerência de Mobilidade 4. *Handover* Vertical

REFERÊNCIA BIBLIOGRÁFICA

TRINETO, J. B. (2016). Avaliação de Desempenho de Protocolos de Autenticação para Redes Sem Fio Heterogêneas. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGE.DM - 624/2016, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 147p.

CESSÃO DE DIREITOS

AUTOR: José Benício Menezes Trineto

TÍTULO: Avaliação de Desempenho de Protocolos de Autenticação para Redes Sem Fio Heterogêneas.

GRAU: Mestre ANO: 2016

_____

José Benício Menezes Trineto
UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.
70910-900 – Brasília – DF – Brasil.

AGRADECIMENTOS

Aos meus pais, Jacilene e José Benício, pelo carinho e dedicação ao longo de toda a minha vida.

Aos meus avós, Mari-Sol e José Benício, pelo modelo de vida que são.

A minha noiva Clarissa, pelo companheirismo e paciência ao longo da realização deste trabalho.

Especialmente ao meu orientador Paulo Gondim, pelo apoio desde os meus tempos de aluno de Engenharia de Redes de Comunicação.

RESUMO

AVALIAÇÃO DE DESEMPENHO DE PROTOCOLOS DE AUTENTICAÇÃO PARA REDES SEM FIO HETEROGÊNEAS

Com a crescente evolução das tecnologias de redes sem fio, passou a ser considerada, em anos recentes, a integração e a convergência de diferentes tecnologias de redes, com capacidades e funcionalidades específicas, e favorecida pela existência de terminais com múltiplas interfaces, que podem ser servidos por redes heterogêneas. Essa integração possibilita a oferta de alternativas de conectividade aos usuários e o aumento da área de cobertura, ao mesmo tempo em que uma variada gama de problemas passa a requerer solução, tais como a seleção de redes, o gerenciamento integrado de recursos, o controle de congestão, a autenticação e o gerenciamento de mobilidade.

As redes heterogêneas (HetNets) constituem um dos pilares sobre os quais se baseiam as 4ª e 5ª gerações de redes sem fio (4G e 5G, respectivamente), em que redes baseadas em múltiplas tecnologias de acesso rádio (RAT) devem ser integradas harmoniosamente, o que requer o adequado tratamento de *handovers*, visando a desejada continuidade de serviços durante e após a transição entre diferentes RATs. Esse tratamento é fortemente dependente da adequada solução de alguns dos problemas citados, dos quais se destacam, neste trabalho, os de autenticação e de gerenciamento de mobilidade.

Por outro lado, para o atendimento à demanda de diversas aplicações que apresentam requisitos estritos de QoS (*Quality of Service)*, como as que envolvem comunicações multimídias em tempo real, os dispositivos móveis devem trocar o menor número de mensagens durante o *handover*, o que poderá proporcionar economia de banda e favorecer o atendimento aos requisitos de QoS citados.

Este trabalho avaliou o impacto de recentes métodos de autenticação em *handovers* envolvendo redes LTE e WLAN, interligadas por um núcleo EPC (*Evolved Packet Core)*, com relação a latência e sinalização de *handover*, juntamente com aspectos de segurança, tais como gerenciamento de chaves e proteção contra ameaças.

Em conjunto com os métodos de autenticação, foi utilizado o protocolo PMIPv6 (*Proxy Mobile IPv6*), um dos padrões pelo 3GPP para prover gerenciamento de mobilidade relativo à interconexão de redes heterogêneas.

A avaliação de desempenho se deu por meio de modelagem analítica em três estudos de casos. No primeiro, foi avaliada a latência de *handover*, em um cenário de *handover*

vertical no sentido LTE → WLAN; tal cenário é particularmente importante ao se considerar à possibilidade de *data offloading* para controle de congestão nas redes celulares. No segundo estudo de caso foram avaliadas a latência e a sinalização de *handover* em um cenário de *handover* horizontal entre redes WLANs em que a rede LTE é a rede caseira do móvel; tal cenário também possui relação direta com a possibilidade de *data offloading.* No terceiro estudo de caso utilizou-se o mesmo cenário do segundo estudo de caso, mas considerando outros aspectos relativos à modelagem analítica.

O estudo e a avaliação dos diversos métodos de autenticação serviram como base para a apresentação de proposta preliminar de um novo protocolo de autenticação, dotado de diversas propriedades de segurança, além de assegurar baixa latência de *handover* em uma arquitetura de integração LTE-WLAN.

Palavras Chave: Redes Heterogêneas; Autenticação; Gerência de Mobilidade; PMIPv6; *Handover* Vertical; Latência de *Handover*.

ABSTRACT

With the growing evolution of wireless networking technologies, has been considered, in recent years, the integration and convergence of different network technologies, with specific capabilities and features, and favored by the existence of terminals with multiple interfaces, which can be served by heterogeneous networks. This integration enables the proffer of connectivity options to the users and an increase in coverage area, while a wide range of problems now requires solution, such as the selection of networks, integrated management of resources, congestion control, authentication and mobility management.

Heterogeneous networks (HetNet) constitute one of the pillars on which is based the 4ª and 5ª wireless network generation (4G and 5G, respectively), in which network based on multiple radio access technologies (RAT) must be integrated harmoniously, which requires adequate treatment of *handover*s, aiming at the desired continuity of services during and after the transition between different RATs. This treatment is highly dependent on the adequate solution of some of the problems cited, of which stand out, in this work, authentication and mobility management.

On the other hand, to meet the demand of various applications that has strict QoS (Quality of Service) requirements, such as those involving multimedia communications in real time, the mobile devices must exchange the lower number of messages on *handover*, which will be able to provide bandwidth savings and promote compliance with the QoS requirements.

This work evaluated the impact of recent authentication methods in a vertical *handover* between LTE and WLAN networks, interconnected by a core architecture of the EPC (Evolved Packet Core), regarding the *handover* latency and signaling, along with security aspects, such as key management and threat protection.

In conjunction with the authentication methods, it was used to PMIPv6 (Proxy MobileIPv6) protocol, adopted as a standard by 3GPP to provide mobility management on the interconnection of heterogeneous networks.

The performance evaluation was performed by analytical modeling in three different case studies. In the first case study, the *handover* latency was evaluated in a vertical *handover* scenario in the sense LTE→WLAN; this scenario is particularly important when considering the possibility of data offloading for congestion control in cellular networks. In the second case study the *handover* latency and signaling were evaluated in a horizontal *handover* scenario between WLANs networks where LTE network is the UE's home

network; this scenario also has a direct relationship with the possibility of data offloading. In the third case study was used the same scenario of the second case study, but considering other aspects of the analytical modeling.

The study and evaluation of authentication methods served as the basis for presentation of preliminary proposal of a new authentication protocol, having several security properties and ensuring low latency *handover* in a LTE-WLAN integration architecture.

Keywords: Heterogeneous Network; Authentication; Mobility Management; PMIPv6; Vertical *Handover; Handover* Latency.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

3GPP	*3rd Generation Partnership Project*
AAA	*Authentication, Authorization and Accounting*
AKA	*Authentication and Key Agreement*
AP	*Access Point*
AR	*Access Router*
AuC	*Authentication Centre (3GPP)*
BCE	*Binding Cache Entry*
CN	Nó Correspondente
CoA	*Care Of Address*
DSMIPv6	*Dual Stack Mobile IP version 6*
EAP	*Extensible Authentication Protocol (IETF)*
FA	*Foreign Agent*
FER	*Frame Error Rate*
GW	*Gateway*
HA	*Home Agent*
HNP	*Home Network Prefix*
HoA	*Home Address*
HSS	*Home Subscriber Server (3GPP)*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol (IETF)*
IPv6	*Internet Protocol version 6 (IETF)*
LMA	*Local Mobility Anchor*
LTE	*Long Term Evolution*
MAG	*Mobile Access Gateway*
MIPv6	*Mobile IP version 6 (IETF)*
MME	*Mobility Management Entity (3GPP)*
UE	*User Equipment (3GPP)*
UE-HNP	*Home Network Prefix do Móvel*
UE-ID	Identificador do Móvel
NEMO BS	*Network Mebility Basic Support (IETF)*

PBA	*Proxy Binding Acknowledgment*
PBU	*Proxy Binding Update*
PCC	*Policy and Charging Control*
PCRF	*Policy and Charging Rules Function (3GPP)*
PDN-GW	*Packet Data Network Gateway*
PMIPv6	*Proxy Mobile IP version 6*
QoS	*Quality of Service*
Rtr-Adv	*Router Advertisement*
RFC	*Request for Comments (IETF)*
Rtr-Sol	*Router Solicitation*
KDC	Centro de Distribuição de Chaves
SGW	*Serving Gateway (3GPP)*
SS7	*Signaling System number 7 (ITU-T)*
TCP	*Transport Control Protocol (IETF)*
UDP	*User Datagram Protocol (IETF)*
UMTS	*Universal Mobile Telecommunications System (3GPP)*
UTRAN	*UMTS Terrestrial Radio Access Network (3GPP)*
WLAN	*Wireless Local Area Network*
WiMAX	*Worldwide Interoperability for Microwave Access (IEEE)*
WWAN	*Wireless Wide Area Network*
AAA	Autenticação, Autorização e Accounting
HHO	*Handover* Horizontal
VHO	*Handover* Vertical
RADIUS	*Remote Authentication Dial In User Service*
APN	*Access Point Name*
HIU	*Hybrid Interconnection Unit*
SAE	*System Architecture Evolution*
CRA	*Coordinated Robust Authentication*
MAC	Código Autenticador de Mensagem

LISTA DE VARIÁVEIS

1) Variáveis relativas à interface aérea

1.a) 1º e 3º estudos de caso

μ_{UE}	Taxa de processamento de mensagens do terminal para rede WLAN
$\mu_{UE'}$	Taxa de processamento de mensagens do terminal para aplicação
μ_{AP}	Taxa de processamento de mensagens da rede WLAN para Internet
μ_{AP}'	Taxa de processamento de mensagens da rede WLAN para os terminais
λ_{UE}	Taxa de chegada de mensagens da aplicação para terminal
λ_{UE}'	Taxa de chegada de mensagens no terminal da rede WLAN
λ_{AP}	Taxa de chegada de mensagens na rede WLAN pelos terminais
λ_{AP}'	Taxa de chegada de mensagens na rede WLAN pelo AR
RTO_0	Valor inicial do temporizador de retransmissão do pacote
RTO_i	Valor do temporizador de retransmissão na i-nésima tentativa de transmissão do pacote
N_m	Número máximo de retransmissão
D	Atraso médio de propagação fim a fim do quadro sobre enlace WLAN
D'	Atraso médio para transmitir pacote com controle de retransmissão sobre interface WLAN
D_{UE}	Atraso de processamento/filas para o móvel
D_{AP}	Atraso de processamento/filas para o Access Point
D_{EAP}	Troca de mensagens EAP através da interface WLAN
p	Probabilidade de um quadro estar com erro no enlace aéreo
q	Taxa de perda de pacotes
τ	Tempo inter-quadro
c	Valor constante
k	Número de quadros do enlace aéreo contidos no pacote

1.b) 2º estudo de caso

W_{wl}	Taxas de dados dos meios sem fio
$D_{pp(wl)}$	Atrasos de propagação dos meios sem fio
$T_{prot\text{-}sem\text{-}fio}$	Atraso causado a um móvel no meio sem fio quando este realiza o *handover*

1.c) 2º e 3º estudos de caso

$D_{t(wl)}$	Atrasos de transmissão do meio sem fio

1.d) 3º estudo de caso

$T_{prot\text{-}sem\text{-}fio'}$	Atraso causado a um móvel no meio sem fio quando este realiza o *handover*

1.e) 1º, 2º e 3º estudos de caso

M_{wl}	Número de mensagens trocadas nos meios sem fio

2) Variáveis relativas à rede cabeada

2.a) 1º e 3º estudos de caso

μ_{WAAA}	Taxa de processamento de mensagens do servidor AAA da rede WLAN no sentido LTE
$\mu_{WAAA'}$	Taxa de processamento de mensagens do servidor AAA da rede WLAN no sentido do AR
μ_{AR}	Taxa de processamento de mensagens do Access Router no sentido do WAAA
$\mu_{AR'}$	Taxa de processamento de mensagens do Access Router no sentido do AP
$\mu_{PDN\text{-}GW}$	Taxa de processamento de mensagens do PDN-G no sentido do S-GW
$\mu_{PDN\text{-}GW'}$	Taxa de processamento de mensagens do PDN-G no sentido da rede WLAN
$\mu_{S\text{-}GW}$	Taxa de processamento de mensagens do S-GW no sentido do MME
$\mu_{S\text{-}GW'}$	Taxa de processamento de mensagens do S-GW no sentido do PDN-GW
μ_{MME}	Taxa de processamento de mensagens do MME no sentido do HSS
$\mu_{MME'}$	Taxa de processamento de mensagens do MME no sentido do S-GW

λ_{WAAA}	Taxa de chegada de mensagens no servidor AAA da WLAN pelo Access Router
$\lambda_{WAAA'}$	Taxa de chegada de mensagens no servidor AAA da WLAN pela rede LTE
λ_{HAAA}	Taxa de chegada de mensagens no servidor AAA da rede LTE pela WLAN
$\lambda_{HAAA'}$	Taxa de chegada de mensagens no servidor AAA da rede LTE pelo HSS
λ_{AR}	Taxa de chegada de mensagens no Access Router pelo Access Point
$\lambda_{AR'}$	Taxa de chegada de mensagens no *Access Router* pelo servidor de AAA da WLAN
λ_{PDN-GW}	Taxa de chegada de mensagens no PDN-GW pela WLAN
$\lambda_{PDN-GW'}$	Taxa de chegada de mensagens no PDN-GW pelo S-GW
λ_{S-GW}	Taxa de chegada de mensagens no S-GW pelo PDN-GW
$\lambda_{S-GW'}$	Taxa de chegada de mensagens no S-GW pelo MME
λ_{MME}	Taxa de chegada de mensagens no MME pelo S-GW
$\lambda_{MME'}$	Taxa de chegada de mensagens no MME pelo HSS
Δ_{SS7}	Atraso médio de mensagens na rede SS7
ΔHSS	Atraso médio de processamento para consulta ao HSS
D_{AR}	Atraso de processamento/filas para o Access Router
D_{AAA_WLAN}	Atraso de processamento/filas para o servidor de AAA da rede WLAN
D_{AAA_LTE}	Atraso de processamento/filas para o servidor de AAA da rede LTE
D_{HSS}	Atraso de processamento/filas para o HSS
D_{PDN-GW}	Atraso de processamento/filas para o PDN-GW
D_{S-GW}	Atraso de processamento/filas para o S-GW
D_{MME}	Atraso de processamento/filas para o MME

2.b) 2º estudo de caso

W_{wd}	Taxas de dados dos meios com fio
D_{AV}	Atraso gerado pelo HSS para a geração dos vetores de autenticação
$T_{prot-com-fio}$	Atraso causado a um móvel no meio com fio quando este realiza o *handover*

2.c) 2º e 3º estudos de caso

H_{wd}	Número de hops na rede cabeada
$D_{t(wd)}$	Atraso de transmissão dos meios com fio
$D_{pp(wd)}$	Atraso de propagação dos meios com fio

2.d) 3º estudo de caso

$T_{prot-com-fio'}$	Atraso causado a um móvel no meio com fio quando este realiza o *handover*

2.e) 1º, 2º e 3º estudos de caso

M_{wd}	Número de mensagens trocadas nos meios com fio

3) Variáveis relativas à interface aérea e rede cabeada

3.a) 1º estudo de caso

$D_{Prot-Aut}$	Latência de *handover* para determinado protocolos de autenticação

3.b) 2º estudo de caso

D_{pc}	Atraso de processamento em cada nó
LC	Latência de *handover* em todo o domínio das redes WLANs
SC	Sinalização de *handover* em todo o domínio das redes WLANs
$T_{prot.}$	Atraso causado a um móvel quando este realiza o *handover*
S_{prot}	Tamanho total das mensagens trocadas durante o *handover* de um determinado protocolo
$S_{prot-aut}$	Tamanho total das mensagens trocadas relativas a autenticação

$S_{prot-MM}$	Tamanho total das mensagens trocadas relativas ao gerenciamento de mobilidade

3.c) 2º e 3º estudos de caso

D_{ED}	Atraso relacionado à encriptação/decriptação
D_{MAC}	Atraso causado pelo cálculo e verificação de um código de autenticação de mensagem
D_{KEY}	Atraso induzido na derivação de chaves
D_{ID}	Atraso relacionado na geração de identificadores (ID)
$HO_{Rate-Dom}$	Taxa de *handover* para um domínio
TE_{prot}	Atrasos adicionais causados no protocolo
S_{prot}	Tamanho total das mensagens trocadas no *handover*
$S_{prot-aut}$	Tamanho total das mensagens relativas a autenticação
$S_{prot-MM}$	Tamanho total das mensagens realtivas ao gerenciamento de mobilidade
HO_{Rate}	Taxa de *handover* por célula
n	Número de usuários por célula
v	Velocidade média do móvel
B	Número de células no domínio das redes WLANs
R	Círculo virtual representando o domínio das redes WLANs
a	Lado da célula hexagonal

3.d) 3º estudo de caso

LC’	Latência de *handover* em todo o domínio das redes WLANs
SC ‘	Sinalização de *handover* em todo o domínio das redes WLANs

3.e) 1º, 2º e 3º estudos de caso

Avg M_{prot}	Tamanho médio das mensagens de determinado protocolo
$N_{msg-prot}$	Número de mensagens totais trocadas por determinado protocolo
$N_{msg-aut-tot}$.	Número de mensagens totais relativas a autenticação trocadas
Avg $M_{prot-aut}$	Tamanho médio das mensagens de autenticação de determinado protocolo
$N_{msg-MM-tot}$.	Número de mensagens totais relativas ao gerenciamento de mobilidade trocadas
Avg $M_{prot-MM}$	Tamanho médio das mensagens de gerenciamento de mobilidade de determinado protocolo

1 – INTRODUÇÃO

A evolução no campo das telecomunicações tem permitido um aumento considerável do emprego de novos serviços de comunicações móveis pelos usuários finais, dentre os quais será destacado os serviços de dados multimídia em tempo real, como as transmissões de vídeo pela internet e VoIP (Voz sobre IP).

Diversas tecnologias de redes sem fio coexistem nos dias de hoje, cada uma com vantagens específicas para certos tipos de serviço, como altas taxas de dados, ampla cobertura e baixo custo de implementação, dentre outras. A interconexão entre redes sem fio distintas proporciona às operadoras de telefonia móvel suprir as desvantagens de uma determinada rede com as vantagens de outra rede, criando uma única infraestrutura robusta e eficiente.

A integração de redes de acesso sem fio com tecnologias de acesso diferentes se baseia no conceito de redes sem fio heterogêneas. Uma rede sem fio heterogênea consiste de um conjunto de duas ou mais redes com tecnologias de acesso e-ou arquiteturas diferentes, interconectadas com o objetivo de aumentar a capacidade, cobertura e o desempenho de redes móveis.

Com a recente popularização das redes LTE e WLAN, a integração destas duas redes sem fio está em crescente evolução. Assim também, com o grande aumento de dispositivos móveis, as operadoras de telefonia móvel estão buscando alternativas para se evitar gargalos e diminuir custos com infraestrutura de rede. Uma ótima alternativa encontrada é a interconexão das redes LTE e WLAN, pois as redes WLANs oferecem alta taxa de transferência de dados a um custo com infraestrutura baixo, se comparado às redes do padrão LTE.

Apesar de a integração entre as redes LTE e WLAN ter se mostrado uma ótima alternativa, aspectos como segurança, latência de *handover* e gerenciamento de mobilidade ainda tem sido o foco de diversos trabalhos, a fim de se desenvolver redes mais eficientes.

1.1– MOTIVAÇÃO

Alguns tipos de serviços, principalmente os baseados em comunicações multimídias,

possuem requisitos de tempo real cujo atendimento é de grande importância para o adequado provimento com níveis mínimos de QoS (do inglês, *Quality of Service*), que constituirão fatores determinantes para uma adequada QoE (do inglês, *Quality of Experience*) por parte do usuário. Tais serviços são impactados em sua qualidade por diferentes aspectos atinentes à operação e funcionamento de redes sem fio (tais como desvanecimento, perdas de quadros e desconexões), bem como por outros, dentre os quais destaca-se aqui os atrasos, por representarem um fator que pode contribuir de maneira significativa para um baixo nível de QoS e, por conseguinte, um baixo nível de QoE.

Em se tratando de redes heterogêneas, e mais especificamente de uma rede integrada LTE-WLAN, um dos processos que comumente impõe atrasos é o de *handover* vertical, face à necessidade de garantir que, em uma dada área de cobertura, uma ou mais novas redes terão sido descobertas, em seguida uma determinada rede terá sido selecionada e, após autenticação tanto na rede origem quanto na rede destino e procedimentos de estabelecimento de conexão na nova rede, ocorrerá a recepção segura de pacotes pela nova interface. Dentre os processos mais onerosos em termos de trocas de mensagens, ocasionando uma lentidão no processo de *handover*, destaca-se a autenticação.

O *3rd Generation Partnership Project* (3GPP) define como protocolo padrão para uso em *handovers* no LTE o protocolo *Extensible Authentication Protocol - Authentication* and *Key Agreement* (EAP-AKA), descrito em [1], porém o grande problema desse protocolo é o grande número de mensagens trocadas para autenticar o móvel, juntamente com algumas falhas de segurança que o tornam vulnerável a ataques. Esse grande número de mensagens leva, naturalmente, a um atraso que pode causar redução dos níveis de QoS e de QoE.

Para contornar esses problemas da elevada latência de *handover* e de segurança em uma interconexão LTE-WLAN, o foco de diversos recentes trabalhos envolve métodos de autenticação que possuem baixa latência de *handover* e sejam seguros.

1.2– OBJETIVOS

1.2.1 - Objetivo Geral

Este trabalho tem por objetivo principal responder à seguinte pergunta de pesquisa: como os protocolos de autenticação existentes ou propostos impactam a latência e a

sinalização de *handover* entre redes heterogêneas?

1.2.2 - Objetivos Específicos

- Caracterizar alguns dos principais protocolos de autenticação para redes heterogêneas, especialmente LTE-WLAN;

- Apresentar proposta preliminar de um protocolo seguro e caracterizado por uma baixa latência de *handover* em uma arquitetura de integração LTE-WLAN;

- Avaliar o desempenho do protocolo proposto, em comparação com o de recentes protocolos de autenticação propostos para utilização em redes heterogêneas;

- Caracterizar e comparar aspectos de gerenciamento de chaves e de propriedades de segurança do protocolo proposto e dos demais protocolos de autenticação.

1.3 - JUSTIFICATIVA

A integração de redes sem fio constitui uma forte tendência nos últimos anos, face à proliferação de padrões oriundos de diferentes organizações normativas, voltados comumente para diferentes tecnologias de acesso, ao mesmo tempo em que terminais multimodo estão disponíveis com relativa facilidade.

Ao tempo em que essa integração pode se mostrar útil para um melhor aproveitamento de capacidades e funcionalidades específicas de cada rede (como ocorre, por exemplo, em estratégias de *data offloading*), observa-se que os procedimentos de autenticação podem produzir atrasos às vezes elevados e indesejados, que podem se traduzir em redução da qualidade da experiência percebida pelos usuários, especialmente aqueles que estejam fazendo uso de serviços que envolvam tráfego de tempo real (como os baseados em comunicações multimídias).

Os protocolos de autenticação possuem interação direta com os mecanismos de gerenciamento de mobilidade (MM, do inglês *Mobility Management*); assim, os protocolos construídos para tratar a movimentação dos terminais entre redes integradas são utilizados

considerando pelo menos uma das principais opções de protocolos para MM, tais como DSMIPv6, PMIP e GTP.

Por outro lado, as redes sem fio (RSF) de 4a e 5a gerações pressupoõem a integração de redes heterogêneas (HetNets), dessa forma a adequada implantação das mais recentes gerações de RSF certamente não será bem sucedida, no tocante à segurança, sem uma boa escolha e uma boa definição de protocolos de autenticação, cujo desempenho deve ser judiciosamente avaliado.

1.4 – METODOLOGIA

A partir da definição do tema e de um problema de pesquisa, foi realizado o estudo de conceitos julgados importantes para o entendimento do tema, seguido de levantamento e revisão bibliográfica, que permitiu identificar propostas recentes, especialmente em termos de protocolos de autenticação aplicados a redes heterogêneas, com foco precípuo em redes LTE e WLAN. Foram também verificadas as normas providas por organizações como o ETSI e o 3GPP, visando assegurar interoperabilidade com sistemas tratados por aquelas entidades.

Por delimitação de escopo, considerou-se que alguns problemas, apesar de intimamente ligados ao tema da dissertação, não foram tratados de forma explícita, como por exemplo, os de descoberta e seleção de redes, roteamento, alocação de recursos, controle de congestão, modelagem de confiança computacional, dentre outros.

Trata-se aqui de um trabalho de pesquisa aplicada, para o qual foram utilizados dados obtidos tanto de forma experimental, colhidos em operação de redes reais, quanto dados estimados, obtidos analiticamente, ou simplesmente adotados com base em referências já publicadas.

A avaliação de desempenho dos protocolos foi tratada por meio de modelagem analítica em três estudos de casos. No primeiro estudo de caso foi avaliada a latência de *handover*, em um cenário de *handover* vertical no sentido LTE → WLAN; tal cenário é particulamente importante ao se considerar a possibilidade de *data offloading* para controle de congestão nas redes celulares. No segundo estudo de caso foram avaliadas a latência e a sinalização de *handover* em um cenário de *handover* horizontal entre redes WLANs em que a rede LTE é a rede caseira do móvel; tal cenário também possui relação direta com a

possibilidade de *data offloading*. No terceiro estudo de caso utilizou-se o mesmo cenário do segundo estudo de caso, mas considerando outros aspectos relativos à modelagem analítica. Foi realizada a avaliação da latência de *handover,* pois este parâmetro está diretamente relacionado com a QoS associada de certas aplicações.

O estudo e a avaliação dos diversos métodos de autenticação serviram como base para a apresentação de proposta de um novo protocolo de autenticação, dotado de diversas propriedades de segurança, além de assegurar baixa latência de *handover* em uma arquitetura de integração LTE-WLAN.

1.5– CONTRIBUIÇÕES (RESULTADOS OBTIDOS)

Os seguintes resultados foram obtidos ao longo da presente dissertação:

1) Publicação de 2 (dois) artigos em conferências internacionais;

2) Submissão de artigo para periódico de bom fator de impacto;

3) Caracterização dos principais protocolos de autenticação para redes heterogêneas (especialmente LTE-WLAN), tanto os já padronizados quanto outros recentemente publicados;

4) Proposta preliminar de um protocolo seguro e que apresente uma baixa latência de *handover* em uma arquitetura de integração LTE-WLAN;

5) Avaliação do desempenho do protocolo proposto, em comparação com o de recentes protocolos de autenticação propostos para utilização em redes heterogêneas, visando *handover* vertical LTE-WLAN;

6) Avaliação do desempenho do protocolo proposto, em comparação com o de recentes protocolos de autenticação propostos para utilização em redes heterogêneas, visando *handover* horizontal entre WLAN´s controladas pelo núcleo de uma rede LTE;

7) Levantamento de valores mais comuns relativos a parâmetros passíveis de adoção

em modelagens de redes sem fio;

8) Caracterização e comparação de aspectos de gerenciamento de chaves e de propriedades de segurança do protocolo proposto e dos demais protocolos de autenticação.

1.6– ORGANIZAÇÃO

O documento está organizado da seguinte forma: no Capítulo 2 é apresentada uma visão geral sobre a tecnologia *Long Term Evolution* (LTE), considerando aspectos arquiteturais e de características dessas tecnologias.

O Capítulo 3 é dedicado ao estudo da integração entre as redes LTE e WLAN, apresentando aspectos de arquitetura, autenticação, gerenciamento de mobilidade e fluxos de mensagens em *handovers* entre essas redes.

O Capítulo 4 apresenta os trabalhos relacionados, que serão tomados como base para o projeto a ser desenvolvido. Adicionalmente, é apresentado um detalhamento de recentes métodos de autenticação utilizados em redes heterogêneas do tipo LTE-WLAN.

A proposta preliminar do protocolo é descrita no Capítulo 5, apresentando o fluxo de mensagens, formato de mensagens, procedimentos de autenticação, procedimentos de desconexão e comparações com o fluxo original.

São realizados três estudos de caso no capítulo 6, apresentando uma análise e discussão detalhada em termos de latência e sinalização de *handover*, bem como de propriedades de segurança.

Por fim, no Capítulo 7, são descritas as conclusões e propostas para trabalhos futuros.

2 – LONG TERM EVOLUTION

Neste Capítulo, será feita uma discussão sobre os aspectos arquiteturais e a evolução das redes LTE (acrônimo de *Long Term Evolution*). Serão descritos aqui seus principais componentes (rede de núcleo e rede de acesso), bem como as interfaces e algumas características desse padrão produzido pelo 3GPP. A ênfase da apresentação é bem reduzida em relação à camada física do padrão.

2.1 – INTRODUÇÃO

Na busca de soluções para tornar a transmissão de dados mais eficiente, enquanto o volume de tráfego desses dados encontra-se em ascensão, o padrão LTE, foi desenvolvido como uma evolução das redes 3G com as seguintes motivações [2]:

- Necessidade de assegurar a competitividade dos sistemas de comunicações móveis para o futuro;

- Demanda por altas taxas de dados e qualidade do serviço;

- Necessidade da redução de custos;

- Arquitetura simplificada.

Esta tecnologia, apresentada a partir do *release* 8 pelo 3GPP, é uma evolução das redes GSM/EDGE e UMTS/HSPA, porém com uma alta eficiência espectral e altas taxas de transmissões, taxas de transmissão de dados teóricas de 300 Mb/s de *downlink* e 75 Mb/s de *uplink* [2]. No LTE *Advanced* (LTE-A), essas taxas são de 3 Gb/s no *downlink* e de 1,5 Gb/s no *uplink.*

O LTE é baseado em OFDMA (*Orthogonal Frequency Division Multiple Access*) para *downlink* e em SC-FDMA (*Single Carrier - Frequency Division Multiple Access)* para *uplink,* em combinação com modulações QPSK, 16 QAM e 64 QAM no *downlink,* e BPSK, QPSK, 8PSK e 16 QAM no *uplink,* grandes larguras de banda (até 20 MHz) e multiplexação espacial no *downlink* [2].

2.2–ARQUITETURA

Nesta seção será feita uma descrição da arquitetura SAE (*System Architecture Evolution*), definida pelo 3GPP no Release 8, arquitetura de rede projetada com baixa complexidade, com poucos elementos, otimização do desempenho da rede, suporte a vários tipos de redes de acesso sem fio, como LTE, WLAN, UMTS, e suporte à mobilidade entre redes de acesso heterogêneas. De acordo com [4], esta arquitetura é formada por uma rede de núcleo, chamada de *Evolved Packet Core Network* (EPC) e as demais possíveis redes de acesso que podem se acoplar com esta arquitertura, como por exemplo, a rede de acesso E-UTRAN e a WLAN. Em uma arquitetura SAE, a junção da rede E-UTRAN com a rede de núcleo EPC é chamada de *Evolved Packet System* (EPS).

2.2.1– Rede de Acesso

A arquitetura SAE possui suporte a vários tipos de redes de acesso; esta subseção irá tratar sobre a *Evolved Universal Terrestrial Radio Access Network* (E-UTRAN), que é a rede de acesso projetada para as redes LTE, como mostrada na Figura 2.1:

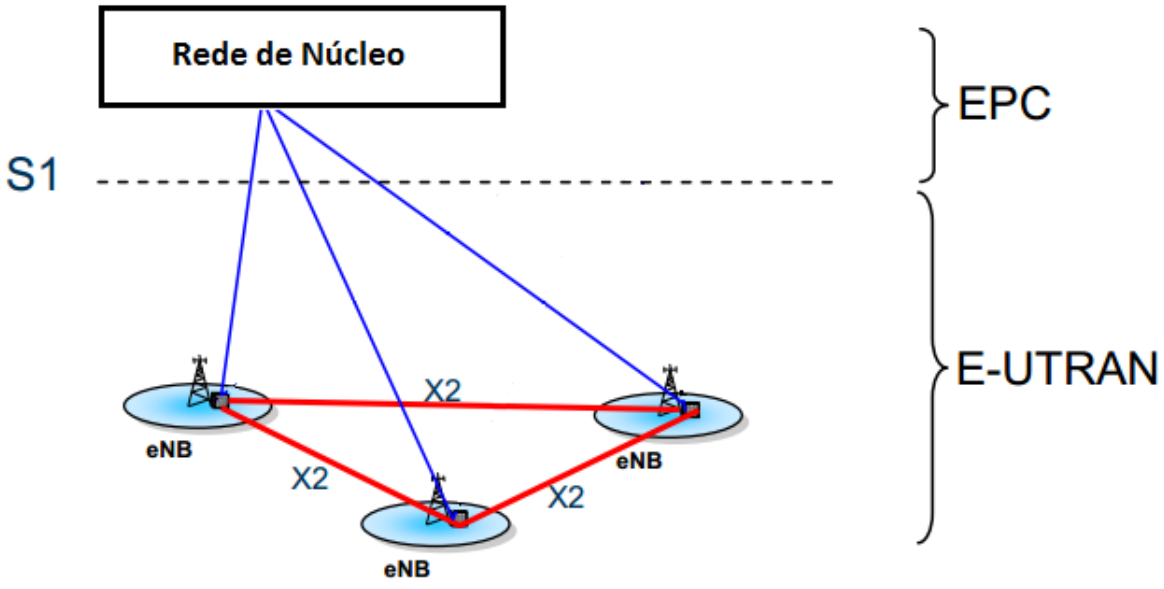

Figura 2.1 – *Arquitetura da rede LTE* (Baseado em [3]).

Esta subseção irá tratar apenas da rede de acesso E-UTRAN, deixando para detalhar a rede EPC em uma subseção posterior.

Além dos terminais móveis (UE, do inglês *User Equipment*), os únicos elementos contidos na E-UTRAN são as estações base, conhecidas como eNBs (do inglês, *evolved Node Bs*) para macro-células e HeNBs (do inglês, *Home-eNBs*) para femto-células. Doravante, será referido apenas como eNB de forma genérica. A eNB é uma estação base que age como uma *bridge* de camada 2 entre o dispositivo móvel (UE) e a EPC. A eNB realiza ciframento e deciframento dos dados referentes ao *User Plane* (tráfego de dados do usuário) e também compressão e descompressão de cabeçalhos IPs.

A eNB também é responsável por funções relativas ao *Control Plane* (sinalização do sistema). A eNB é responsável também pelo *Radio Resource Management* (RRM), isto é, controle do uso de recursos da interface rádio. Dentre essas funções, pode-se citar o controle do fluxo de dados de acordo com as necessidades requeridas de QoS e o constante monitoramento do uso dos recursos da interface de rádio. A eNB também participa na troca de mensagens com o EPC referentes à gerência de mobilidade do UE e na troca de mensagens com outras eNBs durante o *handover*s. A Figura 2.2 ilustra as funções da eNB já citadas nesta subseção, bem como outras: configurações de segurança, segurança e otimização da entrega de dados na interface rádio, entrega de dados para o plano do usuário e algumas funções relativas ao *User Plane*.

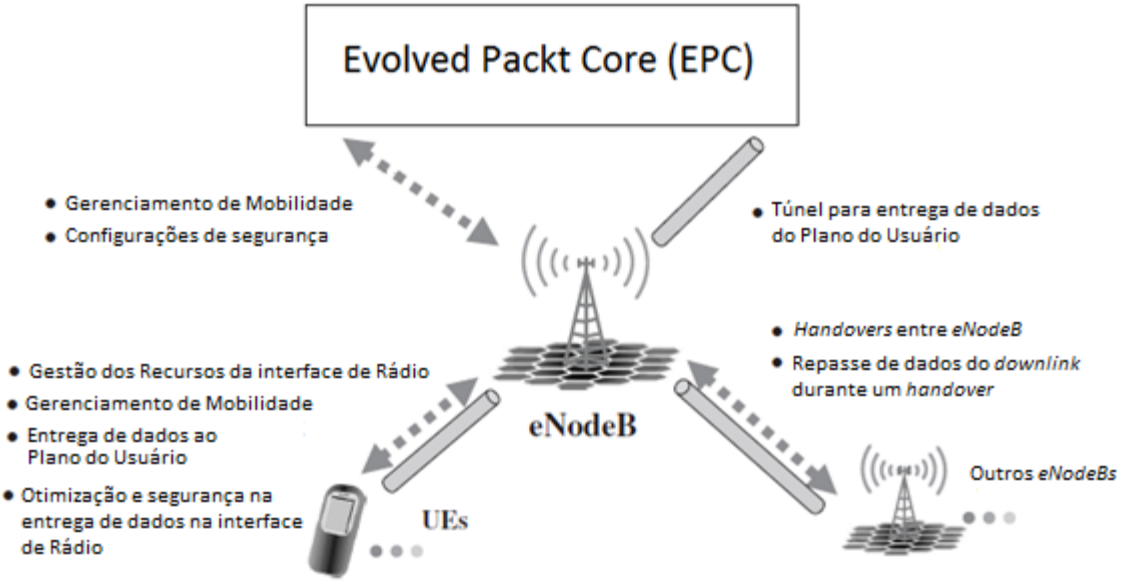

Figura 2.2 – Principais funções e conexões da eNB (Baseado em [4]).

2.2.2 –*Evolved Packet Core*

O EPC foi projetado para ser uma arquitetura com poucos elementos e com um eficiente desempenho em termos de tráfego de dados. Outra vantagem desta arquitetura é a separação entre os tráfegos pertencentes ao *User Plane* e ao *Control Plane*, tornando-se mais fácil o dimensionamento e a adaptação da rede por parte do operador. A Figura 2.3 ilustra os elementos da arquitetura SAE com suas respectivas interfaces:

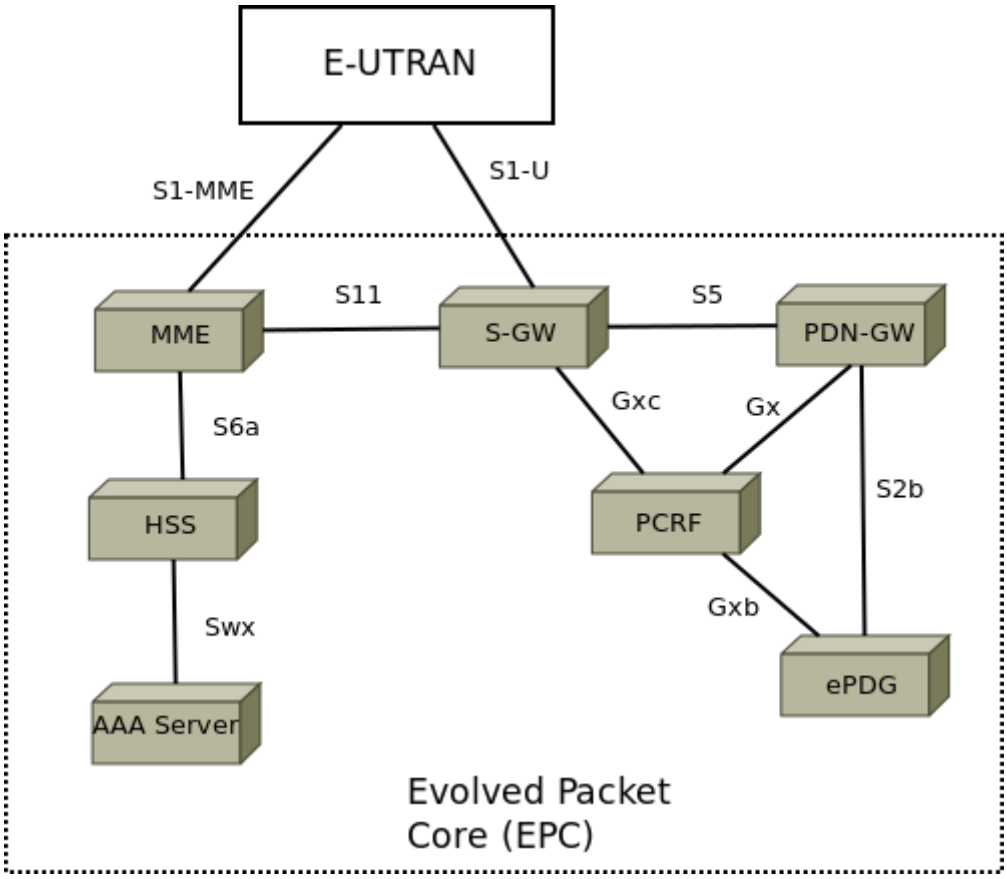

Figura 2.3 – *Evolved Packet Core* e interfaces com E-UTRAN (baseado em [5] e [6]).

Esta arquitetura apresenta os seguintes elementos:

- *Mobility Management Entity* (MME): principal elemento de controle da rede EPC, operando apenas no *Control Plane*, não participando das trocas de mensagens relativas ao *User Plane*. De acordo com [4] e [5], este elemento tem por funções a autenticação e autorização do UE, interceptação de tráfego de sinalização e transferência de mensagens de controle, gerenciamento de perfil de usuário, conectividade de serviço, sinalizações

relativas à *Non-Access-Stratum* (NAS), ou seja, sinalizações relativas aos protocolos que não fazem parte da rede de acesso e etc.

- *Home Subscription Server* (HSS): base de dados que contém informações relativas aos assinantes e usuários da rede. O HSS inclui funções de gerenciamento de mobilidade e de autenticação e autorização de acesso a usuários;

- *AAA Server*: servidor responsável pelas funções de autenticação, autorização e *accounting*;

- *Policy and Charging Rules Function* (PCRF): responsável pelo PCC – *Policy and Charging Control*. O PCRF decide quando e como se deve gerenciar os serviços em termos de QoS. Desta forma, políticas adequadas podem ser configuradas para um determinado serviço;

-*Serving Gateway* (SGW): O SGW roteia e repassa os pacotes referentes ao *User Plane* e também exerce importante função no gerenciamento de mobilidade, neste caso atuando na troca de dados relativas ao *Control Plane;*

- *PDN Gateway* (PDN-GW): é um elemento que provê conectividade do UE para redes de pacotes externas. O PDN-GW realiza aplicações de políticas da rede, filtragem de pacotes para cada usuário e uma importante função no gerenciamento de mobilidade do móvel;

- *Evolved Packet Data Gateway* (ePDG): elemento que possui função principal de propiciar uma comunicação segura entre a rede EPC e uma rede *untrusted* (que não há uma associação de segurança prévia entre os elementos da rede EPC e da rede não 3GPP) que não seja do padrão 3GPP.

2.3 – LTE ADVANCED

A partir do release 10 do LTE, o 3GPP propôs um conjunto de melhorias naquele sistema de rede, que passou a ser referenciado como LTE *Advanced* (LTE-A). O LTE-A foi desenvolvido para ter total compatibilidade com o LTE; nesse sentido, tem-se que uma

base station do LTE-A pode controlar uma *base station* do LTE e vice e versa, provavelmente sem perda de desempenho [7].

Uma das mudanças propostas no LTE-A é o uso da técnica de *Carrier Aggregation* (CA) para o aumento da largura de banda, gerando assim um aumento da taxa de transmissão de pacotes. Outra mudança no LTE-A foi a evolução das técnicas de MIMO, permitindo utilizar 8x8 no *downlink* e 4x4 no *uplink.*

Em termos arquiteturais, foram inseridos repetidores nas redes de acesso para permitir que o sinal seja amplificado em regiões onde o sinal não possui boa qualidade, como regiões próximas às bordas da célula. A Figura 2.4 ilustra o funcionamento de um repetidor:

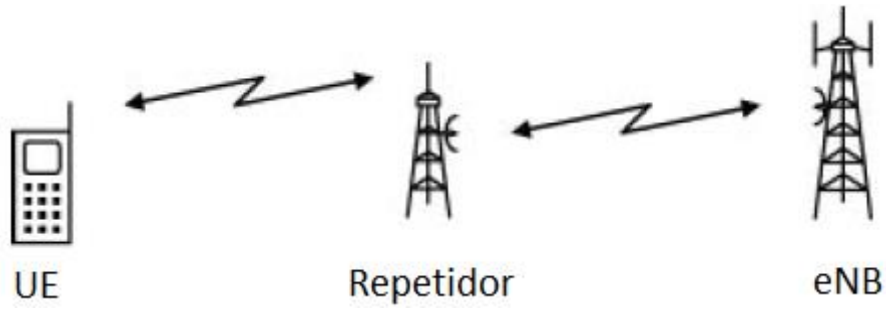

Figura 2.4 – Operação de repetidores [7].

Verifica-se que as principais modificações ocorridas no LTE-A em relação ao LTE foram relativas à camada física do citado padrão, mantendo as características da rede de núcleo e suas funções relativas ao *Control Plan* como gerenciamento de mobilidade e segurança.

2.4 – CONSIDERAÇÕES FINAIS

Este Capítulo apresentou uma breve descrição sobre o padrão de redes 4G *Long Term Evolution* (LTE). Foi apresentada a arquitetura SAE (*System Architecture Evolution*), arquitetura base para as redes LTE, e suas redes de acesso e núcleo, representadas pela E-UTRAN e pelo *Evolved Packet Core* (EPC), respectivamente. O estudo do padrão LTE e da arquitetura SAE serão de suma importância para este trabalho, pois serão utilizados diretamente nos estudos de casos apresentados no Capítulo 6. Por fim, foi apresentado o padrão LTE-*Advanced* (LTE-A), uma das evoluções recentes das redes LTE.

3 – REDES HETEROGÊNEAS

Este Capítulo será focado na integração das redes LTEs e WLANs, com foco inicialmente em conceitos associados a essa integração, bem como na apresentação de arquitetura para interconexão LTE-WLAN.

O Capítulo também apresenta protocolos propostos ou adotados por organizações normativas, para autenticação e gerenciamento de mobilidade em redes heterogêneas, com foco predominante nas redes LTE e WLAN. Por fim, são apresentados os fluxos de mensagens em um *handover* no sentido LTE→WLAN com o uso dos protocolos PMIPv6 e DSMIPv6.

3.1 – INTRODUÇÃO

A evolução das redes sem fio tem levado ao aparecimento de diversos padrões, com base em diferentes tecnologias de acesso, levando ao conceito de redes de acesso heterogêneas, baseadas na integração de diferentes redes sem fio.

A convergência destas redes vem para unificar e criar uma única infraestrutura inteligente e eficiente baseada na integração provida por essas redes de acesso heterogêneas. Entre as diversas vantagens das redes heterogêneas podem-se citar algumas como:

- Aumento da área de cobertura das redes;
- Possível diminuição do custo de serviços para usuários;
- Disponibilização de novos serviços por parte das operadoras;
- Possibilidade de maior eficiência em termos de QoS aos usuários.

Em termos de arquiteturas de redes heterogênas, existem dois tipos: as fracamente e as fortemente acopladas. Em uma arquitetura fracamente acoplada existe uma independência entre as redes, a troca de sinalização é feita através do núcleo de uma das redes, normalmente a rede caseira do móvel, porém, o fluxo de dados é encaminhado diretamente para a outra rede. No caso de redes fortemente acopladas, uma das redes está intimamente

ligada ao núcleo da outra rede, fazendo com que o tráfego de sinalização e de dados sejam sempre roteados para o núcleo de uma das redes. Existem muitas vantagens em redes fracamente acopladas, como a independência na implantação e no tráfego das redes envolvidas, bem como na implementação dessa interconexão, em que se torna mais simples o gerenciamento das redes [12].

Outro conceito importante em redes heterogênas envolve os vários tipos de *handovers*. Quando ocorre um *handover* entre redes usando uma mesma tecnologia de acesso diz-se que é um *handover* horizontal (HHO), e quando ocorre um *handover* entre redes usando tecnologias de acessos diferentes diz-se que é um *handover* vertical (VHO). Pode-se também classificar os *handovers* verticais como VHO para baixo em que se migra de uma rede de maior cobertura (por exemplo, uma WWAN) para uma de menor cobertura (por exemplo, uma WLAN) e tem-se também o VHO para cima quando a migração ocorre em direção inversa [12].

3.2 – INTERCONEXÃO DE REDES LTE E WLAN

Uma das interconexões mais usuais nos dias de hoje é a realizada entre redes LTE e WLAN. Um dos motivos de se fazer essa integração é devido ao crescente aumento do número de dispositivos móveis multimodo (múltiplas interfaces), com isso, buscando-se alternativas para se evitar gargalos nas redes celulares. As redes LTEs e WLANs também possuem características antagônicas que favorecem a sua integração, pois as redes LTEs provêem uma ampla área de cobertura, porém com uma taxa de transferência de dados relativamente baixa. Por outro lado, as redes WLANs provêem uma alta taxa de transferência de dados, mas com uma área de cobertura bastante limitada. Outro fator relevante para a integração dessas duas redes de acesso sem fio é o fator custo. Para a implementação da uma rede WLAN, o custo com infraestrutura é muito mais baixo se comparado a uma rede do tipo LTE.

3.2.1- Arquitetura para integração LTE-WLAN

O 3GPP, na norma TS 23.402 [9], traz detalhadamente aspectos relativos à integração de uma rede que não seja do padrão 3GPP com uma rede do padrão 3GPP por meio da rede de núcleo SAE. A Figura 3.1 ilustra a integração de uma rede LTE com uma rede WLAN:

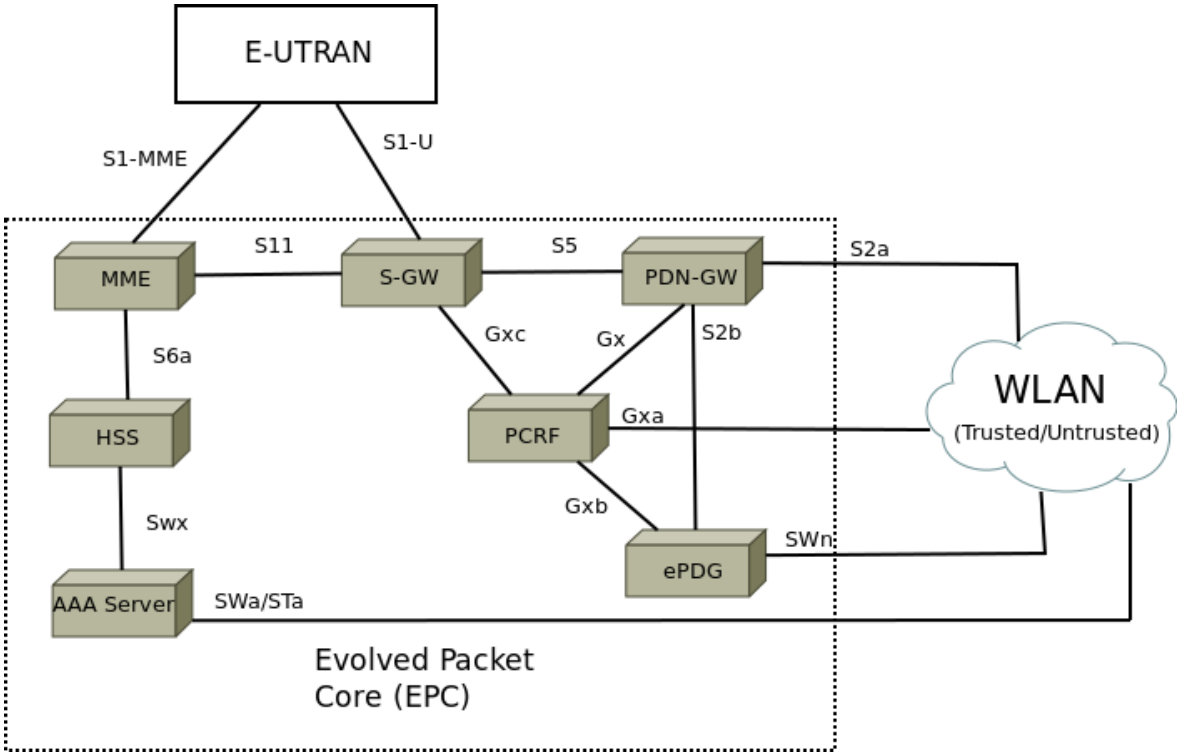

Figura 3.1 – Arquitetura de integração LTE-WLAN (baseado na Figura 4.2.1-1 de [9]).

Neste caso, a rede WLAN pode ser do tipo *trusted* ou *untrusted*, ou seja, os elementos de rede da WLAN podem ou não ter uma prévia associação de segunraça com a EPC. Quando a WLAN for do tipo *untrusted*, esta se conecta apenas com o AAA *server* e com o ePDG por meio das interfaces SWa e Swn, respectivamente. Por outro lado, quando a WLAN é do tipo *trusted* as conexões são realizadas pelo AAA *server*, PDN-GW e PCRF por meio das interfaces STa, S2a e Gxa, respectivamente. A norma TS 23.402 não especifica quais elementos deverão conter na rede WLAN, porém na literatura é amplamente utilizado um AAA *server* na rede WLAN para se conectar com o AAA *server* da rede 4G e um *Access Router* (AR) que se conecta com os demais elementos da rede 4G.

3.3 – AUTENTICAÇÃO EM UMA INTEGRAÇÃO LTE-WLAN

3.3.1 – *Extensible Authentication Protocol*

O *Extensible Authentication Protocol* (EAP) é um *framework* de autenticação definido na RFC 3748 [14] e com sua versão atualizada pela RFC 5247 [15]. O EAP é executado

diretamente na camada de enlace e possui suporte a uma grande variedade de mecanismos de autenticação.

O protocolo EAP foi desenvolvido para ser utilizado em enlaces dedicados ou em circuitos comutados, bem como em redes com ou sem fio. Os padrões IEEE 802.1x e 802.11i para redes cabeadas e sem fio, respectivamente, são baseados no protocolo EAP. Outra característica do EAP é o fato deste protocolo possuir seu próprio mecanismo de retransmissão, porém não suporta fragmentação e remontagem de pacotes recebidos fora de ordem.

O pacote EAP possui quatro tipos de campos, como mostrado na Figura 3.2:

- Código (1 byte) – É utilizado para identificar qual o tipo do pacote EAP, sendo que quatro códigos são designados a este campo: *Request* (1), *Response* (2), *Success* (3) e *Failure* (4).

- Identificador (1 byte) –Tem por finalidade sincronizar requisições e respostas.

- Comprimento (2 bytes) –Indica o comprimento em bytes do pacote EAP como um todo, considerando os campos código, identificador, c omprimento e dados.

- Dados – Campo com tamanho variável, podendo ter zero byte ou mais, dependendo do tipo do pacote, definido no campo código.

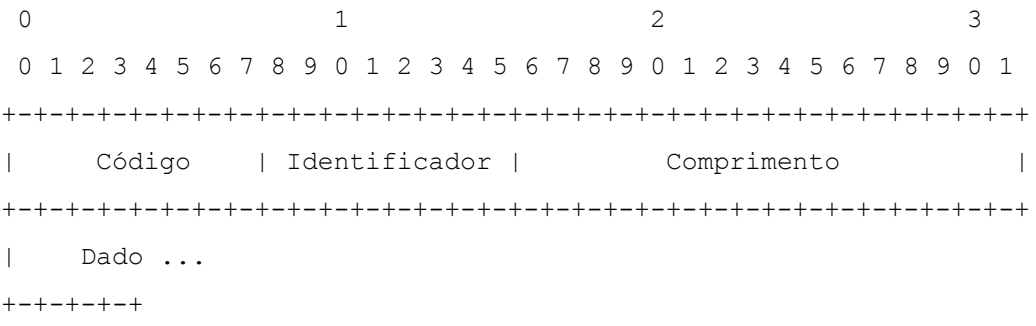

Figura 3.2 – Pacote EAP (Baseado em [14]).

As autenticações baseadas no EAP são sempre iniciadas pelo autenticador (quem autentica) e não pelo suplicante (quem deseja autenticar-se), diferentemente de outras propostas de autenticação. Independentemente do método de autenticação utilizado em

conjunto com o EAP, as seguintes mensagens genéricas sempre irão ser trocadas entre o suplicante e o autenticador, como mostrado na Figura 3.3:

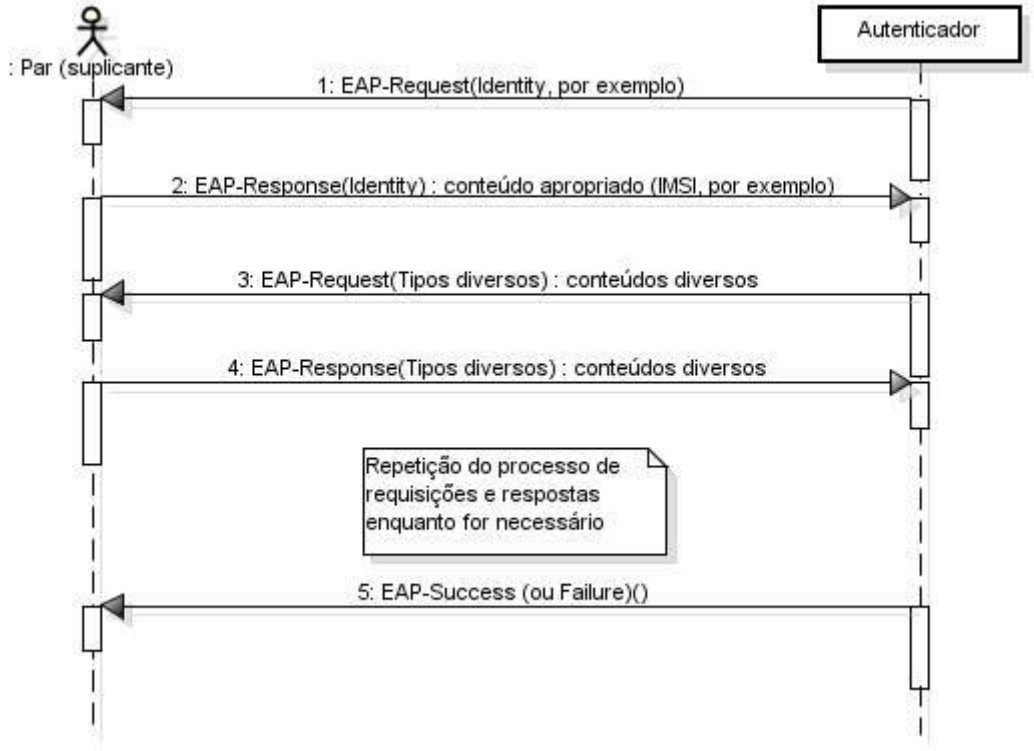

Figura 3.3 – Troca de mensagens genéricas do protocolo EAP [13].

A seguir é realizada a descrição dos eventos:

1 - O autenticador envia uma solicitação de autenticação ao suplicante, requisitando algum parâmetro de autenticação, como por exemplo, o ID do suplicante;

2 – O suplicante responde com a mensagem adequada ao tipo de autenticação solicitada;

3 e 4 –São trocadas diversas mensagens de requisição (*EAP-Request*) e resposta (*EAP-Response*) entre o suplicante e o autenticador, denpendendo do método de autenticação que se esteja utilizando em conjunto com o protocolo EAP.

5 – Por fim, o autenticador irá decidir se o processo de autenticação foi bem sucedido ou não e enviará um pacote sinalizando o resultado (sucesso ou falha).

3.3.2 – RADIUS

O RADIUS (*Remote Authentication Dial In User Service*) é um protocolo definido na RFC 2865 [16] com a finalidade de transportar mensagens relativas às funções de AAA (Autenticação, Autorização e *Accounting*). O RADIUS permite que um servidor de acesso de rede possa acessar um servidor centralizado e compartilhado para buscar serviços de AAA [17].

De acordo com [18] e [19], o protocolo RADIUS tem por funções prover:

- Autenticação: determinar a identidade de um usuário com base em um método de autenticação.

- Autorização: permitir ou rejeitar o acesso do usuário a um determinado serviço ou a rede de acordo com as poíliticas de segurança.

- Configuração de *host*: fornecer dados de configurações aos usuários conectados ao servidor de acesso à rede.

- Contabilização (*Accounting*): levantamentos estatísticos para fins de contabilização.

O RADIUS se encontra na camada de aplicação e utiliza o UDP (*User Datagram Protocol*) como protocolo da camada de transporte. A Figura 3.4 representa uma típica mensagem de autenticação e autorização entre um cliente e um servidor RADIUS. Por questões de simplicidade, foram omitidas entidades intermediárias.

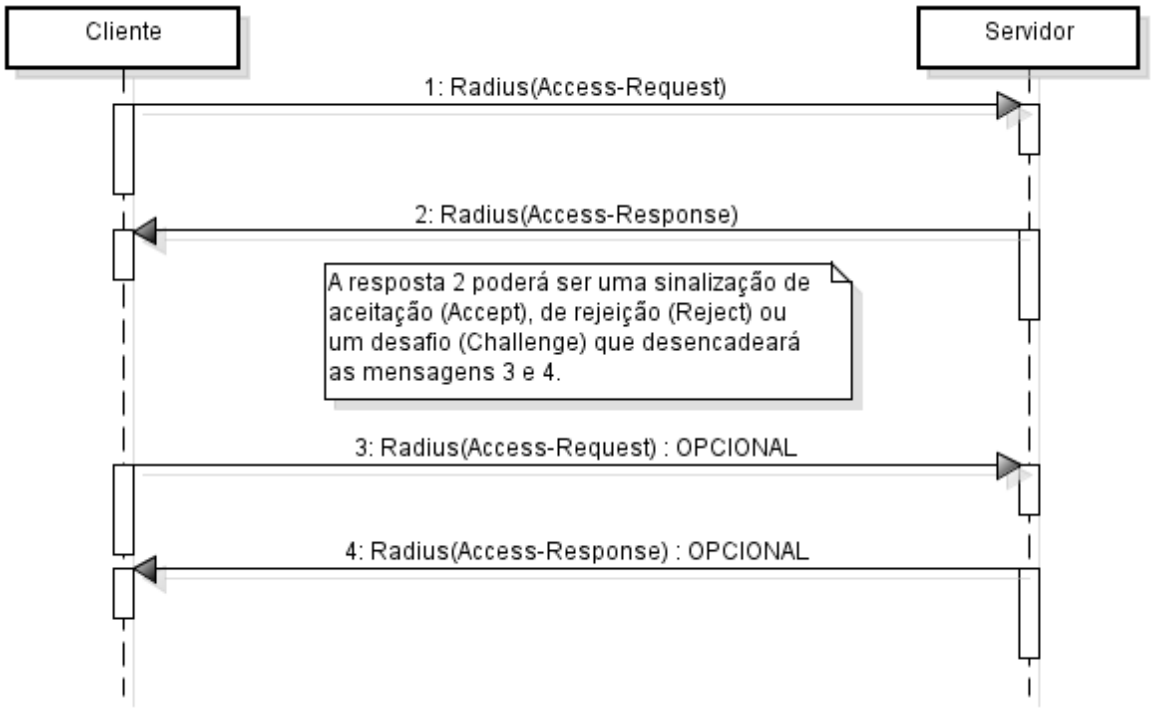

Figura 3.4 – Troca de mensagens de autenticação e autorização RADIUS [19].

A seguir é mostrada a descrição dos eventos:

1 – O Cliente solicita uma conexão, enviando parâmetros de segurança ao Servidor de AAA;

2 – Com base nos parâmetros recebidos, o Servidor de AAA irá decidir se deve ou não conceder acesso a este Usuário. A resposta pode ser de aceitação, de rejeição ou então uma mensagem-desafio, dependendo do método de autenticação utilizado;

3 e 4 – Se a mensagem referente ao ítem 2 for de desafio, a mensagem 3 será uma mensagem resposta ao desafio e a mensagem 4 será uma mensagem de aceitação ou rejeição por parte do Servidor AAA. Se a mensagem de aceitação é recebida pelo Cliente, é iniciado o processo de contabilização por parte do Servidor AAA.

3.3.3 – EAP-AKA

Para um móvel que trafega entre redes heterogêneas, os principais protocolos para a autenticação deste móvel na rede alvo são: o *Extensible Authentication Protocol – Authentication and Key Agreement* (EAP-AKA) e o *Improved Extensible Authentication Protocol –Authentication and Key Agreement* (EAP-AKA'). Esses protocolos foram desenvolvidos pelo 3GPP e são baseados em criptografia de chaves simétricas, fazendo uso

do paradigma desafio-resposta para autenticar o móvel. O EAP-AKA e o EAP-AKA' são protocolos semelhantes, apresentando pequenas diferenças como o uso do algoritmo de *hash* SHA-1 por parte do EAP-AKA e o SHA-256 pelo EAP-AKA'.

A arquitetura do EAP-AKA possui um suplicante, representado pelo terminal móvel (utilizando as chaves e algoritmos de seu USIM (*Universal Subscriber Identity Module*)), um autenticador na rede WLAN e um servidor EAP remoto (implementando autenticação, autorização e *accounting* (AAA) e capaz de requisitar vetores de autenticção ao *Home Subscriber Server* (HSS) da rede caseira do móvel).

A Figura 3.5 ilustra o fluxo de mensagens para a autenticação de um móvel partindo de uma rede LTE e indo em direção a uma rede WLAN:

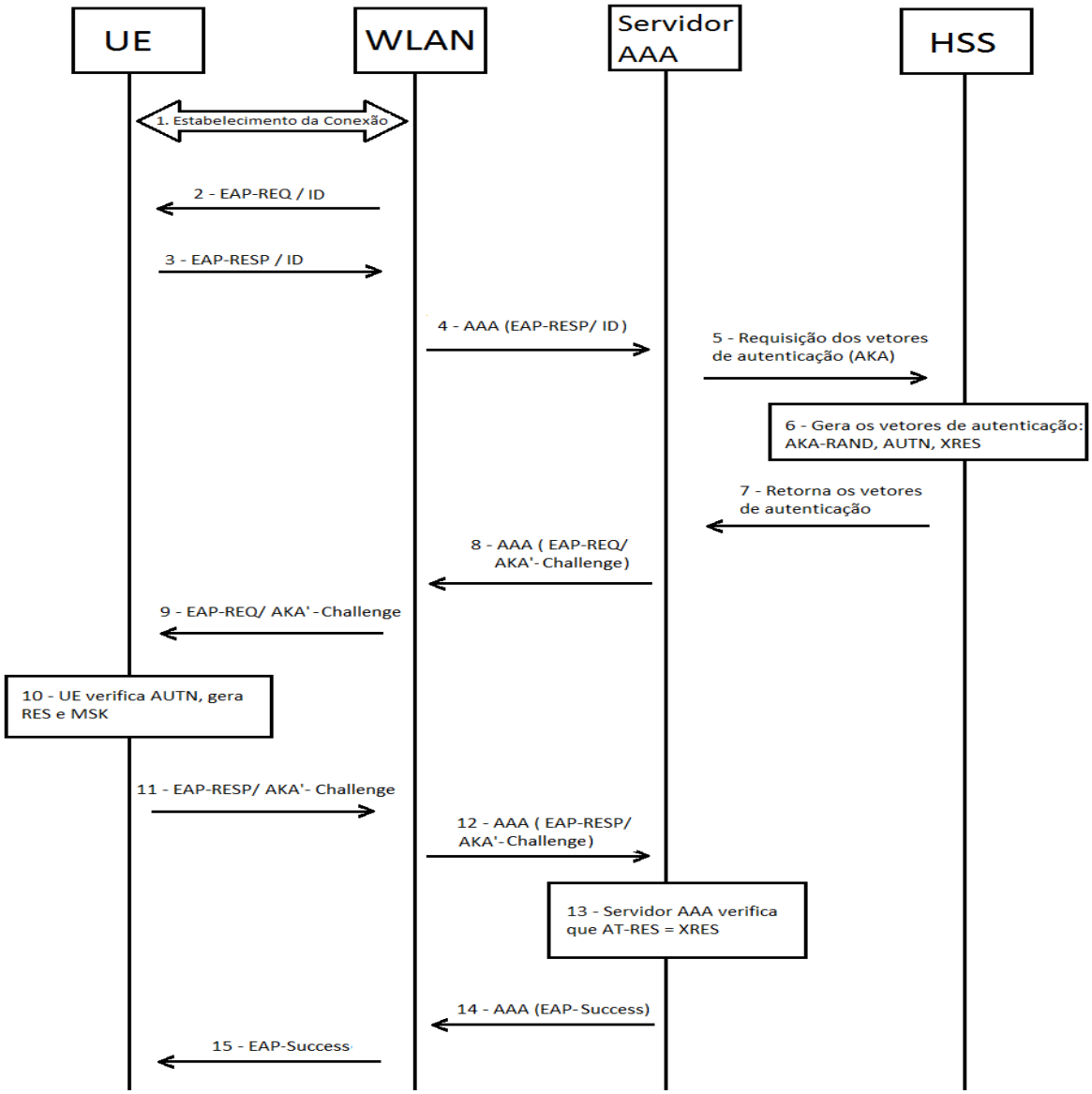

Figura 3.5 – Fluxo de mensagens do protocolo EAP-AKA [1].

Descrição dos eventos:

1 - Tem início a autenticação. Em geral o terminal móvel inicia a autenticação com o envio da mensagem EAPOW-Start (EAP *Over Wireless*).

2 – O autenticador WLAN envia uma mensagem de EAP *Request*/ID ao móvel.

3 – O móvel envia uma mensagem de EAP *Response*/ID, contendo a sua identidade.

4 – A rede WLAN repassa a mensagem EAP *Response*/ID ao servidor AAA da rede LTE.

5 - O AAA da rede LTE requisita os vetores para autenticação do móvel com o HSS.

6 e 7– O AAA da rede LTE deriva chaves a serem usadaspara a autenticação do móvel e as envia ao servidor AAA da rede WLAN.

8 - O servidor AAA envia a mensagem de desafio EAP *Request* /AKA'-*Challenge* contendo o RAND (valor aleatório), AUTN, o código autenticador de mensagem (MAC) e dois identificadores de usuários, que são o pseudônimo protegido e/ou o ID de reautenticação protegido.

9 - O autenticador envia a mensagem EAP *Request*/AKA'-*Challenge* ao móvel.

10 – O móvel executa os algoritmos AKA para a verificação do AUTN e gera chaves para prover segurança à sua comunicação.

11 – Com base nas chaves geradas, o móvel gera a mensagem de resposta do desafio EAP *Response*/AKA'-*Challenge* e a envia ao autenticador.

12 - O autenticador envia a mensagem EAP *Response*/AKA'-*Challenge* ao AAA da rede caseira.

13 – O AAA verifica se a resposta ao desafio enviada pelo móvel está correta.

14 – Se a mensagem de desafio estiver correta, o AAA da rede LTE envia a mensagem EAP-*Success* ao autenticador, informando que a autenticação do móvel foi bem sucedida.

15 – O autenticador repassa ao móvel a mensagem EAP-*Success*, informando ao móvel que sua autenticação foi bem sucedida.

3.4 – GERÊNCIA DE MOBILIDADE EM UMA INTEGRAÇÃO LTE-WLAN

Com os recentes avanços nas tecnologias móveis e dispositivos portáteis, um dos temas mais desafiantes em redes de comunicações móveis é o gerenciamento de mobilidade. O gerenciamento de mobilidade utiliza mecanismos que otimizam a transmissão de pacotes de um ponto a outro da rede, sendo desejável que haja mobilidade sem que o usuário necessite alterar suas configurações de rede.

Um conceito importante em mobilidade é o de micro e macromobilidade. A macromobilidade é o movimento entre domínios administrativos ou o movimento interdomínio de um móvel. Uma das principais características da macromobilidade é não existir limitações geográficas ao movimento do móvel, ou seja, o terminal móvel é capaz de se conectar em qualquer rede e trocar pacotes com um nó correspondente. Neste tipo de mobilidade, as mensagens trocadas em um *handover* são relativas à camada 3, pois normalmente existem configurações nos endereços de camada 3.

A micromobilidade refere-se à mobilidade em um mesmo domínio administrativo. Nesta mobilidade o móvel possui mobilidade apenas local, diferentemente da macromobilidade, na qual a mobilidade é global. Uma das principais características da micromobilidade é que no momento de um *handover*, seja trocado apenas mensagens relativas à camada 2, fazendo com isso que se tenha uma redução na latência de *handover*.

O gerenciamento de mobilidade pode ser provido por abordagens baseadas no móvel ou por baseadas na rede. Para o caso dos protocolos em que a gerência é baseada no móvel, as funções de gerenciamento são de responsabilidade do móvel. Por outro lado, as abordagens baseadas na rede isentam o móvel de qualquer troca de mensagens relativas ao gerenciamento de mobilidade.

De acordo com a norma TS 23.402 [9], em uma arquitetura de integração LTE-WLAN podem ser utilizados dois protocolos para prover as funções de gerenciamento de mobilidade: o *Dual Stack Mobile* IPv6 (DSMIPv6), baseado no móvel, e o *Proxy Mobile*IPv6 (PMIPv6), baseado na rede. As Subseções 3.3.1 e 3.3.2 especificam os protocolos DSMIPv6 e o PMIPv6, respectivamente.

3.4.1 – DSMIPv6

O DSMIPv6 foi proposto na RFC 5555 [20] com a função de prover gerenciamento de mobilidade, feito com a participação do móvel em um escopo da mobilidade global, ou seja, de macromobilidade. Este protocolo é uma extensão dos protocolos *Mobile* IPv4 (MIPv6) [21] e *Network Mobility Basic Support* (NEMO BS) [22] e suporta tanto o IPv4 quanto o IPv6.

Neste protocolo coexistem quatro entidades:

- Nó móvel (UE): dispositivo móvel que pode se conectar redes de acesso IPv4, IPv6 ou *dual stack.*

- *Home Agent* (HA): tem por função armazenar o endereço IP permanente do UE (HoA, do inglês *Home Address*) e associarcom o endereço *care-of* (CoA, do inglês *Care of Address*), que é o endereço da rede estrangeira em que o UE está conectado. A associação entre os endereços HoA e CoA é chamada de *binding.* Outra função do HA é interceptar e rotear os pacotes destinados ao UE.

- *Foreign Agent* (FA): Gateway localizado na rede estrangeira, sua função é repassar os pacotes recebidos pelo HA ao UE e vice e versa. O FA também tem por função prover o CoA ao UE.

- Nó correspondente (CN, do inglês *Correspondent Node*): Dispositivo, móvel ou não, que se comunica com o UE.

Na arquitetura apresentada na Figura 3.1, o PDN-GW exercerá a função de *Home Agent* (HA) enquanto a função de *Foreign Agent* (FA) deverá ser cumprida pelo *Access Router* localizado na rede WLAN.

O funcionamento desse protocolo quando um CN deseje enviar uma mensagem ao UE é descrito abaixo:

1 – O UE se conecta a uma rede estrangeira e recebe um CoA. Para informar o CoA ao HA, o móvel envia uma mensagem de *Binding Update* (BU), informando seu CoA e o HA responde com uma mensagem de *Binding Acknowledgement* (BA) se o armazenamento for feito com seucesso.

2 – Um CN envia um pacote endereçado ao HoA do móvel.

3 – O HA irá interceptar a mensagem endereçada ao HoA, encapsulará esta mensagem em um pacote com o CoA e o repassa ao FA.

4 – Por fim, ao receber o pacote, o FA desencapsula o pacote e envia ao UE.

O processo de envio de mensagens do UE para o CN é mais simples. O UE envia as mensagens ao FA e este as repassa diretamente ao CN.

Se o protocolo estiver fazendo uso do IPv6, pode-se fazer uso de otimização de rota. Neste caso os nós correspondentes podem armazenar *bindings* da mesma maneira que os HAs fazem. Para o envio de mensagens ao UE, os nós correspondentes consultam em sua *binding* o CoA correspondente ao HoA e envia as mensagens diretamente ao nó móvel, sem a necessidade de enviar primeiro ao HA.

Assim como os protocolos que possuem a gerência de mobilidade baseada no móvel, o DSMIPv6 possui algumas desvantagens como a alta latência de *handover* e a modificação da pilha de protocolos do nó móvel pois é um protocolo que possui a gerência de mobilidade baseada no móvel.

3.4.2 – PMIPv6

O *Proxy Mobile IPv6* (PMIPv6), proposto na RFC 5213 [23], é um protocolo em que a gerência de mobilidade é realizada pela rede e o escopo da mobilidade é apenas local (micromobilidade), restrito a um domínio administrativo, chamado de domínio PMIPv6.

No protocolo PMIPv6, além do UE, existem duas entidades, o LMA (*Local Mobility Anchor*) e o MAG (*Mobile Access Gateway*):

- *Local Mobility Anchor* (LMA): esta entidade tem por função interceptar os pacotes destinados ao UE e os tunela ao MAG. Assim como no HA, o LMA possui uma estrutura, chamada de *Binding Cache Entry* (BCE), que irá associar o HoA do móvel com um endereço chamado de *Proxy*-CoA (*Proxy Care of Address*). Diferentemente do DSMIPv6, o *Proxy*-CoA é o endereço associado com cada MAG.

- *Mobile Access Gateway* (MAG): este elemento funciona como um *proxy*, detectando o movimento do UE no enlace de acesso e, em nome deste, trocando as mensagens relativas ao gerenciamento de mobilidade com o LMA.

Na arquitetura apresentada na Figura 3.1, o PDN-GW exercerá a função de LMA enquanto as funções de MAG serão providas pelo SGW na rede LTE e pelo *Access Router* localizado na rede WLAN.

O funcionamento desse protocolo é semelhante ao do DSMIPv6 quando um nó correspondente (CN) deseje enviar uma mensagem ao UE. Como o escopo de mobilidade desse protocolo é apenas local, considera-se que o móvel encontra-se em um domínio PMIPv6.

1 – Um CN envia um pacote endereçado ao HoA do móvel.

2 – O LMA irá interceptar a mensagem endereçada ao HoA, encapsulará esta mensagem (tunelamento) em um pacote com o endereço do *Proxy*-CoA e o repassa ao MAG.

3 – Por fim, ao receber o pacote, o MAG desencapsula o pacote e envia ao UE.

O processoinverso, de envio de uma mensagem do UE ao CN, é descrito abaixo:

1 – Se o UE desejar enviar uma mensagem ao CN, a rota padrão do móvel será sempre o MAG.

2 – Ao receber o pacote, o MAG irá verificar se o CN pertence ou não ao domínio PMIPv6.

3 – Se o CN estiver dentro do domínio PMIPv6, a mensagem é encaminhada diretamente a ele. Caso contrário, o MAG repassa a mensagem ao LMA e este a encaminha ao CN.

Ao realizar o *handover* em direção a um MAG, ocorre a seguinte troca de mensagens, mostrada na Figura 3.6:

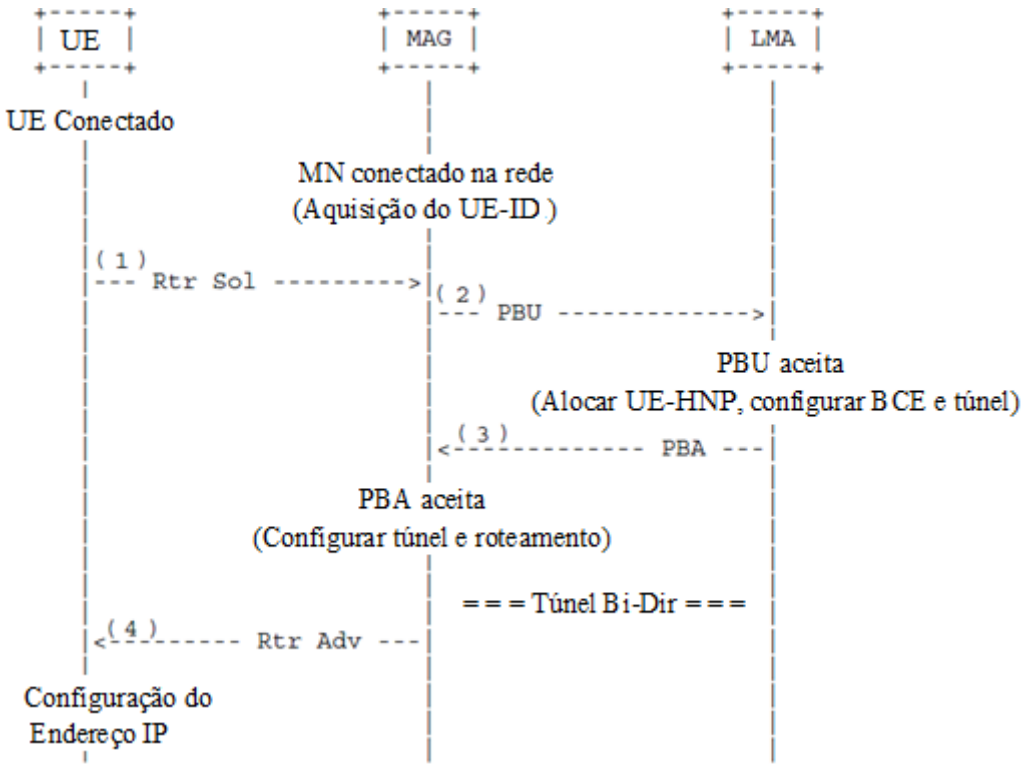

Figura 3.6 – Fluxo de mensagens quando o móvel se conecta ao MAG (Baseado em [23]).

- 1: O UE primeiramente se conecta ao MAG e obtém o seu identificador (UE-ID); após esse processo o móvel envia uma mensagem de *Router Solicitation* ao MAG, solicitando a configuração de seu endereço de camada 3.

- 2: O MAG envia uma mensagem do tipo *Proxy Binding Update* (PBU), contendo o UE-ID, para o LMA estabelecer uma associação entre os endereços UE-HoA e o *Proxy*-CoA. De posse desta mensagem, o LMA aloca um prefixo (UE-HNP) que será utilizado para configurar o endereço do móvel. O LMA configura o seu *endpoint* do túnel bidirecional e cria a *Binding Cache Entry* (BCE) para o móvel.

- 3: O LMA responde com o envio de uma mensagem de *Proxy Binding Acknowledgment* (PBA) contendo o UE-HNP. Após o MAG receber a mensagem, este configura seu *endpoint* do túnel bidirecional, deste modo permitindo o acesso do tráfego de rede ao móvel.

- 4: O MAG envia uma mensagem de *Router Advertisement* ao nó móvel contendo UE-HNP. No domínio PMIPv6 não existirá endereços duplicados nos nós móveis devido ao

fato do UE-HNP ter uso exclusivo para cada móvel. Por este motivo o PMIPv6 realiza apenas uma vez a detecção de endereço duplicado (DAD), no momento em que o UE entra no domínio, fazendo com que ocorra uma menor troca de mensagens.

- 5: A configuração do endereço de camada 3 do móvel pode ser do tipo *stateless,* caso em que o móvel configura seu próprio endereço, ou em modo *statefull*, onde o endereço é gerado por um servidor de DHCP. Após a configuração de endereço estar completa, o UE pode continuar utilizando seu endereço a todo o momento em que estiver conectado no domínio PMIPv6. Assim, a configuração do endereço do móvel só ocorrerá uma única vez, no momento em que o móvel adentrar o domínio PMIPv6, diferentemente do DSMIPv6, em que a cada *handover* é gerado um novo CoA.

3.4.2.1 – Formato das mensagens de *Proxy Binding Update*

A Figura 3.7 ilustra o formato das mensagens de PBU:

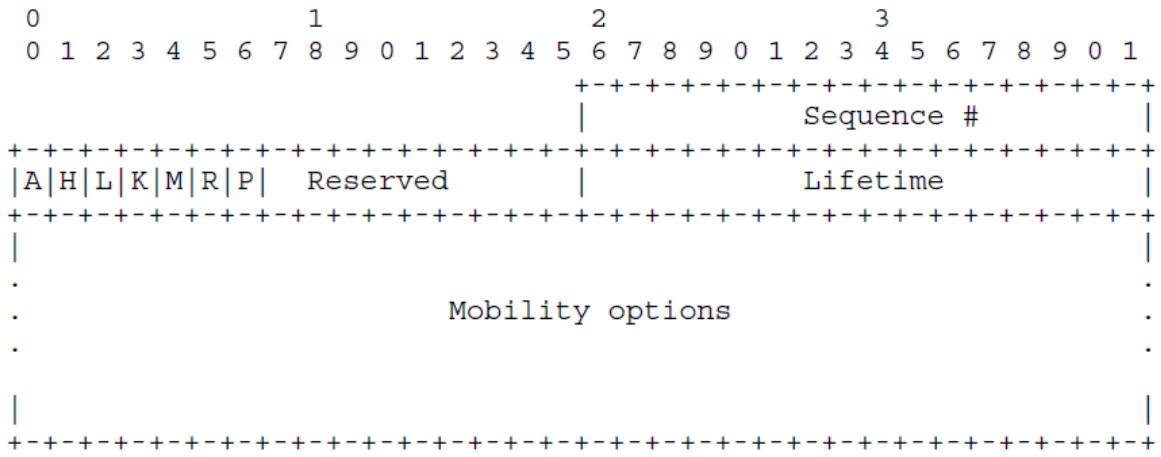

Figura 3.7 – Formato das mensagens de *Proxy Binding Update* [23].

Abaixo é explicado cada campo:

-*Flag* (A): solicitar o envio de uma mensagem de *Proxy Binding Acknowledgement* em resposta a mensagem de Proxy Binding Update enviada.

-*Flag* (H): indica que o nó que receber esta mensagem deverá exercer a função de LMA para o móvel.

-*Flag* (L): indica que o MN-HoA possui o mesmo identificador do *link-local address* do UE.

-*Flag* (K): está relacionada com questões de segurança envolvendo o protocolo IPsec.

-*Flag* (R): indica ao LMA que a mensagem de PBU foi enviada pelo MAG.

-*Flag* (M): indica um registro no LMA.

-*Flag* (P): é incluída na mensagem de *Proxy Binding Update* para indicar ao LMA que a mensagem de PBU é um registro do tipo *proxy*.

-Campo *Reserved*: Este campo por enquanto não é utilizado.

-Campo Lifetime: indica o tempo de vida da mensagem de PBU.

-Campo Sequence #: indica o número sequencial da mensagem de PBU.

-Campo *Mobility Options*: campo que contém diversas informações como o UE-ID, o UE-HNP, o tipo de tecnologia de acesso utilizada pelo móvel ao se conectar ao MAG, dentre outras informações.

3.4.2.2 – Formato das mensagens de *Proxy Binding Acknowledgement*

A Figura 3.8 ilustra o formato das mensagens de PBA:

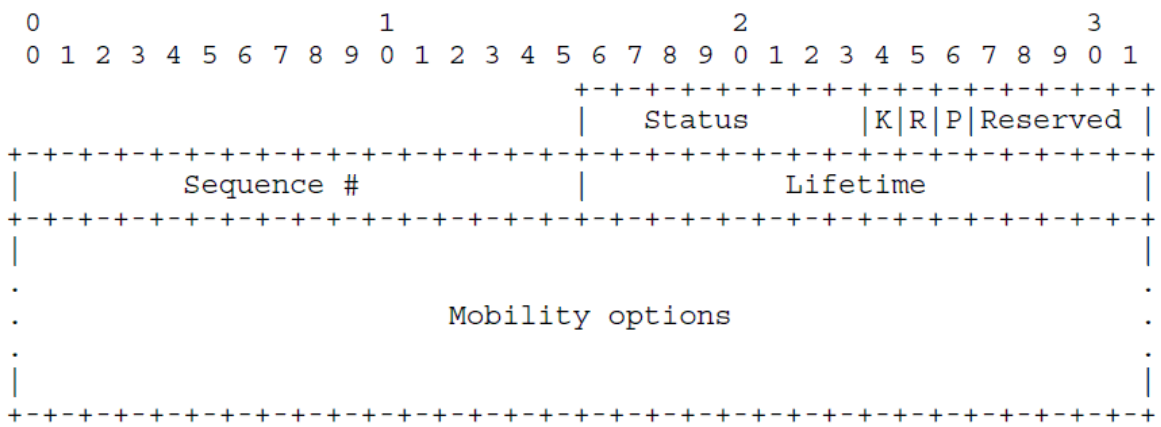

Figura 3.8 – Formato das mensagens de *Proxy Binding Acknowledgement* [23].

Os campos *Lifetime*, *Reserved*, *Sequence #* e *Mobility Options* e as *flags* (K), (R) e (P) possuem as mesmas funções dos campos/*flags* apresentados na Subseção 3.3.2.1.

O campo *Status* indica se a mensagem de PBU foi aceita ou não.

3.5 – FLUXO DE MENSAGENS EM UM *HANDOVER* LTE → WLAN

Esta subseção irá descrever os fluxos de um *handover* entre redes LTE e WLAN, descritos na norma 3GPP TS 23.402 [9]. Os fluxos de *handover* são subdivididos em dois, as abordagens que utilizam o protocolo PMIPv6 e aquelas que fazem uso do DSMIPv6 para prover gerência de mobilidade.

Para todos os fluxos de mensagens que serão apresentados nesta subseção, será considerado que a política de controle e tarifação (PCC) é realizada em modo estático, ou seja, é provido pela infraestrutura de AAA da rede WLAN como especificado na Seção 4.10.4 da norma 3GPP TS 23.402 [9]. Por simplificação, serão omitidos os elementos intermediários entre o PDN-GW e o HSS/AAA.

3.5.1 – Fluxo de Mensagens em um *Handover* LTE → WLAN Não Otimizado Utilizando o PMIPv6

A Figura 3.9 ilustra o fluxo de mensagens em um *handover* vertical LTE-WLAN fazendo uso do protocolo PMIPv6 para prover gerência de mobilidade.

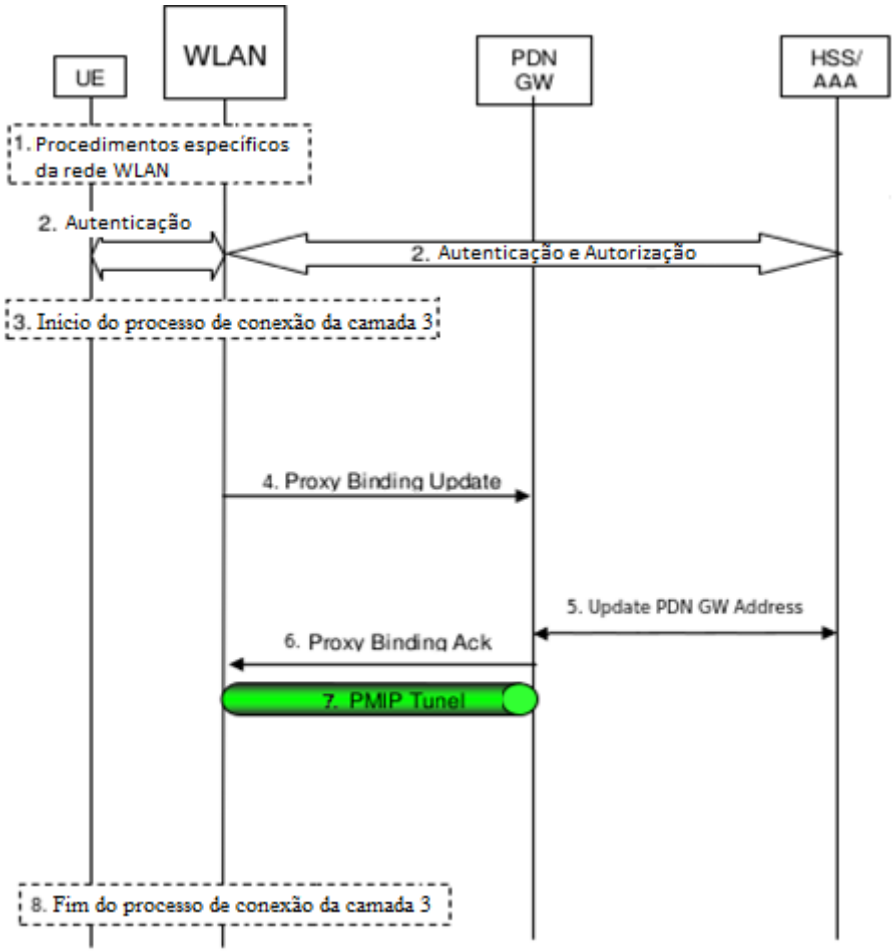

Figura 3.9 – Fluxo de mensagens em um *handover* vertical no sentido LTE →WLAN utilizando o PMIPv6 (Baseado em [9]).

Descrição dos eventos:

1 – Primeiramente são realizados os procedimentos relativos ao *handover* de camada 2 da rede WLAN.

2 – É feita a autenticação do móvel na rede WLAN.

3 - Tem-se o início do processo de conexão relativos à camada 3.

4 - O MAG localizado na rede WLAN envia uma mensagem de *Proxy Binding Update.*

5 - O PDN-GW informa ao servidor 3GPP AAA o seu ID e o APN (*Access Point Name*) correspondente à conexão com o UE.

6 – Ao receber a mensagem de *Proxy Binding Update*, o PDN-GW cria a *Binding Cache Entry* para o UE e envia uma mensagem de *Proxy Binding Acknowledgement* ao MAG, representado pelo AR, da rede WLAN.

7 - Um túnel bidirecional é configurado entre o MAG da rede WLAN e o PDN-GW.

8 – O processo de *handover* está completo.

3.5.2 – Procedimento de desconexão em uma rede WLAN utilizando o PMIPv6

O procedimento de *handover* quando o móvel se desconecta da rede WLAN e volta para a sua rede caseira LTE é mostrado na Figura 3.10:

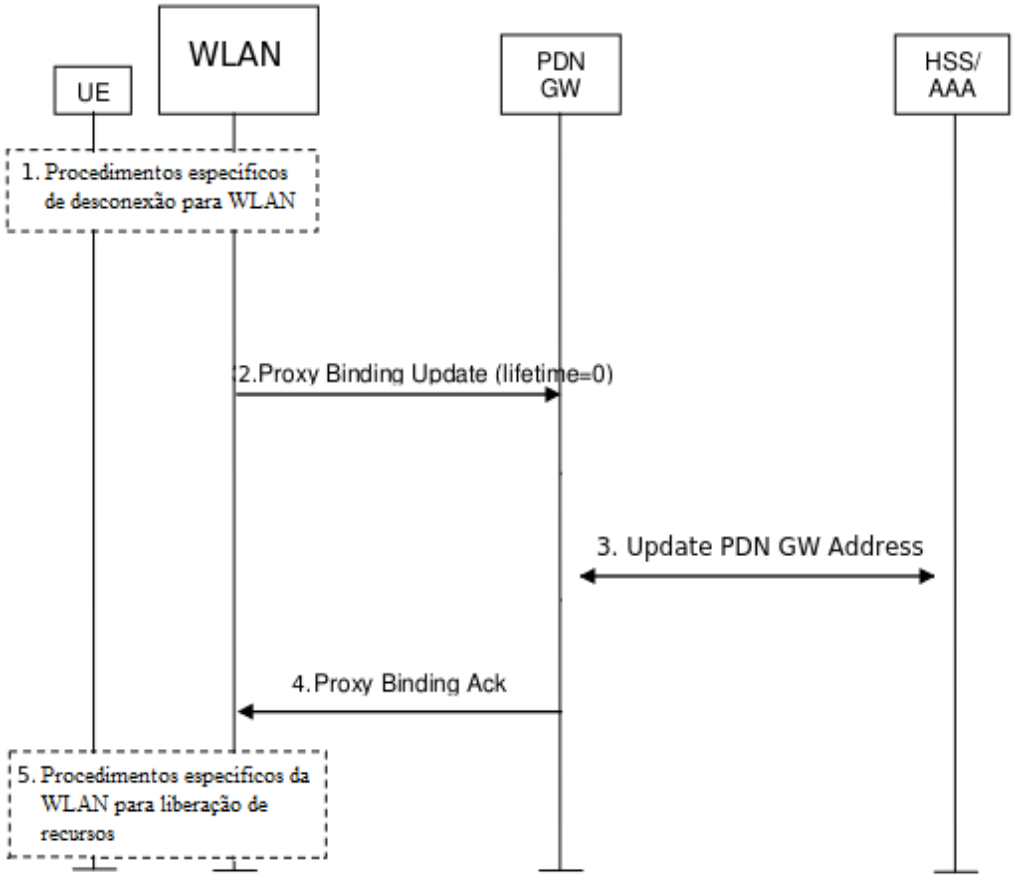

Figura 3.10 – Procedimento para desconexão em uma rede WLAN utilizando o PMIPv6 (Baseado em [9]).

Descrição dos eventos:

1 – Tem-se o início do processo de desconexão do UE com a rede WLAN.

2 - O MAG envia uma mensagem de PBU ao PDN-GW, contendo o campo *lifetime* setado para zero, indicando uma mensagem de cancelamento de registro do móvel.

3 - O PDN-GW informa ao HSS/AAA a desconexão do UE com a rede WLAN.

4 - O PDN-GW ao receber a mensagem de PBU, deleta a BCE do UE e envia uma mensagem de PBA ao MAG.

5 - O procedimento de liberação de recursos na rede WLAN é executado.

3.5.3 – Fluxo de Mensagens em um *Handover* LTE-WLAN Utilizando o DSMIPv6

A Figura 3.11 ilustra o fluxo de mensagens em um *handover* vertical no sentido LTE → WLAN fazendo uso do protocolo DSMIPv6 para prover gerência de mobilidade.

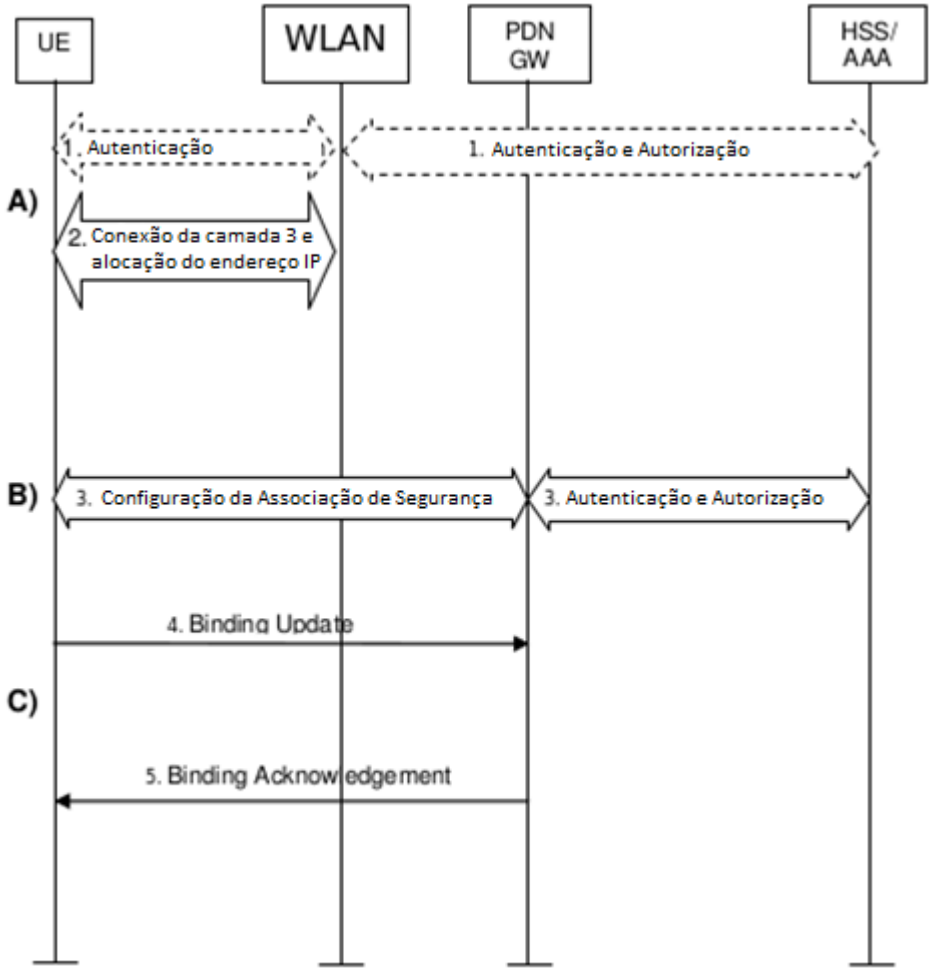

Figura 3.11 – Fluxo de mensagens em um *handover* vertical LTE-WLAN utilizando o DSMIPv6 (Baseado em [9]).

O *handover* da Figura 3.11 é descrito em três módulos, A, B e C:

- A : Em A, o UE configura a conectividade IP com a rede WLAN. Neste módulo ocorrem os seguintes eventos:

1 – São realizados os procedimentos de autenticação.

2 – A conexão de camada 3 é estabelecida entre o UE e a rede WLAN e como resultado é alocado um endereço IP (CoA) ao móvel.

- B : Em B é realizado a associação de segurança entre o móvel e o PDN *Gateway*. Neste módulo ocorre apenas o seguinte evento:

3 – É feito uma associação de segurança utilizando o IKEv2 entre o UE e o PDN *Gateway*, descrito na norma 3GPP TS 33.402 [1].

- C : Em C são realizados os procedimentos relativos a gerência de mobilidade . Neste módulo ocorrem os seguintes eventos:

4 - O UE envia a mensagem de *Binding Update* ao PDN GW, contendo os endereços HoA e CoA.

5 - O PDN GW envia uma mensagem e *Binding Acknowledgement* ao móvel.

3.5.4 – Procedimento de desconexão em uma rede WLAN utilizando o DSMIPv6

O procedimento de *handover* quando o móvel se desconecta da rede WLAN e volta para a sua rede caseira LTE é mostrado na Figura 3.12:

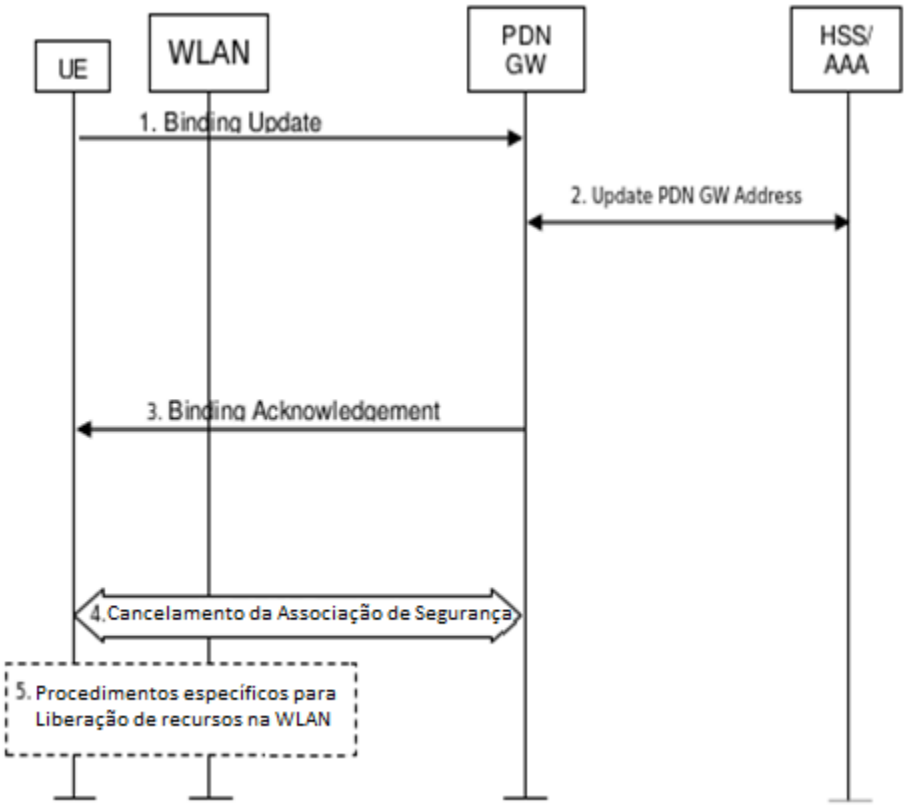

Figura 3.12 – Procedimento para desconexão em uma rede WLAN utilizando o DSMIPv6 (Baseado em [9]).

Descrição dos eventos:

1 – O móvel envia uma mensagem de *Binding Update* ao PDN GW indicando cancelamento de registro.

2 – O PDN-GW informa ao servidor de AAA da desconexão do UE com a rede WLAN.

3 – O PDN-GW responde a mensagem de BU com uma mensagem de *Binding Acknowledgement* ao móvel.

4 - O móvel encerra a associação de segurança IKEv2 com o PDN GW.

5 - O procedimento de liberação de recursos na rede WLAN é executado.

3.6 – CONSIDERAÇÕES FINAIS

Neste Capítulo foram apresentados importantes aspectos arquiteturais, de segurança, de gerenciamento de mobilidade e *handover* em uma arquitetura de integração LTE-WLAN. Primeiramente foi apresentada a arquitetura de integração LTE-WLAN, ilustrada na norma TS.23402 [9], e que será utilizada como base para a análise de desempenho nos estudos de caso do Capítulo 6. Em termos de segurança, foram apresentados o *Extensible Authentication Protocol* (EAP), protocolo em que diversos métodos de autenticação se baseiam, e o *Remote Authentication Dial In User Service* (RADIUS), um dos protocolos mais utilizados para transportar mensagens relativas às funções de Autenticação, Autorização e *Accounting*. Adicionalmente, foram apresentados os protocolos EAP-AKA e EAP-AKA', protocolos que são utilizados por padrão pelo 3GPP para autenticação de um dispositivo móvel uma integração LTE-WLAN. De acordo com a norma TS 23.402, podem ser utilizados o DSMIPv6 e o PMIPv6 para prover as funções de gerenciamento de mobilidade ao móvel em uma arquitetura de integração LTE-WLAN como discutidos neste Capítulo, porém deu-se uma maior ênfase no PMIPv6, pois será o protocolo utilizado como base nos estudos de caso do Capítulo 6. Por fim, foram apresentados os fluxos de mensagens em um *handover* no sentido LTE → WLAN com o uso dos protocolos PMIPv6 e DSMIPv6.

4 – TRABALHOS RELACIONADOS

A integração de redes LTE e WLAN tem sido o foco de diversos trabalhos devido às inúmeras vantagens existentes na interconexão dessas redes. Apesar da integração das redes LTE e WLAN ter se mostrado uma boa alternativa para o excesso de tráfego nas redes das operadoras de telefonia móvel, alguns problemas necessitam serem solucionados, dentre eles pode-se citar os relacionados aos serviços de comunicações multimídias em termpo real, por apresentarem certos níveis aceitáveis de QoS.

Em um *handover* no sentido LTE→WLAN, um dos processos que mais consomem recursos é o de autenticação do móvel na rede WLAN. O foco de diversos trabalhos está em métodos de autenticação que possuam baixa latência de *handover* e sejam seguros, ou seja, possuam certas propriedades de segurança como proteção contra ataques do tipo *Man in the Middle* e *Replay*, autenticação mútua entre o móvel e a rede WLAN, verificação de integridade, dentre outros.

Outro mecanismo que pode prover o aumento da latência de *handover* em uma integração LTE-WLAN é a gerência de mobilidade. Protocolos que possuem a gerência baseada no móvel e na rede são amplamente estudados a fim de se alcançar uma redução na latência de *handover*.

Neste Capítulo, serão descritos os trabalhos que possuem o foco principal na redução da latência de *handover* baseados em mecanismos de autenticação e gerência de mobilidade.

4.1 – GERENCIAMENTO DE MOBILIDADE

Os trabalhos descritos por [24] e [25] provêem um *overview* sobre os métodos de gerência de mobilidade em redes heterogêneas. Nesses artigos são descritos diversos tipos de integrações entre redes sem fio como UMTS-WLAN, UMTS-WiMax, LTE-WLAN e as principais técnicas de gerenciamento de mobilidade. São apresentados também as principais tendências e desafios nessa área.

Em [26], foi feito uma análise dos protocolos PMIPv6 e DSMIPv6 em um *handover* vertical no sentido LTE→WLAN, fazendo uso do EAP-AKA para prover autenticação. Como resultado, foi verificado que o PMIPv6 apresentou uma latência de *handover* significativamente menor se comparado ao DSMIPv6. O principal fator do DSMIPv6 possuir uma maior latência é o processo de associação de segurança do UE com o PDN-GW ser muito oneroso.

Outro trabalho que também tem por objetivo a redução e a avaliação da latência de *handover* é o [27]. Neste artigo é proposto um protocolo baseado no PMIPv6, chamado de *Fast Handovers for Proxy Mobile IPv6.* São utilizados dois cenários, um *handover* vertical no sentido LTE→WiMax e outro no sentido LTE→WLAN. Para a avaliação deste protocolo foi utilizado um modelo analítico.

Outra proposta para melhoria do protocolo PMIPv6 é tratada em [28]. Em uma arquitetura do tipo SAE, todo o tráfego de dados das estações móveis deve ser processado pelo PDN-GW, entidade responsável por prover as funções de LMA. Com essa centralização de todo o tráfego em um único nó, ocorre uma dependência e sobrecarga sobre o PDN-GW que pode afetar o desempenho da rede. Os autores propuseram um esquema para o balanceamento de carga com a introdução de uma nova entidade de controle chamada de *Mobility Control Agent* (MCA). Avaliou-se o impacto referente aos atrasos de transmissão e ao tráfego de *overhead* (número total de pacotes de controle e dados) do protocolo proposto.

4.2 – PROTOCOLOS DE AUTENTICAÇÃO

4.2.1 – Visão geral

Uma descrição detalhada dos aspectos de segurança em redes LTE/LTE-A é feito em [29]. Neste trabalho primeiramente é feito um *overview* sobre os principais aspectos da arquitetura de segurança LTE. Em seguida são discutidos as ferramentas e mecanismos de segurança no LTE, dentre eles pode-se citar, a segurança no processo de *handover* vertical entre uma rede LTE e outra que não seja do padrão 3GPP, como a rede WLAN. São descritos também vulnerabilidades na segurança do LTE, como vunerabilidades na arquitetura, nos procedimentos de *handover* e também diversos trabalhos em que são apresentadas as soluções para essas vulnerabilidades. Por fim, são discutidas as questões em aberto sobre o tema.

Em [30] foi proposto um método de autenticação rápido e seguro para *handovers* verticais tanto no sentido LTE →WLAN quanto no sentido WLAN → LTE. Este protocolo foi batizado de UNAEN e tem por objetivo a redução da latência de *handover*. O UNAEN consiste de duas fases, uma fase de preparação, em que é feita a preparação para a

futura autenticação do móvel e outra em que o móvel é autenticado na rede WLAN. Os autores avaliaram o protocolo proposto em termos da latência de *handover*, sendo que este apresentou uma significativa redução na latência.

O trabalho apresentado por [31], consiste de um método de autenticação derivado do EAP-AKA, chamado de EAP-FAKA (do inglês EAP - *Fast Authentication and Key Agreement)*. O protocolo proposto consiste de um método de autenticação baseado no paradigma desafio resposta em que a principal vantagem desse método é o uso do servidor de AAA da rede WLAN para autenticar o móvel, diferentemente do EAP-AKA em que o servidor de AAA da rede LTE que é utilizado para a autenticação. A principal vantagem do uso do servidor de AAA da rede WLAN é a redução do número de menagens para a realização do processo de autenticação do UE. Um robusto método para reautenticação do EAP-FAKA é apresentado em [32]. Batizado de EAP-FLAKA (do inglês *Fast Local Authentication and Key Agreement*), este protocolo reaproveita as chaves geradas no processo de autenticação completa do EAP-FAKA, fazendo com que não haja a necessidade de se fazero oneroso processo de consulta ao HSS.

Uma abordagem para autenticação em um *handover* LTE-WLAN com o uso de certificação digital é proposto por [33]. Chamado de EAP-LUTLS (do inglês EAP - *Lightweight USIM based Transport Layer Security*), o protocolo proposto consiste de um pré-compartilhamento de uma chave secreta entre o móvel e o HSS da rede 4G. Neste esquema, as entidades que participam do processo de autenticação fazem uso de certificações digitais. Assim como no EAP-FAKA, o servidor de AAA da WLAN é utilizado para autenticar o móvel.

Em [34], foi utilizada uma arquitetura para integração das redes LTEs e WLANs um pouco diferente da apresentada na Figura 3.1, adicionando um elemento chamado de *Hybrid Interconnection Unit* (HIU), *gateway* com a finalidade de interconectar as redes WLAN e LTE. Assim como no UNAEN, o protocolo proposto possui três fases, a de preparação para o futuro *handover,* de pré-autenticação e a de autenticação. Para a análise de desempenho, foi utilizada uma simulação computacional para avaliação de latência de *handover*, taxa de bloqueio de *handover* e taxa de perda de pacotes. Esta abordagem inclui apenas o *handover* no sentido LTE → WLAN.

Em [35] foi proposto um protocolo baseado no EAP-AKA para *handovers* no sentido LTE → WLAN. Este protocolo inclui uma significativa diferença nas entidades que participam do processo de autenticação no *handover* LTE-WLAN, não utilizando o servidor de AAA da rede 4G, sendo toda a responsabilidade pelas funções de autenticação, autorização e *accounting* providas pelo servidor de AAA da rede WLAN. Neste caso foi assumido um canal seguro entre o servidor de AAA da rede WLAN e o HSS.

Em [36] é apresentado um método de autenticação baseado em criptografia de chave pública, chamado de EAP-CRA (do inglês EAP-*Coordinated Robust Authentication*). Neste protocolo a principal vantagem é a isenção do UE de qualquer procedimento de desafio-resposta, fazendo com que o móvel não precise guardar nenhum tipo de *token*. Este protocolo também possui um método de reautenticação proposto por [37]. Assim como o EAP-FLAKA, o método de reautenticação do EAP-CRA segue as mesmas pemissas, utilizando as chaves criptográficas geradas na autenticação completa do EAP-CRA, fazendo com que não haja a necessidade de se fazer nenhuma consulta ao HSS.

Nesta subseção, foi apresentada uma visão geral sobre os trabalhos relacionados que tratam sobre gerência de mobilidade e métodos de autenticação em uma integração LTE-WLAN. Nas próximas subseções serão detalhados os protocolos de autenticação que serão de interesse direto para o trabalho a ser feito.

4.2.2 – Protocolo UNAEN

4.2.2.1 – Descrição do Protocolo

Em [30], foi proposta uma técnica de autenticação rápida e segura para *handovers* entre redes do tipo 3GPP e outra que não seja do padrão 3GPP, por exemplo, entre redes LTE e WLAN. Foi utilizada uma arquitetura do tipo SAE, com as redes de acesso 3GPP e não 3GPP conectadas por uma mesma arquitetura de núcleo do tipo EPC (*Evolved Packat Core*).

Nesta proposta, o termo *Access Point* é empregado com sentido genérico, abrangendo a E-UTRAN, as redes de acesso do tipo *trusted* que não sejam do padrão 3GPP e o ePDG para redes do tipo *untrusted* que não sejam do padrão 3GPP, que são, entâo, nesta proposta, vistas como APs.

Neste cenário, o móvel move-se entre dois *Access Points*, o AP da rede atual (AP_1) e o AP da rede alvo (AP_2). Adaptando este cenário a este trabalho, pode-se considerar que o AP_1 é representado pela eNB na rede LTE e o AP_2 é o *Access Points* da rede WLAN, quando se considera o *handover* no sentido LTE → WLAN. O protocolo não restringe o sentido do *handover*, podendo este ser realizado tanto no sentido rede 3GPP em direção à rede não 3GPP ou então no sentido rede não 3GPP em direção à rede 3GPP.

O esquema proposto, batizado de UNAEN, consiste de duas fases, uma fase de preparação para o futuro *handover* do móvel chamada de "fase de preparação de *handover*" e outra consistindo da autenticação do móvel durante o *handover,* chamada de "fase de autenticação".

A "fase de preparação de *handover*" tem por objetivo fazer a preparação da autenticação para o futuro *handover*. Nesta etapa primeiramente os *Acccess Points* (no sentido genérico adotado pelos autores, e não somente para WLANs) e os dispositivos móveis recebem de um Centro de Distribuição de Chaves (KGC, do inglês *Key Generation Center*), função provida pelo HSS, suas chaves privadas (que são de *long term* ou longo prazo), sendo que apenas APs e dispositivos móveis autenticados podem receber chaves privadas do KGC. Esta fase é subdividida em outras duas fases, Inicialização e Distribuição de chaves. Na subfase de inicialização o KGC gera os parâmetros de segurança do sistema e a *Master Key*. A subfase para distribuição das chaves só será realizada na primeira vez que o AP e o UE registrarem-se na rede ou sua chave privada expirar. Para a aquisição da chave privada, cada UE/AP envia uma mensagem contendo seu ID ao KGC via servidor de AAA utilizando a chave secreta pré negociada entre os elementos.

Na "fase de autenticação", é realizado um procedimento de autenticação mútua entre o móvel e o AP alvo (AP_2), como mostrado na Figura 4.1:

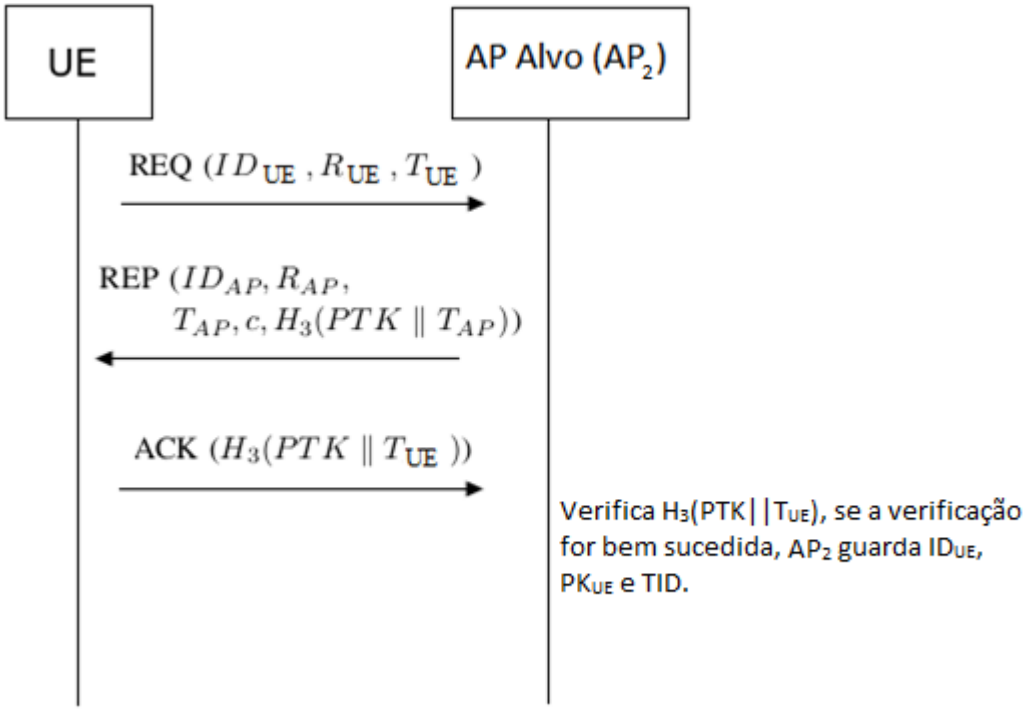

Figura 4.1 – Fluxo de mensagens do UNAEN (Baseado em [30]).

Este protocolo faz a troca de apenas 3 mensagens para a realização da autenticação mútua entre o móvel e o AP. Inicialmente, o móvel envia uma mensagem ao AP, contendo o seu identificador temporário (ID_{UE}) e os parâmetros de segurança R_{UE} e T_{UE}. Após o AP receber a mensagem, ele computa a chave pública do móvel, a chave de sessão PTK e os parâmetros $K1_{AM}$ e $K2_{AM}$, que serão utilizados para a realização da autenticação mútua e geração da chave de sessão PTK. O AP também gera aleatoriamente um ID temporário TID para o móvel e o encripta com PTK (c = EncPTK(TID)) e envia uma mensagem ao UE contendo o seu identificador temporário (ID_{AP}), os parâmetros de segurança $R_{AP,}$ T_{AP}, c e H3(PTK || T_{AP}), em que H3() é uma função de *hash* segura. Após receber a mensagem, o móvel computa $K1_{AM}$, $K2_{AM}$ e PTK. Ele então verifica H3(PTK || T_{AP}), e se esta for bem sucedida, o móvel decripta c e guarda TID. Em seguida, o móvel envia uma mensagem de ACK contendo o H3(PTK || TME). Ao receber o ACK, o AP verifica o valor da função de *hash* H3, se este for bem sucedido, o procedimento de autenticação é bem sucedido. A próxima vez que o móvel retornar a esta WLAN os parâmetros (ID_{UE}, R_{UE}) serão substituídos por TID, a nova chave de sessão é gerada com base em TID e o AP irá gerar um novo identificador temporário TID' ao móvel.

O esquema proposto pode ser aplicado não apenas a redes WLAN, mas em todos os cenários de mobilidade entre redes LTE e redes que não sejam do padrão 3GPPP, tanto do tipo *trusted* quanto do tipo *untrusted*.

Alguns tipos de serviços, como transmissões de vídeo pela internet e VoIP (Voz sobre IP), possuem determinados níveis aceitáveis de QoS para que os serviços funcionem com uma boa qualidade ao usuário. Em especial, para se alcançar esses níveis de QoS, a latência de *handover* deverá ser a mínima possível, e a grande vantagem desse método de autenticação é existência de poucas trocas de mensagens para autenticação no processo de *handover*, reduzindo assim a latência de autenticação.

Em contrapartida, todos os APs e dispositivos móveis conectados a alguma rede integrada à arquitetura SAE devem realizar pelo menos uma vez a preparação para o futuro *handover* com o centro de distribuição de chaves, podendo ocorrer uma sobrecarga do servidor e da rede.

4.2.2.2 – Gerenciamento de chaves

O diagrama de gerenciamento de distribuição de chaves do protocolo é mostrado na Figura 4.2:

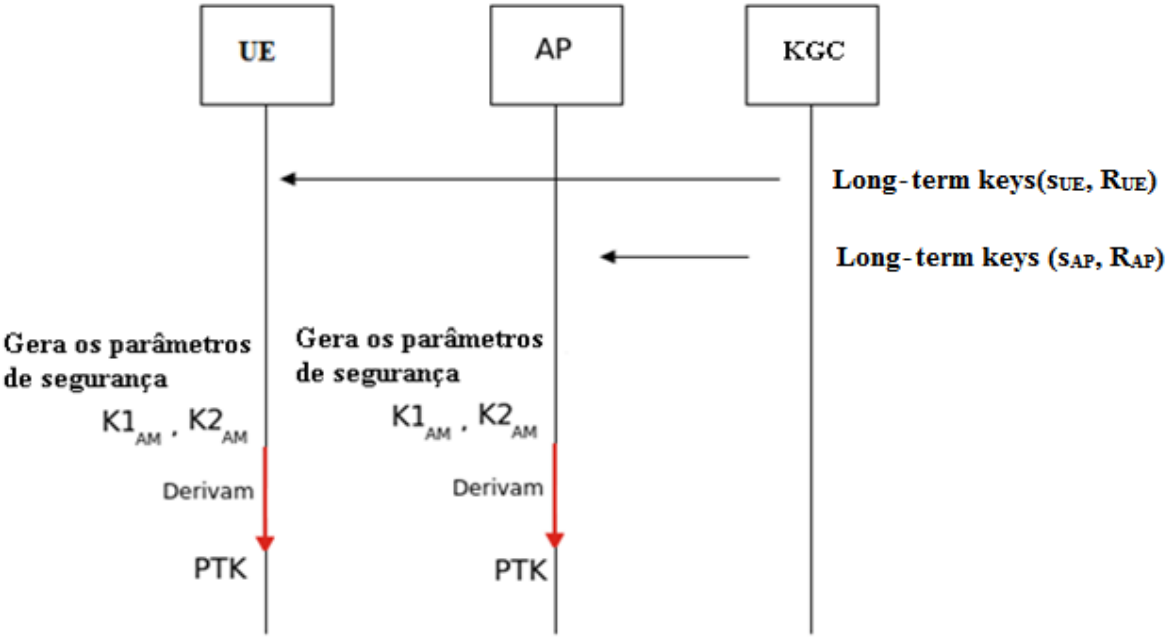

Figura 4.2 – Gerenciamento e distribuição de chaves do UNAEN.

O protocolo UNAEN é dividido em duas fases: preparação e *handover*. Durante a fase de preparação, além de o KGC possuir seu par de chaves privada/pública x/PK, gera as chaves *long term* do móvel (s_{UE}, R_{UE}) e do AP (s_{AP}, R_{AP}).

Durante a fase de *handover*, são gerados os parâmetros de segurança $K1_{AM}$ e $K2_{AM}$ que são utilizados para autenticação mútua entre o móvel e a rede WLAN. Por fim, o móvel e o AP geram a chave de sessão *Parwise Transient Key* (PTK), derivada de $K1_{AM}$ e $K2_{AM}$.

4.2.3 – Protocolo EAP-FAKA

4.2.3.1 – Descrição do Protocolo

Em [31] foi proposto um protocolo de autenticação para ser utilizado em um *handover* no sentido LTE →WLAN, chamado de EAP-FAKA (EAP - *Fast Authentication and Key Agreement*). O método simplifica o processo de autenticação, reduz o atraso de autenticação e oferece um flexível método para reautenticação. O EAP-FAKA é baseado no EAP-AKA e faz a combinação do uso de sistemas de chave simétrica e assimétrica.

Nesta abordagem os autores utilizam uma arquitetura de integração das redes LTE e WLAN do tipo SAE, com uma rede de núcleo do tipo EPC, como a apresentada na Figura 3.1.

Para este protocolo foram assumidos alguns pressupostos:

- Um canal seguro entre os elementos *Access Point* (AP), servidor de AAA da rede WLAN (WAAA), servidor de AAA da rede caseira (HAAA) e o HSS;

- Um WAAA é responsável por vários APs;

- O dispositivo móvel (UE) pode identificar o ID do AAA e do AP;

- Todo HAAA possui uma chave pública conhecida;

- Cada UE tem um par de chaves secretas pré-compartilhadas com o servidor HSS.

O funcionamento do protocolo é descrito pelo fluxo de mensagens apresentado na Figura 4.3:

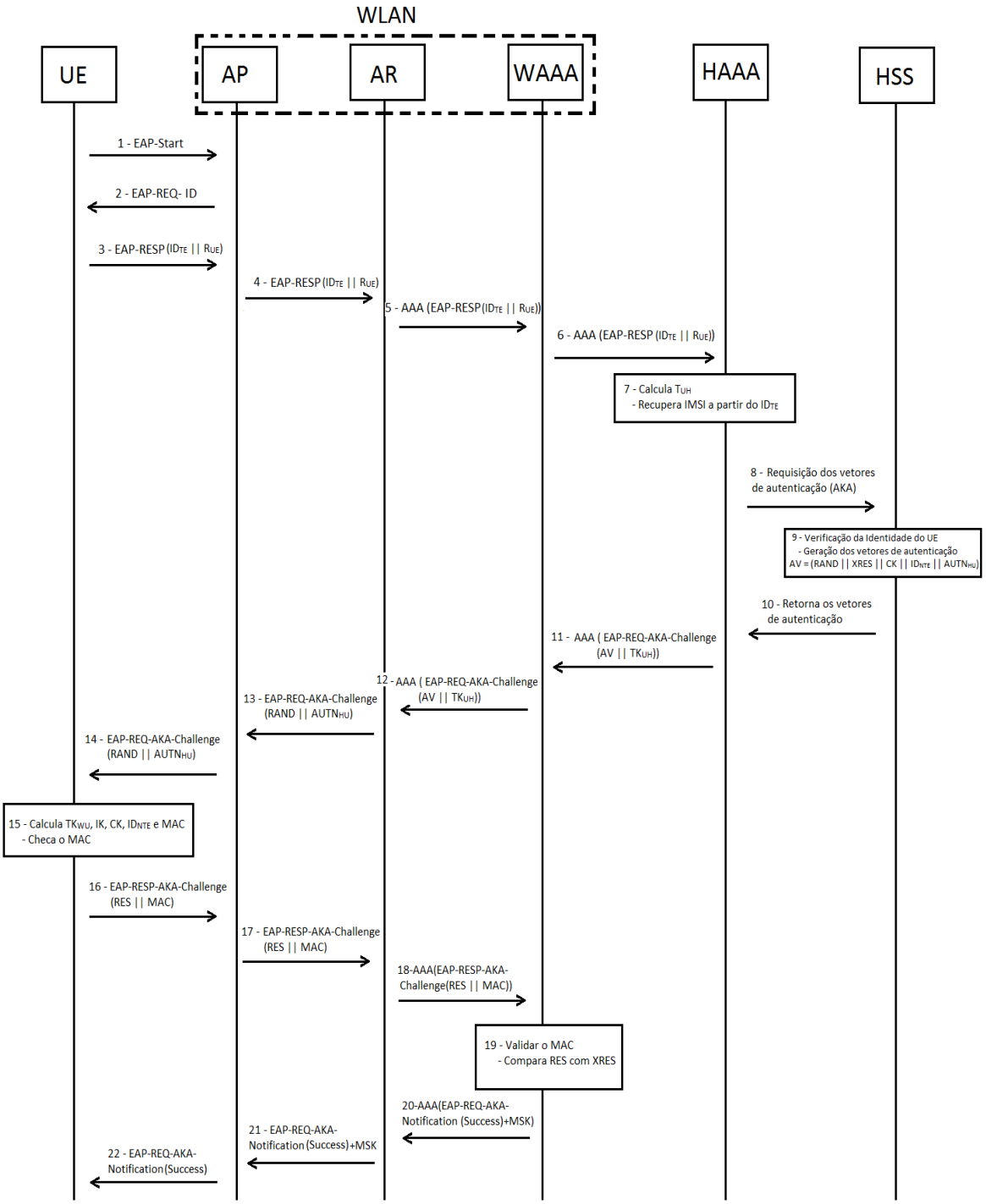

Figura 4.3 – Fluxo de mensagens do EAP–FAKA (Baseado em [31]).

Este protocolo apresenta o fluxo de mensagens semelhante ao do EAP-AKA (Figura 3.5), como apresentado na Figura 4.3. Após a detecção do UE pela rede, o AP requisita ao móvel seu identificador e os repassa ao HSS, por meio dos servidores de AAA, para a obtenção dos vetores de autenticação, que serão utilizados para o processo de autenticação

do tipo desafio-resposta. Após receber os vetores de autenticação, o WAAA envia a mensagem de desafio ao AP para ser repassada ao dispositivo móvel. O UE ao receber a mensagem de desafio verifica-a com seus parâmetros de segurança. Se a verificação for bem sucedida, o móvel envia a resposta do desafio ao WAAA. De posse da mensagem de resposta, o WAAA irá fazer a validação dessa mensagem, e se esta for bem sucedida, enviará uma mensagem ao móvel notificando-o que a autenticação foi bem sucedida.

A principal vantagem desse protocolo é o uso do servidor de AAA da rede WLAN (WAAA) para autenticar o móvel, diferentemente do EAP-AKA que utiliza o HAAA para este procedimento. Com isso trocam-se 4 mensagens a menos em comparação ao EAP-AKA, fazendo com que haja a redução da latência de *handover* e uma diminuição do consumo de banda.

Em contrapartida, por não apresentar uma abordagem baseada na preparação para o futuro *handover*, este protocolo ainda apresenta um elevado número de mensagens trocadas durante o *handover* se comparado ao UNAEN [30]. Outra desvantagem apresentada por este método é o fato de ser limitado ao uso em redes WLAN, diferentemente do EAP-AKA que possibilita seu uso para qualquer tipo de redes que não sejam do padrão 3GPP.

4.2.3.2 – Gerenciamento de chaves

A Figura 4.4 apresenta o diagrama do gerenciamento e distribuição de chaves do EAP-FAKA. Primeiramente, o móvel e o servidor AAA da sua rede caseira (HAAA) pré-compartilham o par de chaves (U_E, d_E), e a partir de U_E é gerada uma chave TK_{UH}, utilizada para esconder o verdadeiro ID do móvel. Uma chave TK_{HU} é gerada pelo HSS para derivação dos vetores de autenticação, compostos pelas chaves de integridade IK e ciframento CK. As chaves IK, CK e TK_{HU} são enviadas ao HAAA e repassadas ao WAAA. A partir da TK_{HU} é derivada a *Master Session Key* (MSK), utilizada para uma comunicação segura entre o AP e o móvel. Por fim é realizado o procedimento de 4-*way handshake* entre o móvel e o AP para a geração da *Transient Session Key* (TSK).

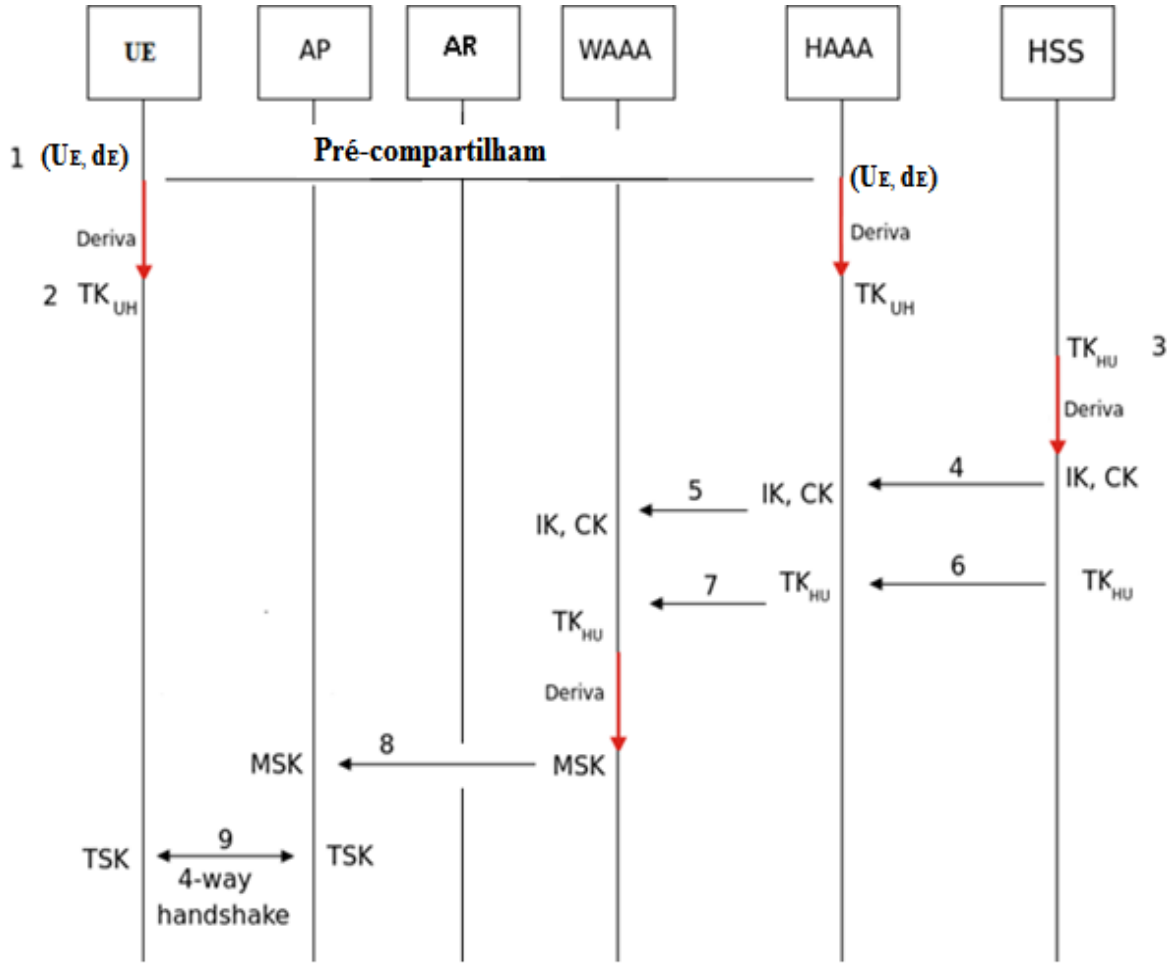

Figura 4.4 – Gerenciamento e distribuição de chaves do EAP-FAKA.

4.2.4 – Protocolo EAP-FLAKA

4.2.4.1 – Descrição do Protocolo

O EAP-FLAKA, descrito em [32], é um protocolo de reautenticação derivado do EAP-FAKA, utilizado nos casos em que o móvel se reassocia com uma mesma rede WLAN com frequência.

Nesta abordagem foram assumidos os mesmos pressupostos e os mesmos aspectos arquiteturais considerados para o EAP-FAKA [31].

Neste método, o WAAA autentica o móvel em nome do HAAA utilizando a chave recebida anteriormente na autenticação completa do protocolo EAP-FAKA.

O funcionamento do protocolo é descrito pelo fluxo de mensagens apresentado na Figura 4.5:

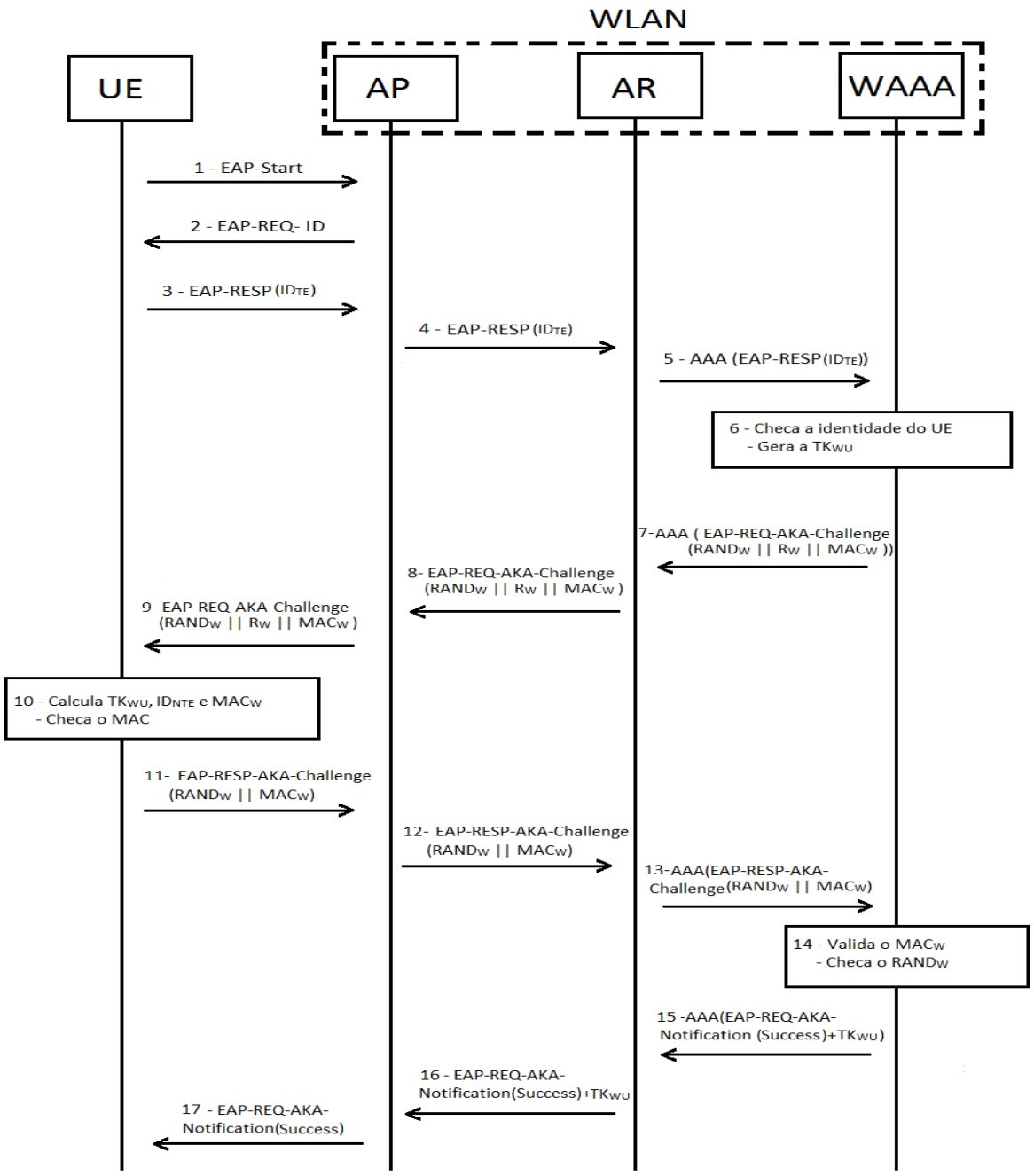

Figura 4.5 – Fluxo de mensagens do EAP-FLAKA (Baseado em [32]).

No esquema de reautenticação rápida, após a detecção do móvel, a rede WLAN primeiramente requisita a identificação do móvel, identificação esta que foi previamente entregue ao móvel no processo de autenticação do EAP-FAKA. Após isso, são feitos os

procedimentos de reautenticação do móvel utilizando as chaves derivadas da autenticação completa anterior. É realizado o procedimento de autenticação desafio-resposta, e se este for bem sucedido, o servidor de AAA da rede WLAN envia uma mensagem de notificação (EAP-REQ/AKA-*Notification*) ao móvel informando que a autenticação foi bem sucedida.

O uso do EAP-FLAKA acarreta baixa latência de *handover*, devido a uma troca menor de mensagens e a não necessidade de se fazer nenhum tipo de consulta ao HSS, pois o processo de geração dos vetores de autenticação pelo HSS é bastante oneroso. Porém o uso do EAP-FLAKA se restringe aos casos de usuários que retornam com frequência a uma mesma WLAN.

4.2.4.2 – Gerenciamento de chaves

A Figura 4.6 apresenta o diagrama do gerenciamento e distribuição de chaves do EAP-FLAKA.

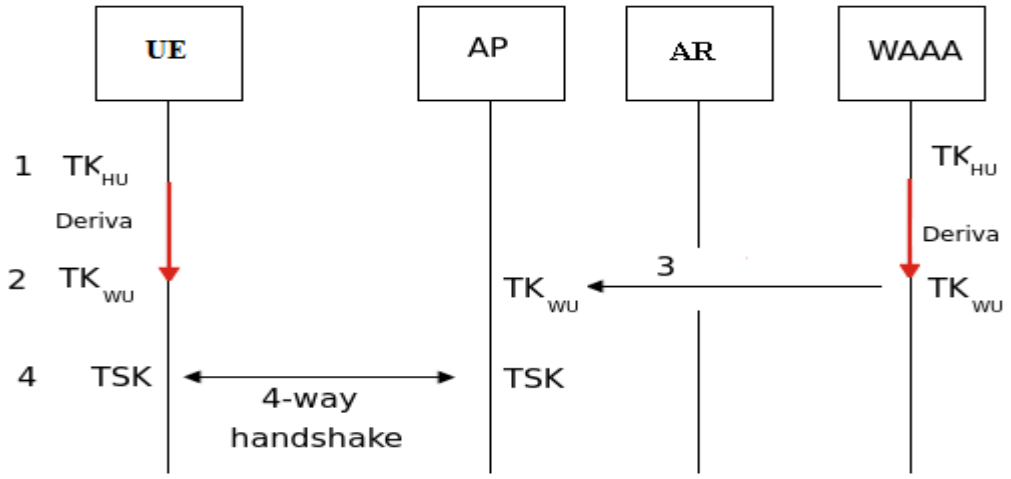

Figura 4.6 – Gerenciamento e distribuição de chaves do EAP-FLAKA.

Neste método é utilizada a chave TK_{HU} gerada anteriormente na autenticação completa do protocolo EAP-FAKA. A partir da TK_{HU}, é derivada a nova chave de autenticação TK_{WU}. Para finalizar, o móvel e o AP geram a *Transient Session Key* (TSK), chave utilizada para a comunicação segura entre essas entidades.

4.2.5 – Protocolo EAP-LUTLS

4.2.5.1 – Descrição do Protocolo

O protocolo de autenticação EAP-LUTLS [33] pode ser utilizado na arquitetura de integração LTE-WLAN apresentada na Figura 3.1, com base no fluxo de mensagens da Figura 4.7, para um *handover* no sentido LTE → WLAN.

Neste protocolo é assumido um pré-compartilhamento de uma chave secreta entre o móvel e o HSS da rede celular. O esquema proposto utiliza de certificados entre os elementos para a autenticação mútua do móvel e da entidade autenticadora. O trabalho apresenta o fluxo de *handover* nos sentidos LTE → WLAN e WLAN → LTE.

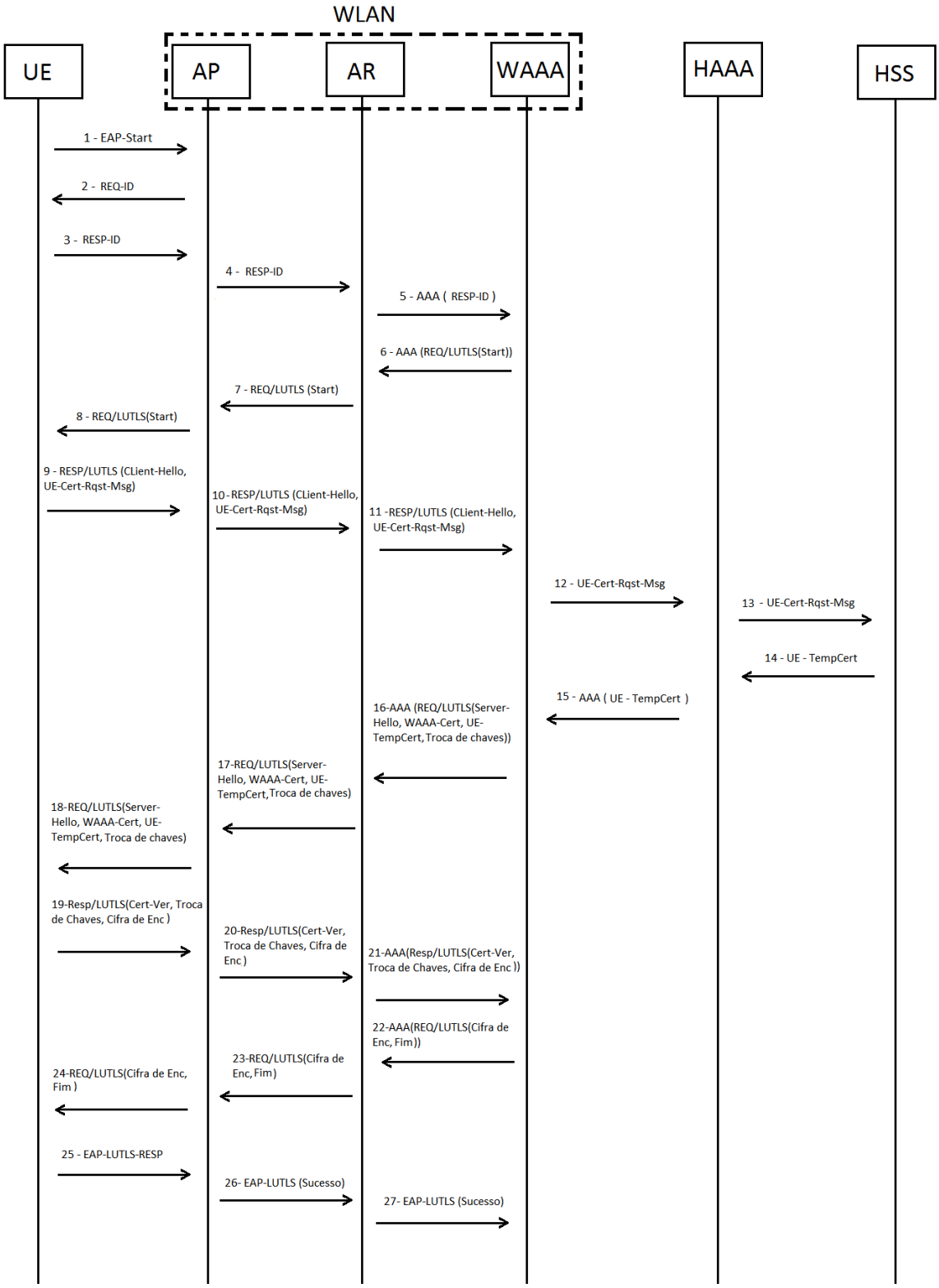

Figura 4.7 – Fluxo de mensagens do protocolo EAP-LUTLS (Baseado em [33]).

No EAP-LUTLS, após a detecção do móvel pela rede WLAN, é realizado o processo de autenticação do móvel. Então o AP requisita o ID do móvel e este envia um Identificador Temporário (TID) para ser substituir pelo seu real ID, desta maneira garantindo a proteção da privacidade do UE. Após estes passos, o WAAA requisita o certificado do UE e este o envia com alguns parâmetros encriptados com a chave pré-compartilhada com o HSS. Após receber a mensagem, o WAAA a repassa ao HSS e este confere o certificado. Se este certificado for válido, significa que o UE é legítimo. Por fim o HSS envia o seu certificado ao UE, e se este certificado for validado pelo móvel, o procedimento de autenticação é bem sucedido.

O uso do EAP-LUTLS, além de diminuir a latência de *handover* pelo fato de utilizar o WAAA como entidade autenticadora, assim como acontece no EAP-FAKA, propicia também segurança a ataques de impersonificação, devido ao uso da chave pré-compartilhada com o HSS, possui autenticação mútua entre o UE e o WAAA e garantia da privacidade do usuário com a utilização de um ID temporário.

Por outro lado, o EAP-LUTLS possui alguns problemas, como a alta de latência de *handover* se comparado a protocolos que utilizam esquemas de preparação para o futuro *handover* e a necessidade de um pré-compartilhamento de uma chave secreta entre o dispositivo móvel e o HSS da rede LTE.

4.2.5.2 – Gerenciamento de chaves

A Figura 4.8 apresenta o diagrama do gerenciamento e distribuição de chaves do EAP-LUTLS:

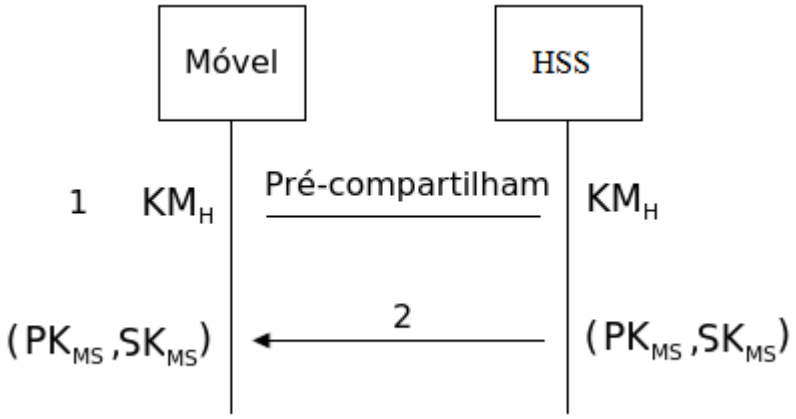

Figura 4.8 – Gerenciamento e distribuição de chaves do EAP-LUTLS.

Este protocolo apresenta uma estrutura de gerenciamento e distribuição de chaves simples. O móvel e o HSS pré-compartilham uma chave secreta KM_H, que será utilizada para a troca de mensagens entre essas duas entidades durante o processo de autenticação. Devido ao uso decertificação digital, o HSS possui seu par de chaves pública/privada (SK_C, PK_C) e gera o par (SK_{MS}, PK_{MS}) utilizado pelo móvel.

4.2.6 – Protocolo proposto por Hassanein, A, H, et al. [35]

4.2.6.1 – Descrição do Protocolo

Neste trabalho os autores propuseram um protocolo para autenticação em redes heterogêneas, visando uma melhoria do EAP-AKA.

Foi utilizada a arquitetura SAE em um *handover* apenas no sentido LTE → WLAN, porém nesse caso não se utilizou um servidor de AAA na rede celular, tendo como pressuposto um canal seguro estabelecido entre o AAA da rede WLAN e o HSS da rede celular.

A Figura 4.9 ilustra o fluxo de mensagens do protocolo proposto:

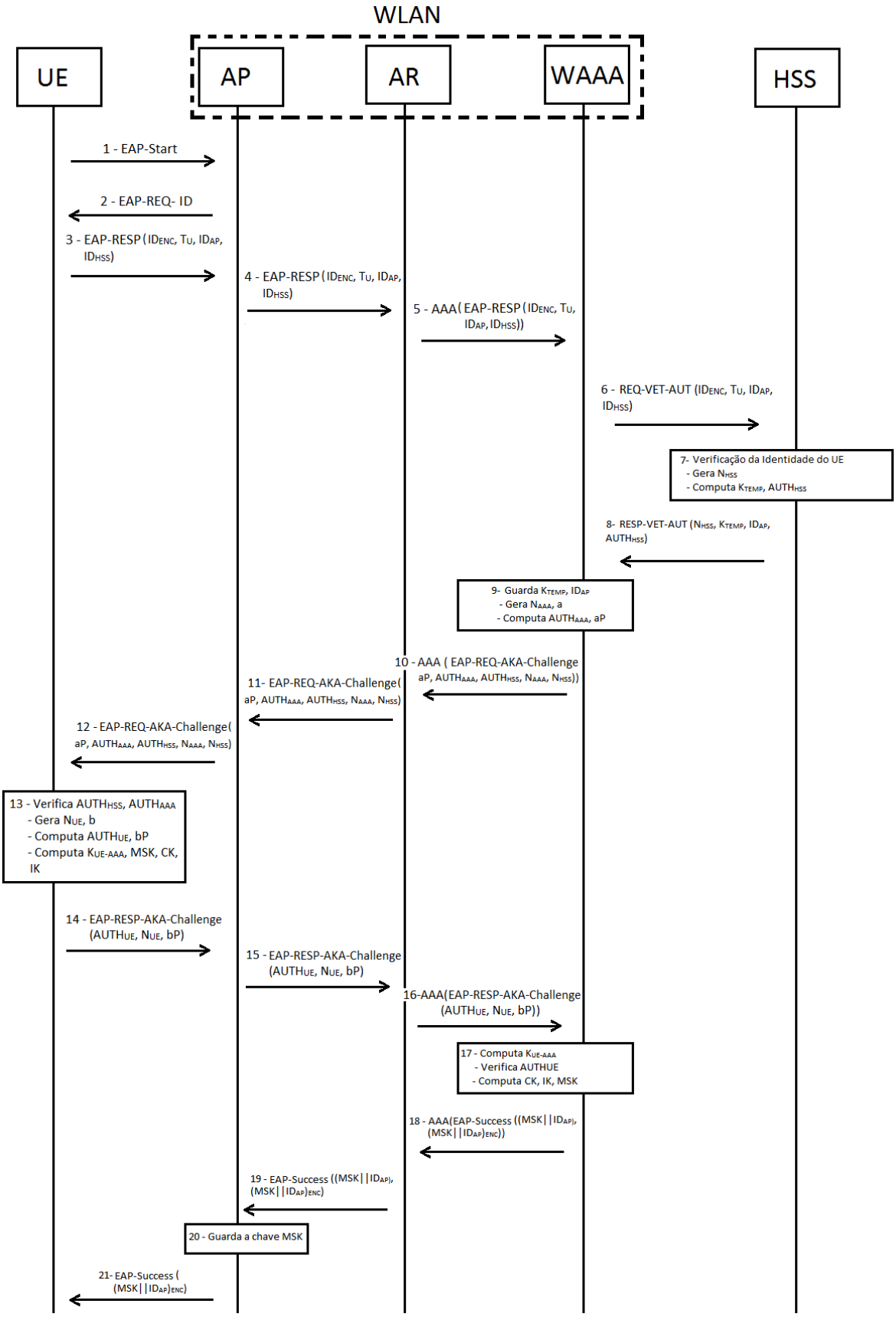

Figura 4.9 – Fluxo de mensagens do protocolo proposto por Hassanein, A, H, et al. ([35]).

Após o UE detectar a rede alvo, o AP requisita algumas informações do UE e este envia seu ID encriptado com uma chave temporária (K_{TEMP}) que foi derivada de uma chave pré-compartilhada com o HSS, o *Timestamp*, o ID do AP e o ID do HSS. O HSS em posse dos dados gera parâmetros que serão utilizados para a autenticação mútua entre o WAAA e o móvel. Logo após, o WAAA envia uma mensagem contendo o seu código de autenticação de mensagem (MAC_{WAAA}) e o MAC_{HSS} encriptados com K_{TEMP}. São enviados também parâmetros que serão utilizados para a geração da chave secreta compartilhada entre o UE e o WAAA ($K_{UE-WAAA}$) através da troca de chaves baseada em *Elliptic Curve Diffie Hellman* (ECDH). De posse dos códigos de autenticação de mensagens, o UE é capaz de autenticar o HSS e o WAAA e gera um código de autenticação de mensagem (MAC_{UE}) utilizando $K_{UE-WAAA}$ e o envia ao WAAA. Ao receber o MAC_{UE}, o WAAA será capaz de autenticar o dispositivo móvel. Se a autenticação do UE por parte do WAAA for bem sucedido, este envia mensagem ao móvel notificando-o do sucesso.

Este protocolo apresenta melhorias em relação ao EAP-AKA, como a proteção do ID do UE, a autenticação mútua entre as entidades e a redução da latência de autenticação com um número menor de mensagens.

Apesar da reduzida latência de autenticação, com a retirada do HAAA no processo de autenticação, o método necessita de uma pequena alteração da arquitetura SAE, a ligação direta WAAA-HSS, alteração que pode não ser viável em redes celulares comerciais.

4.2.6.2 – Gerenciamento de chaves

O diagrama de gerenciamento e distribuição de chaves é mostrado na Figura 4.10. Assim como nos métodos de autenticações anteriores, esta abordagem também faz uso de uma chave secreta pré-compartilhada K_{UE-HSS} entre o móvel e o HSS. A partir de K_{UE-HSS}, o móvel e o HSS derivam uma chave K_{TEMP}, que será utilizada para esconder o verdadeiro ID do móvel. Após gerar K_{TEMP}, o HSS a envia ao WAAA. O móvel e o WAAA geram a chave K_{UE-AAA} derivada de K_{TEMP}, chave utilizada para uma comunicação segura entre o móvel e o WAAA. O WAAA e o móvel geram as chaves IK, CK e MSK. Por último, o WAAA envia a *Master Session Key* (MSK) ao AP.

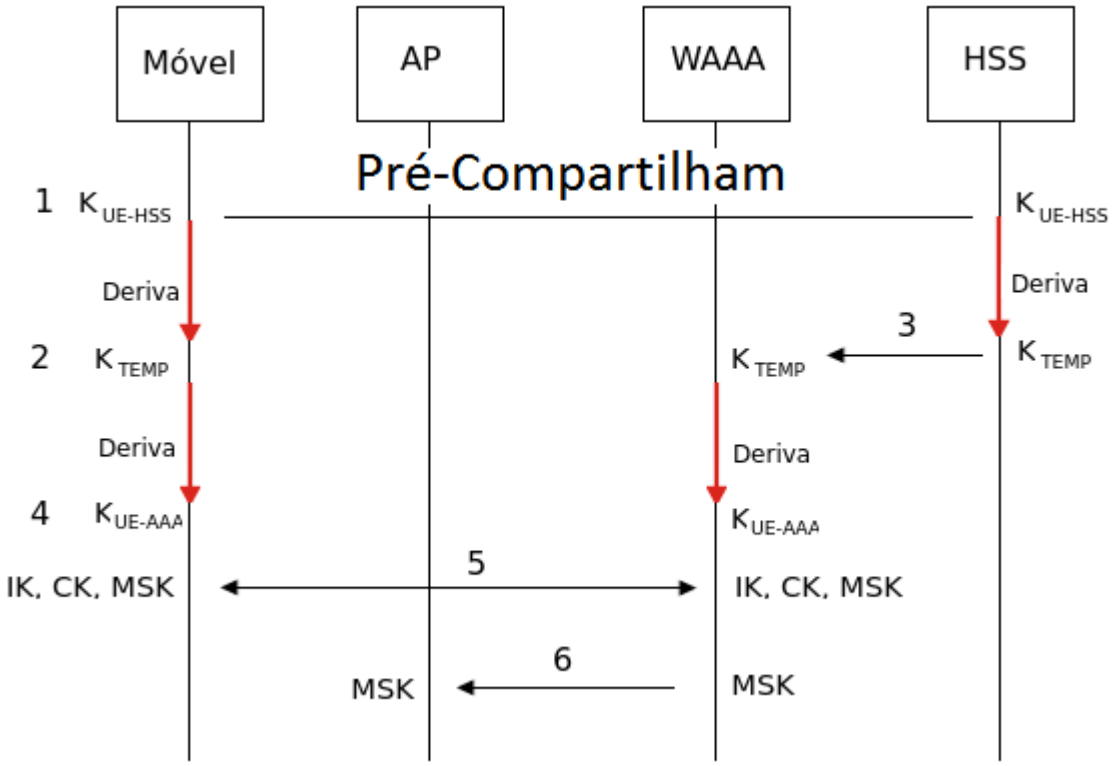

Figura 4.10 – Gerenciamento e distribuição de chaves do protocolo proposto por Hassanein, A., H., et al.[35].

4.2.7 – Protocolo EAP-CRA

4.2.7.1 – Descrição do Protocolo

O EAP-CRA (*Extensible Authentication Protocol-Coordinated Robust Authentication*) é um protocolo proposto inicialmente por [36] e alterado pelos mesmos autores em [37], para autenticação em um *handover* entre redes sem fio heterogêneas. Este protocolo se adequa à arquitetura de integração LTE-WLAN apresentada na Figura 3.1.

Este protocolo é baseado em *Coordinated Robust Authentication*, método em que se utiliza um conjunto único de credenciais nas redes heterogêneas. Na autenticação CRA, um dispositivo primeiramente se associa a uma rede, chamada de *Home Network*, com apenas um único conjunto de credenciais. No caso de um *handover* para uma outra rede, o móvel deve ser capaz de utilizar seu conjunto de credenciais para se autenticar na rede alvo.

Para este método de autenticação, foi assumido que todos os servidores de AAA que participam do processo de autenticação EAP-CRA devem possuir um certificado CA-*Signed* PKI, ou seja, um certificado assinado por uma autoridade certificadora em uma infraestrutura de chave pública. Outra premissa, é que qualquer servidor de AAA pode obter o certificado CA-*Signed* PKI de qualquer outro servidor AAA.

A Figura 4.11 ilustra o fluxo de mensagens do protocolo EAP-CRA:

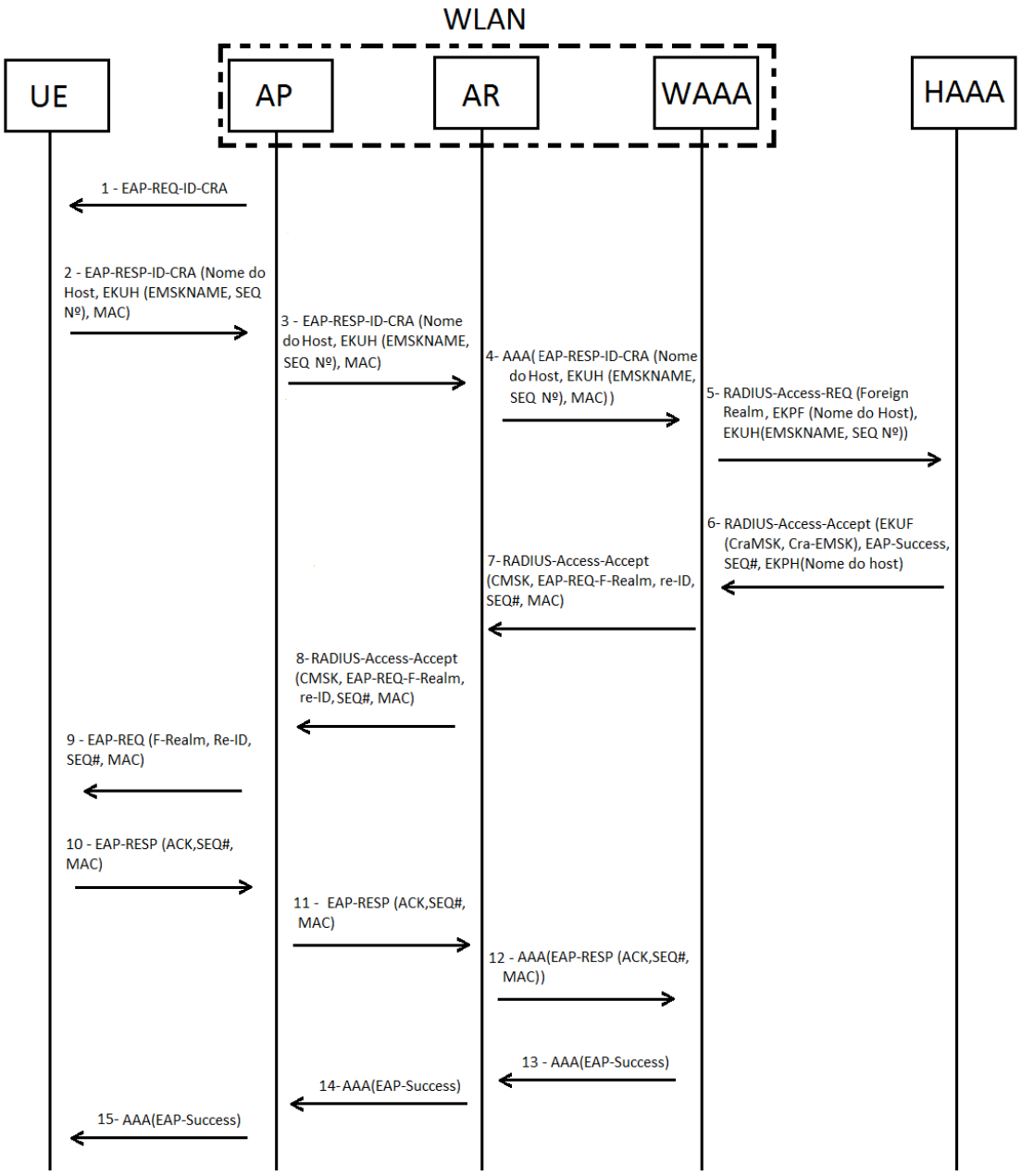

Figura 4.11 – Fluxo de mensagens do protocolo EAP-CRA (Baseado em [36, 37]).

Após a WLAN enviar uma mensagem de EAP-CRA requisitando as informações sobre o UE, este envia uma mensagem contendo seu identificador, o domínio da *Home Network*, dentro outras informações cifradas com a chave pública do HAAA. Ao receber a mensagem, o WAAA irá adicionar seu domínio e irá encriptar a mensagem com a sua chave secreta. Com a posse da chave pública do WAAA, o HAAA consegue autenticar o servidor de AAA da rede WLAN e gera as chaves *masters* de sessão e outros parâmetros de segurança, encripta com a chave pública de WAAA e o envia a rede WLAN. De posse da mensagem, o WAAA checa a validade da mensagem enviada pelo HAAA e grava as chaves de sessão que serão utilizadas em futuras comunicações para prover confidencialidade. Os parâmetros de segurança são enviados ao UE e este responde com uma mensagem de *acknowledgment*. Logo após, o WAAA envia uma mensagem de EAP-*Success*, informando que a autenticação foi bem sucedida.

A grande vantagem desse processo é o fato da *Home Network* realizar o procedimento de autenticação do móvel com base na criptografia de chave pública, isentando o UE de qualquer procedimento de desafio resposta, ou qualquer outro tipo de mecanismo de autenticação. Porém, para isto ser feito, foi assumido que um processo de autenticação robusto foi realizado anteriormente com a *Home Network*.

4.2.7.2 – Gerenciamento de chaves

É apresentado na Figura 4.12 o diagrama de gerenciamento e distribuição de chaves do EAP-CRA:

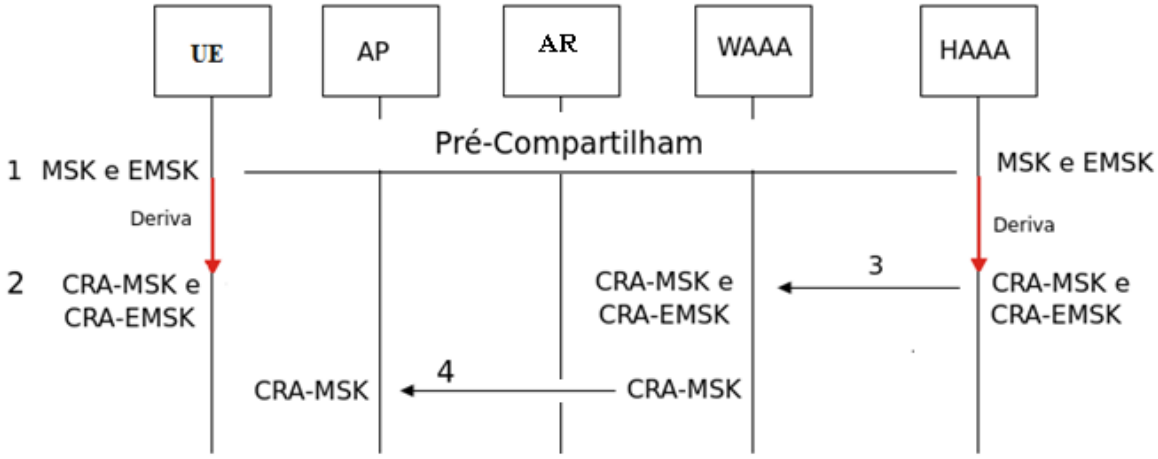

Figura 4.12 – Gerenciamento e distribuição de chaves do EAP-CRA.

Nesta abordagem os servidores de AAA que participam do processo de autenticação EAP-CRA (HAAA e WAAA) devem possuir um certificado *CA-Signed PKI*. As entidades HAAA e WAAA possuem o seu par de chaves pública/privada (PK_{HAAA}, SK_{HAAA}) e (PK_{WAAA}, SK_{WAAA}), respectivamente. O móvel e o HAAA pré-compartilham as chaves de sessão *Master Session Key* (MSK) e *Extended MSK* (EMSK). Para finalizar, o HAAA e o móvel geram as novas chaves de sessão CRA-MSK e CRA-EMSK, que serão utilizadas para prover confidencialidade no processo de reautenticação.

4.2.8 – Protocolo de reautenticação derivado do EAP-CRA

4.2.8.1 – Descrição do Protocolo

Proposto em [37], o protocolo de reautenticação derivado do EAP-CRA é utilizado para os casos em que o usuário retorna com frequência a rede WLAN.

O fluxo de mensagens é mostrado na Figura 4.13:

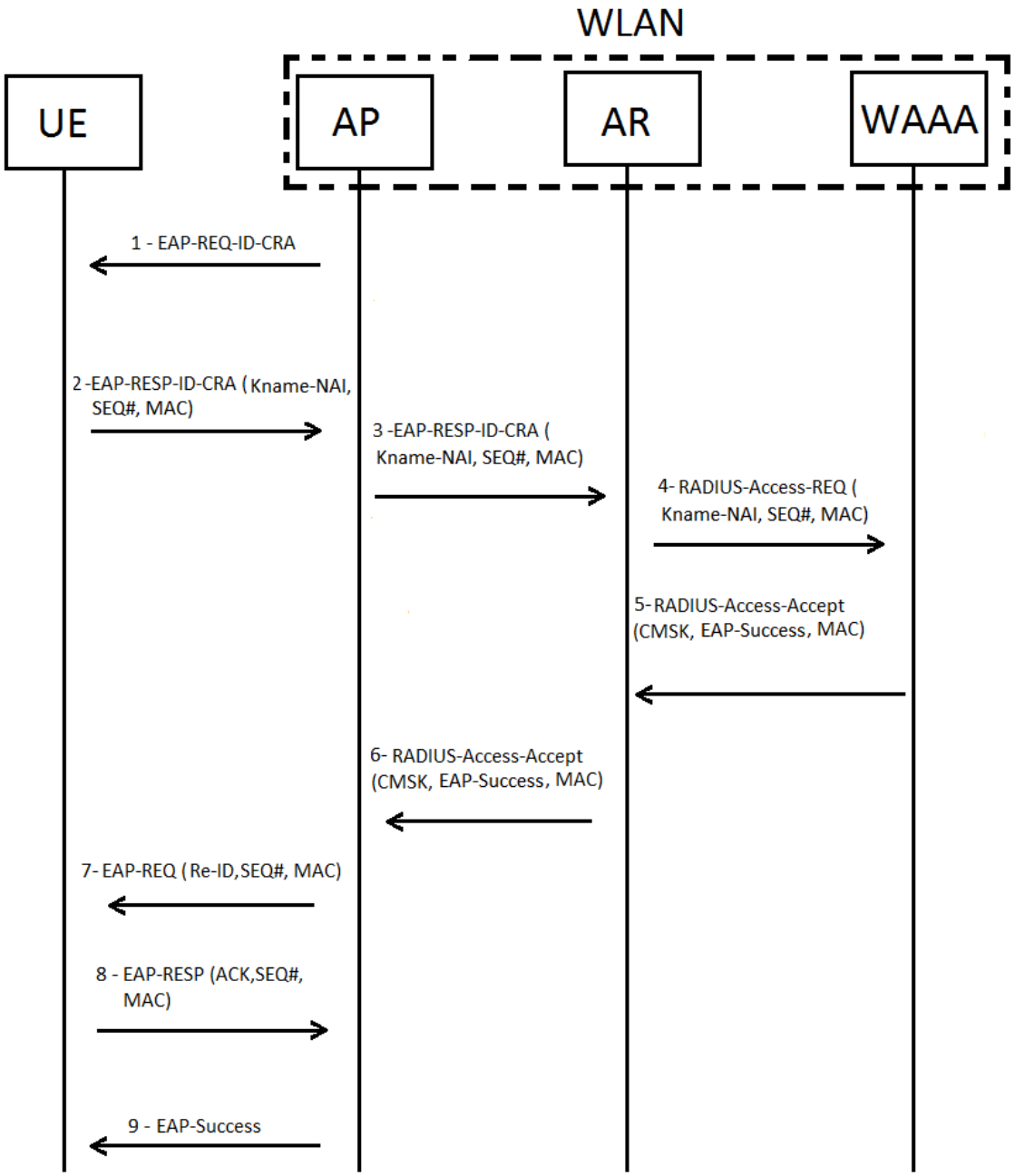

Figura 4.13 - Fluxo de mensagens da reautenticação do EAP-CRA (Baseado em [37]).

No processo de autenticação completa, são geradas duas chaves criptográficas: a CRA-MSK e a CRA-EMSK. A CRA-MSK é utilizada para comunicações na autenticação completa e a CRA-EMSK para os casos de reautenticações. Ao receber a mensagem de EAP-*Request*/*Identity*-CRA, o UE verifica a validade da CRA-MSK, se esta não for mais válida, o móvel irá requisitar a autenticação completa, porém em caso contrário o UE irá enviar seu ID de reautenticação, o nome do seu domínio, um número sequencial aleatório e

o código MAC da mensagem, sendo que este último é gerado a partir da chave CRA-EMSK e o sequencial aleatório. Após receber a mensagem, o WAAA verifica o domínio do UE com o seu repositório de informações de autenticação. Se o domínio for válido, o WAAA checa o MAC da mensagem e incrementa o valor do contador que possui as funções de limitar o número de reautenticações rápidas consecutivas e contribuir com a derivação de chaves. Após isso são trocadas mensagens de sucesso da autenticação.

4.2.8.2 – Gerenciamento de chaves

Este método faz uso das chaves CRA-MSK e CRA-EMSK, geradas anteriormente na autenticação completa do protocolo EAP-CRA, como pode ser visto na Figura 4.12.

4.3 – CONSIDERAÇÕES FINAIS

Neste Capítulo, foram descritos, inicialmente, trabalhos relacionados que possuem o foco principal na redução da latência de *handover* baseados em mecanismos de gerenciamento de mobilidade; em seguida, foram apresentados trabalhos com a finalidade da redução da latência de *handover*, porém baseados em mecanismos de autenticação. Foram detalhados os seguintes dos protocolos de autenticação, de interesse direto para este trabalho: UNAEN, EAP-FAKA, EAP-FLAKA, EAP-LUTLS, Protocolo proposto por Hassanein, A, H, et al., EAP-CRA e o protocolo de reautenticação derivado do EAP-CRA. Para cada protocolo, foram descritos os respectivos fluxos de mensagens e os seus processos de gerenciamento de chaves.

Uma síntese relativa às chaves de "*long term*" (longo prazo) e às chaves de sessão (geradas durante o processo de *handover*) é apresentada na Tabela 4.1.

Tabela 4.1 – Geração de chaves *long term* e de chaves de sessão.

Método de autenticação	**Número de chaves e *long term keys* criptográficos geradas anteriores ao processo de *handover***	**Número de chaves de geradas durante o processo de *handover***
Prot. Proposto	- 1 Par de *long term keys* gerado pelo KGC e enviado ao	- 1 chave criptográfica.

	UE. - 1 Par de *long term keys* gerado pelo KGC e enviado ao AP.	
UNAEN	- 1 Par de *long term keys* gerado pelo KGC e enviado ao UE. - 1 Par de *long term keys* gerado pelo KGC e enviado ao AP.	- 1 chave criptográfica.
EAP-FAKA [31]	- 1 Par de chaves gerado e pré-compartilhado entre o móvel e o HSS.	- 6 chaves criptográficas
EAP-FLAKA [32]	- 1 chave criptográfica gerada anteriormente no procedimento de autenticação completa do EAP-FAKA	- 2 chaves criptográficas.
EAP-LUTLS [33]	- 1 chave gerada e pré-compartilhada entre o móvel e o HSS.	Par de chaves público/privado do UE
Proposto por Hassanein, A., H., et al. [35]	- 1 chave gerada e pré-compartilhada entre o móvel e o HSS. Essa chave é gerada a partir do método *Elliptic Curve Diffie Hellman* (ECDH)	- 5 chaves criptográficas.
EAP-CRA [36]	- 2 chaves geradas e pré-compartilhadas entre o móvel e o HAAA.	- 2 chaves criptográficas.
Reauten. EAP-CRA [37]	- 2 chaves criptográficas geradas anteriormente no procedimento de autenticação completa do EAP-CRA	- Nenhuma chave criptográfica, pois utiliza as chaves geradas anteriormente no procedimento de autenticação completa do EAP-CRA.

5 – PROPOSTA PRELIMINAR DE PROTOCOLO

Este Capítulo irá descrever uma proposta preliminar de protocolo, a partir da descrição de um cenário considerado. As mensagens utilizadas para tratar diferentes eventos, bem como os procedimentos para integração entre as funcionalidades de gerenciamento de mobilidade e preparação para o futuro *handover* são em seguida descritos.

O protocolo PMIPv6 é adotado como base para as alterações propostas, permitindo prover um processo ágil e prático de preparação para um futuro *handover*, bem como os procedimentos necessários para a operação do protocolo.

5.1 – CONSIDERAÇÕES INICIAIS

Em uma integração entre redes com tecnologias de acesso sem fio diferentes, protocolos que utilizam procedimentos de pré-autenticação ou preparação para futuros *handovers* têm se mostrado uma excelente alternativa para a diminuição da latência de *handovers* devido ao baixo número de mensagens trocadas durante o processo de *handover* vertical. Porém os procedimentos relativos a preparação para futuros *handovers* podem se mostrar onerosos e complexos de serem realizados.

Com base na Subseção 4.2.2 do Capítulo anterior, pode-se observar que o UNAEN [30] é um protocolo que realiza um procedimento de preparação para um futuro *handover* e realiza a troca de apenas 3 mensagens durante o *handover* vertical. Todavia, o UNAEN não realiza integração entre a autenticação e o gerenciamento de mobilidade.

Conforme poderá ser constatado, o protocolo proposto, baseado no *Proxy Mobile IPv6* (PMIPv6), realiza a preparação para o futuro *handover* em conjunto com os procedimentos relativos ao gerenciamento de mobilidade. Para isto, foram alteradas as mensagens de *Proxy Binding Update* e *Proxy Binding Acknowledgement*.

Apesar de o protocolo proposto ser baseado no UNAEN e os procedimentos relatados nas seções seguintes serem relativos à preparação para um futuro *handover,* esses mesmos procedimentos podem ser adaptados a protocolos que realizam procedimentos de pré-autenticação.

Nas próximas seções, a partir da descrição do cenário utilizado, serão apresentados os detalhes do protocolo proposto, como o fluxo de mensagens, formato de mensagens, procedimentos de autenticação, procedimentos de desconexão e comparações com o fluxo original.

5.2 – CENÁRIO UTILIZADO

O cenário considerado consiste de um domínio PMIPv6 contendo uma rede 4G, do tipo LTE, e redes WLANs. A rede LTE possui área de cobertura em todo domínio PMIPv6, enquanto as redes WLAN possuem área de cobertura reduzida. Neste cenário, a rede 4G será a rede caseira do dispositivo móvel, enquanto este pode realizar o procedimento de *handover* para qualquer rede WLAN pertencente ao domínio PMIPv6. Todas as redes WLANs pertencentes ao domínio PMIPv6 estão interconectadas à rede LTE, do mesmo modo como mostrado na Figura 3.1. A Figura 5.1 ilustra o cenário proposto:

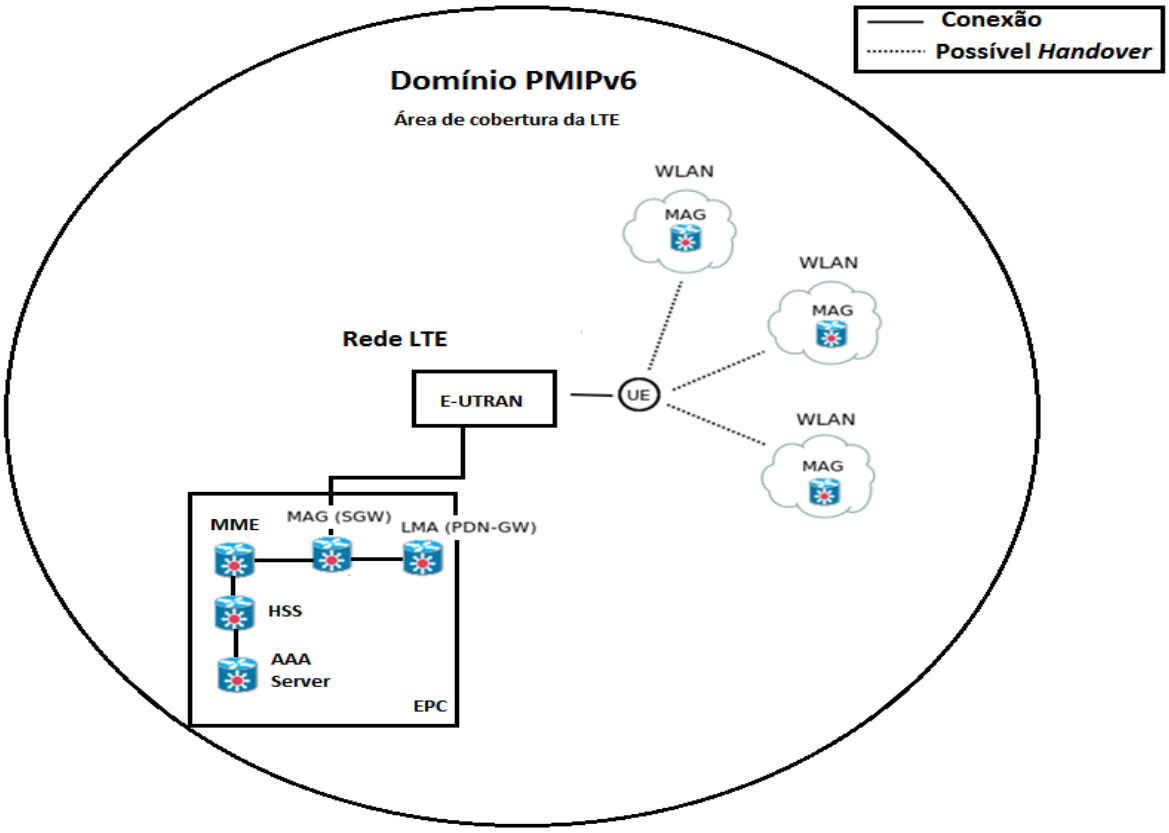

Figura 5.1 – Cenário Utilizado.

No domínio PMIPv6 apresentado na Figura 5.1, o LMA estará contido na rede 4G e o PDN-GW exercerá essa função. A função de MAG será exercida pelo SGW na rede LTE e pelo *Access Router* (AR) nas redes WLANs.

Nesta arquitetura, as redes WLANs são do tipo *trusted*, ou seja, seus elementos de rede possuem uma associação de segurança prévia com a rede EPC.

No protocolo proposto, toda vez que um móvel se conectar a rede LTE, deverá ser realizado o processo de preparação para o futuro *handover*, que será detalhado na Seção 5.3.

5.3 – PROCEDIMENTO DE PREPARAÇÃO PARA O FUTURO *HANDOVER* DO MÓVEL

5.3.1 – Subfase de Inicialização

De acordo com o protocolo UNAEN [30], o procedimento de preparação deverá ser realizado entre o móvel e o Centro de Geração de Chaves (KGC) em duas subfases: Inicialização e Distribuição. A Tabela 5.1 apresenta diversas definições que serão importantes para o entendimento da subfase de Inicialização:

Tabela 5.1 – Definição das notações.

Notação	**Definição**
p	Um k-bit primo
F_p	Um campo finito primo
E/F_p	Uma curva elíptica E sobre F_p
G	$G = \{(x, y) : x, y \in Fp; (x, y) \in E/Fp\} U\{\Theta\}$
P	Gerador para o grupo G
$H_1()$	Uma função de *hash* segura $H_1 : \{0, 1\}^* \times G \rightarrow Z^*$
$H_2()$	Uma função de *hash* segura H2 : $\{0, 1\}^* \times \{0, 1\}^* \times G \times G \times G \times G \rightarrow \{0, 1\}^k$

$H_3()$	Uma função de *hash* segura H_3 : $\{0, 1\}^k \times G \rightarrow \{0, 1\}^k$
T_{exp}	Tempo para expiração
ID_X	Identificador do nó X que é expresso por ID_X = (Endereço MAC (ou outro tipo de identificador) || T_{exp})
x/PK	Chave privada/púlica do KGC, x $\in_R Z^*_p$ e PK = xP
(s_X, R_X)	*Long term keys* do elemento X gerada pelo KGC.

O procedimento de Incialização é feito pelo KGC da seguinte forma:

1 – KGC escolhe um k-bit primo p e determina a tupla $\{F_p, E/F_p, G, P\}$.

2 – KGC escolhe aleatoriamente x $\in_R Z^*_p$ como uma *master key* e computa a chave pública PK= xP.

3 – KGC escolhe três funções seguras de *hash* H1, H2 e H3.

4 – O KGC torna público o sistema de parâmetros $\{F_p, E/F_p, G, P, PK, H1, H2, H3\}$ e mantém a chave x como secreta. Diversos parâmetros de seguranças gerados nessa subfase servirão para a geração das chaves *long term* (de longo prazo) relativas aos dispositivos móveis e *Access Points*.

5.3.2 – Subfase de Distribuição

O procedimento de distribuição é feito em conjunto com os processos relativos ao gerenciamento de mobilidade do PMIPv6, no momento em que é feita a conexão do UE com a rede LTE. A Figura 5.2 ilustra a subfase de Distribuição:

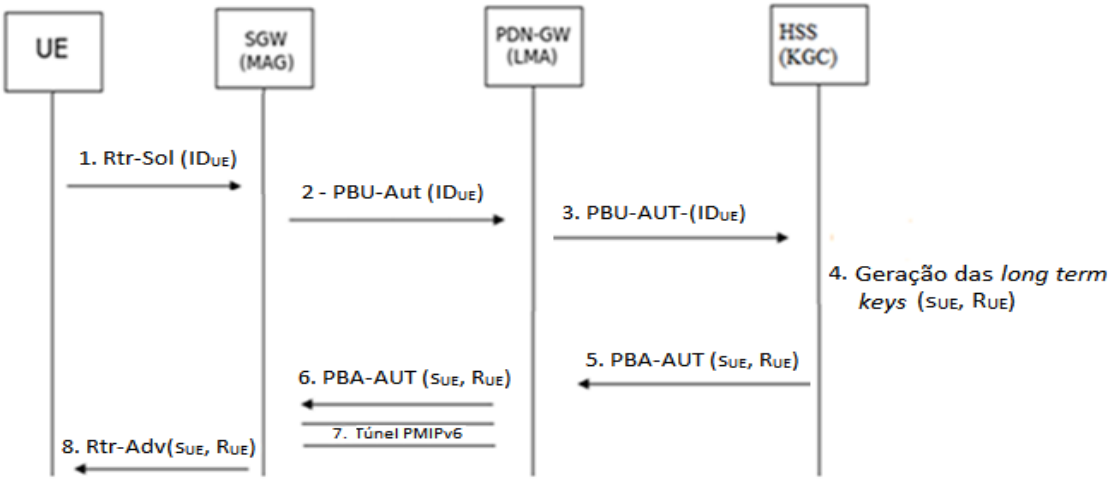

Figura 5.2 – Subfase de Distribuição para o UE.

Durante esta subfase, o KGC envia o par de *long term keys* (s_{UE}, R_{UE}) gerados na subfase de Inicialização para o UE. Esse par de *long term keys* será utilizado durante o procedimento de autenticação (igual ao realizado pelo UNAEN e apresentado na Subseção 4.2.2), realizado durante o *handover*, para a geração de uma chave de sessão entre o móvel e o *Access Point* da rede WLAN. É assumido que já ocorreram o procedimento de autenticação do móvel com a rede LTE e a subfase de Inicialização pelo KGC descrito na Subseção 5.3.1.

A subfase de Distribuição é realizada em conjunto com os procedimentos relativos ao gerenciamento de mobilidade do PMIPv6 no momento em que o UE se conecta a rede LTE. Primeiramente, o móvel envia uma mensagem de *Router Solicitation* ao SGW (MAG) e este envia uma mensagem de *Proxy Binding Update Authentication* (PBU-AUT), contendo o ID (pode ser o IMSI por exemplo) do UE, ao PDN-GW (LMA), solicitando a realização dos procedimentos de gerencia de mobilidade e solicitação das *long term keys* (s_{UE}, R_{UE}). Neste momento, o PDN-GW (LMA) aloca um UE-HNP ao móvel. O PDN-GW então envia a mensagem de PBU-Aut ao KGC, representado pelo HSS, para a realização do procedimento de preparação para o futuro *handover*. De posse do ID do móvel, o KGC realiza o seguinte procedimento, baseado em [30]:

1- Escolhe um número aleatório $r \in_R Z^*_p$ e computa $R_{UE} = rP$ e $h = H_1(ID_{UE} \| RUE)$.

2- Computa $s_{UE} = r + hx$.

Após a geração das *long term keys* ($s_{UE,}$ R_{UE}), o KGC os envia ao PDN-GW na mensagem de *Proxy Binding Acknowledgement-Authentication* (PBA-AUT). Após o recebimento da mensagem de PBA-AUT, o PDN-GW (LMA) configura o seu *endpoint* do túnel bidirecional para o MAG (SGW) e cria a *Binding Cache Entry* (BCE) para o UE. O SGW (MAG) envia uma mensagem de *Router Advertisement* ao nó móvel contendo o UE-HNP e as suas *long term keys*. O UE verifica as suas *long term keys* de acordo com a seguinte expressão:

$$s_{UE}P \equiv R_{UE} + H1(ID_{UE} \,||\, R_{UE})PK \qquad \text{Eq. (5.1)}$$

Por fim, é feita a configuração do endereço do móvel com base no UE-HNP.

Após a realização da fase de Distribuição ser bem sucedida e o UE estiver de posse do seu par de *long term keys* (s_{UE}, R_{UE}), o móvel poderá se autenticar em qualquer WLAN que esteja no domínio PMIPv6. Tomando como base a Figura 5.1, será assumido que o UE já possui o seu par de *long term keys* e que este entre em uma área de cobertura de alguma rede WLAN contida no domínio. Primeiramente deverão ser feitos os procedimentos de descoberta e seleção específicos para redes WLANs e após isso que será realizado o procedimento de *handover* para a rede WLAN alvo. Como o foco deste trabalho são os procedimentos relativos a autenticação e gerenciamento de mobilidade, não será especificado como deverá ser feito a descoberta e seleção da rede WLAN alvo. Durante o procedimento de *handover* o UE irá realizar a autenticação e a geração da chave de sessão com o AP da WLAN alvo. Este procedimento de autenticação é o mesmo realizado na fase de autenticação do protocolo UNAEN [30] e é descrito na Subseção 4.2.2.1. Para o procedimento de autenticação entre o UE e a rede WLAN alvo ser realizado corretamente, o *Access Point* necessitará também do seu par de *long term keys* (s_{AP}, R_{AP}). O procedimento para a geração e distribuição do par de *long term keys* do AP será apresentado na Subseção 5.5.

5.4 – FORMATO DAS MENSAGENS DE PBU-AUT E PBA-AUT

Para o correto funcionamento do protocolo proposto, foi adicionado a *flag* T, indicando que o PBU além de ser responsável por gerenciamento de mobilidade, deverá participar do processo de preparação do móvel. Foi também adicionado a *flag* B, indicando se esta

preparação está sendo realizada pela primeira vez ou então está sendo realizada se a chave privada do AP estiver expirada. Com a adição das *flags* T e B, o campo *Reserved* passou de 9 para 7 bits, como pode ser visto na Figura 5.3:

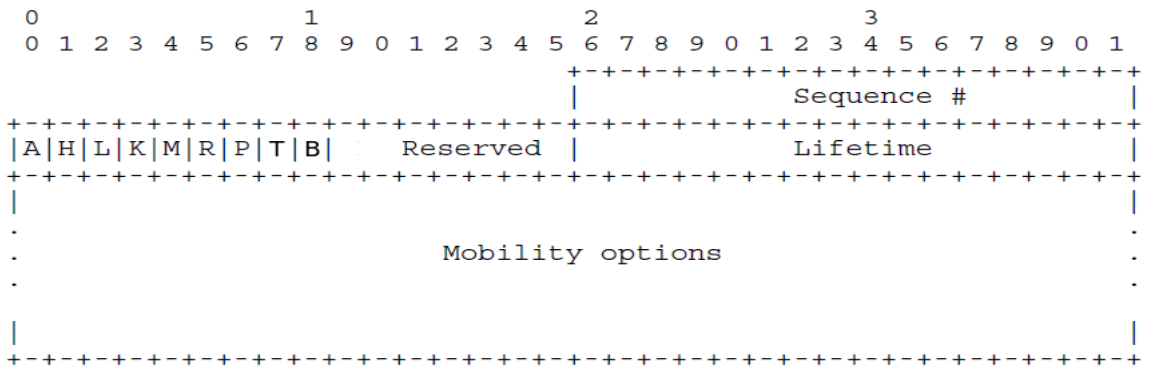

Figura 5.3 – Formato das mensagens de *Proxy Binding Update Authentication.*

Para o caso das mensagens de *Proxy Binding Acknowledgement Authentication*, além da *flag* T e B, foi adicionado a *flag* Y, indicando se o processo de preparação foi realizado com sucesso pelo KGC. A Figura 6.4 ilustra o formato da mensagem de *Proxy Binding Acknowledgement Authentication*.

Os demais campos e *flags* apresentados nas Figuras 5.3 e 5.4 possuem as mesmas funções das mensagens de *Proxy Binding Update*e *Proxy Binding Acknowledgement*, tratadas nas Subseções 3.3.2.1 e 3.3.2.2, respectivamente.

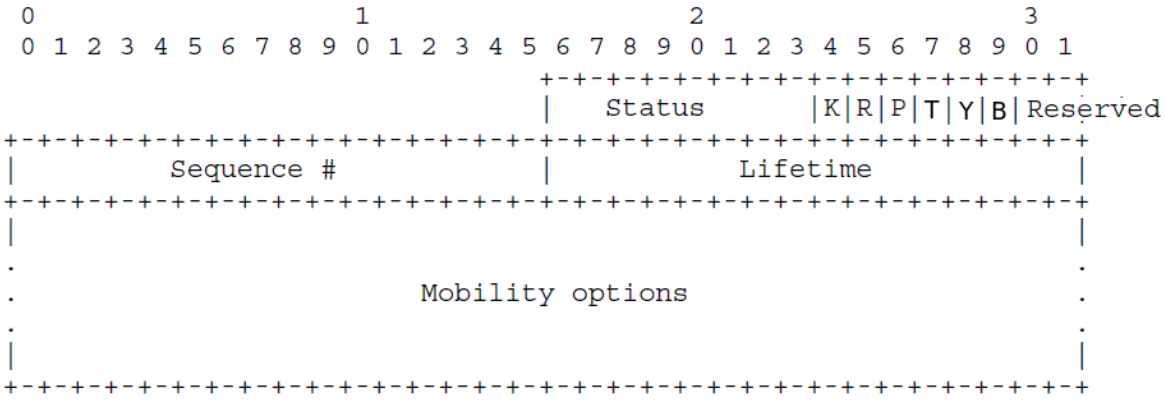

Figura 5.4 - Formato das mensagens de *Proxy Binding Acknowledgement Authentication.*

5.5 – PROCEDIMENTO DE PREPARAÇÃO PARA O FUTURO *HANDOVER* DO *ACCESS POINT*

Um dos pré-requisitos para o correto funcionamento do protocolo UNAEN [30] é de que além do móvel, os APs também devem possuir um par de *long term keys* (s_{AP}, R_{AP}) que serão utilizados no procedimento de autenticação realizados no processo de *handover*, como discutidos na Seção 4.2.2. O procedimento de preparação para os *Access Points* é muito semelhante ao realizado pelo UE, sendo feita primeiramente uma subfase de Inicialização por parte do KGC e outra de Distribuição. A subfase de Inicialização é a mesma apresentada na Subseção 5.3.1, em que o KGC gera diversos parâmetros de segurança que serão utilizados para a derivação das *long term keys* do UE e do AP.

Na subfase de Distribuição, são realizados os procedimentos para a geração e entrega do par de *long term keys* (s_{AP}, R_{AP}) ao AP como apresentado na Figura 5.5:

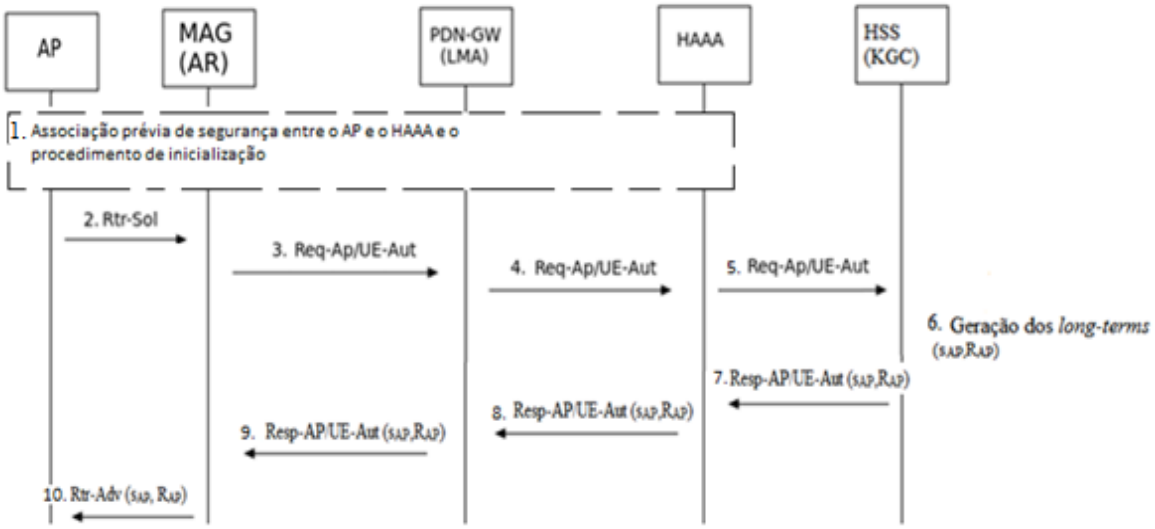

Figura 5.5 – Subfase de Distribuição dos *Access Points.*

Primeiramente, será assumido que já foi feito o procedimento de inicialização por parte do KGC, apresentado na Subseção 5.3.1 e uma prévia associação de segurança entre o AP e o HAAA, por exemplo com o uso do protocolo IKEv2. Durante a subfase de Distribuição, o AP envia uma mensagem de *Router Solicitation* (Rtr-Sol) ao AR (MAG) e este envia uma mensagem de *RequestAP/UE Authentication* (Req-AP/UE-Aut), contendo o ID do AP, ao PDN-GW (LMA) solicitando os *long term keys* (s_{AP}, R_{AP}). O PDN-GW

(LMA) então, envia a mensagem de Req-AP-Aut ao KGC. De posse do ID do AP, o KGC realiza o seguinte procedimento:

1- Escolhe um número aleatório $r \in_R Z^*_p$ e computa $R_{AP} = rP$ e $h = H_1(ID_{UE} \| RUE)$.

2- Computa $s_{AP} = r + hx$.

Após a geração das *long term keys* (s_{AP}, R_{AP}), o KGC as envia ao PDN-GW (LMA) na mensagem de *Response AP/UE Authentication* (Resp-AP/UE-Aut). Após o recebimento da mensagem de Resp-AP/UE-Aut, o AR (MAG) envia uma mensagem de *Router Advertisement* (Rtr-Adv) ao nó móvel o seu par de *long term keys* (s_{AP}, R_{AP}). O AP verifica as suas *long term keys* geradas pelo KGC de acordo com a seguinte expressão:

$$S_{AP}P \equiv R_{AP} + H1(ID_{AP} \| R_{AP})PK \qquad \text{Eq. (5.2)}$$

Para o caso em que a chave privada do AP estiver expirada, o mesmo procedimento mostrado na Figura 5.5 deverá ser realizado.

5.6 – PROCEDIMENTO DE PREPARAÇÃO DO MÓVEL QUANDO A CHAVE PRIVADA ESTIVER EXPIRADA

Para os casos em que a chave privada do móvel estiver expirada, o procedimento de preparação é mostrado na Figura 5.6:

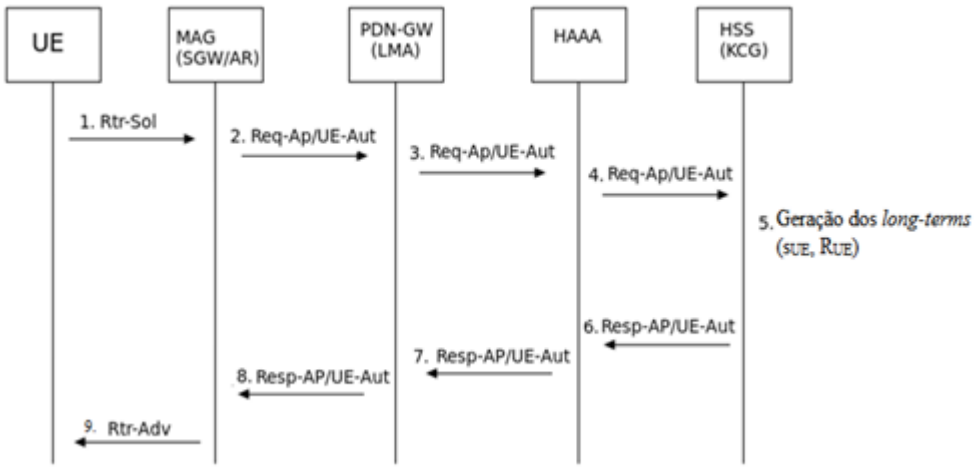

Figura 5.6 - Procedimentos de preparação do UE quando sua chave estiver expirada.

Quando o móvel estiver com sua chave expirada, este irá enviar uma mensagem de *Router Solicitation* (Rtr-Sol) ao MAG, representado pelo SGW, quando o móvel estiver conectado na rede LTE, ou pelo *Access Router*, quando o móvel estiver conectado na WLAN, requisitando os novos pares de *long term keys* (s_{UE}, R_{UE}). O MAG (SGW/AR) envia uma mensagem de Req-AP/UE-Aut, contendo o ID do UE, ao PDN-GW (LMA) para a aquisição de novos parâmetros de segurança. O PDN-GW então envia a mensagem de Req-AP-Aut ao KGC. De posse do ID do UE, o KGC gera o par de *long term keys* (s_{UE}, R_{UE}), da mesma forma como apresentado na Subseção 5.3.2, e os envia ao PDN-GW na mensagem Resp-AP/UE-Aut. Por fim, o MAG envia uma mensagem de *Router Advertisement* (Rtr-Adv) ao móvel contendo o seu par de *long ter keys*.

5.7 – FORMATO DAS MENSAGENS DE *REQUESTAP/UE AUTHENTICATION* E *RESPONSE AP/UE AUTHENTICATION*

A mensagem de *Request AP/UE Authentication* é mostrada na Figura 5.7:

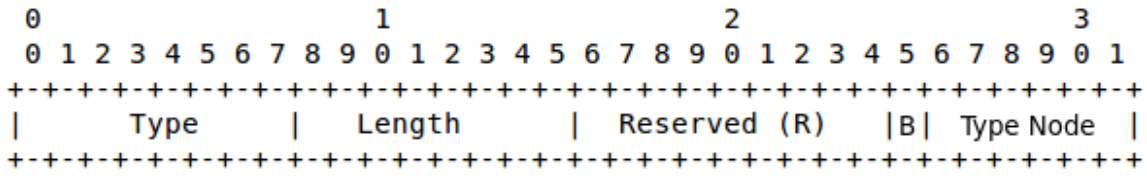

Figura 5.7 - Formato da mensagem de *Request AP/UE Authentication.*

A mensagem de Req-AP/UE-Aut segue o padrão das mensagens do PMIPv6, definidas na RFC 5213 [23], sendo cada campo explicado a seguir:

– *Type*: definido como 28.

–*Lenght*: Seguindo o padrão da RFC 5213, é definido como 2.

–*Reserved*: Este campo por enquanto não é utilizado.

–*Flag* B: Esta flag indica se esta preparação para o futuro *handover* está sendo realizada pela primeira vez ou então está sendo realizada devido a chave privada do AP estiver expirada.

–Type Node: O tipo de dispositivo que está requisitando o processo de preparação para o futuro *handover*:

–0: Reservado;

–1: Dispositivo móvel;

– 2: *Access Point* (AP).

A mensagem de *Response AP/UE Authentication* é mostrada na Figura 5.8:

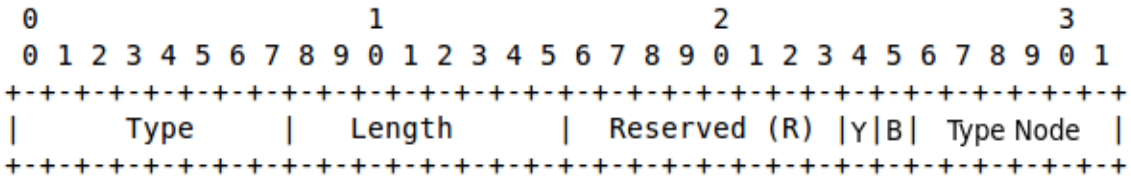

Figura 5.8 - Formato da mensagem de *Response AP/UE Authentication.*

A mensagem de Resp-AP/UE-Aut segue o padrão das mensagens do PMIPv6, definidas na RFC 5213 [23], sendo cada campo explicado a seguir:

– *Type*: definido como 29.

– *Lenght*: Seguindo o padrão da RFC 5213, é definido como 2.

– *Reserved*: Este campo por enquanto não é utilizado.

– *Flag* B: Esta flag indica se esta preparação está sendo realizada pela primeira vez ou então está sendo realizada devido a chave privada do AP estiver expirada.

– *Flag* Y: Esta flag indica se o processo de preparação foi realizado com sucesso pelo KGC.

– *Type Node*: O tipo de dispositivo que foi requisitado o processo de preparação.

– 0: Reservado;

– 1: Dispositivo móvel;

– 2: *Access Point* (AP).

5.8 – PROCEDIMENTO DE *HANDOVER* VERTICAL NO SENTIDO LTE-WLAN

O processo de *handover* quando o móvel se desloca de uma rede LTE para uma rede WLAN no cenário apresentado pela Figura 5.1 é o mesmo descrito pela norma 3GPP TS 23.402 [9] e apresentado na Figura 3.9. A Figura 5.9 apresentta o fluxo de *handover*:

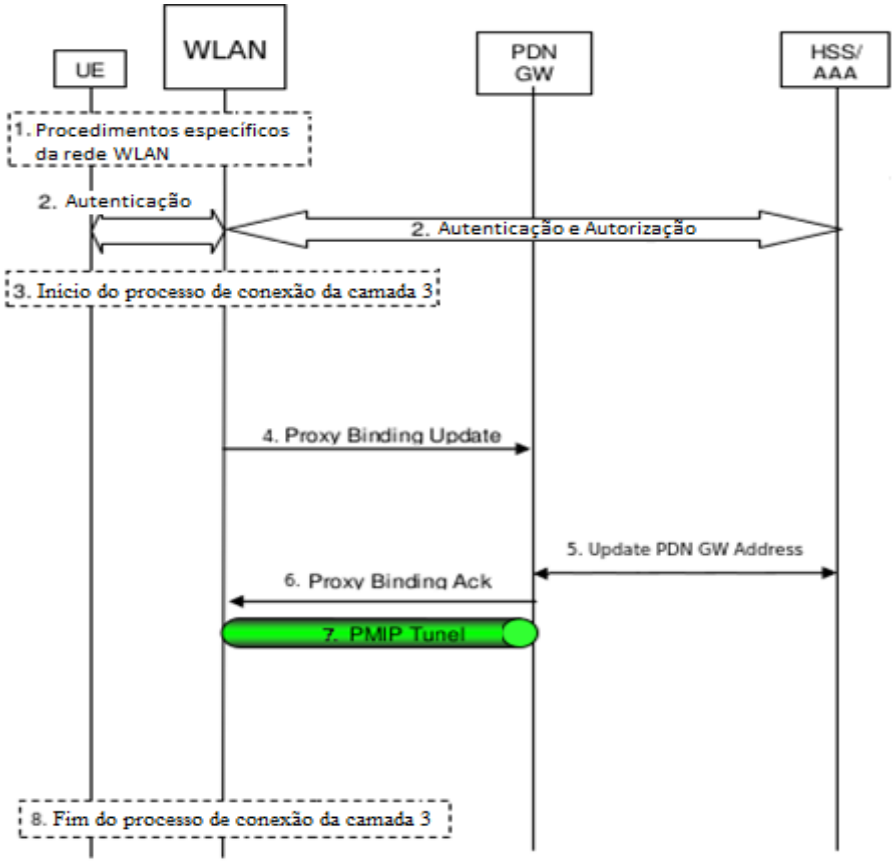

Figura 5.9 – *Handover* vertical no sentido LTE → WLAN (Baseado em [9]).

Primeiramente os procedimentos de *handover* de camada 2 na rede WLAN são realizados. Logo após, é feito o procedimento de autenticação do protocolo UNAEN, descrito na Subseção 4.3.2. Em 3, tem-se o início do processo de conexão L3. Por fim, são realizados os procedimentos de gerenciamento de mobilidade relativos ao protocolo PMIPv6.

5.9 – PROCEDIMENTO DE DESCONEXÃO EM UMA REDE WLAN

O procedimento de *handover* quando o móvel se desconecta da rede WLAN e volta para a sua rede LTE caseira é o mesmo do apresentado na Figura 3.10 e é mostrado a seguir na Figura 5.10:

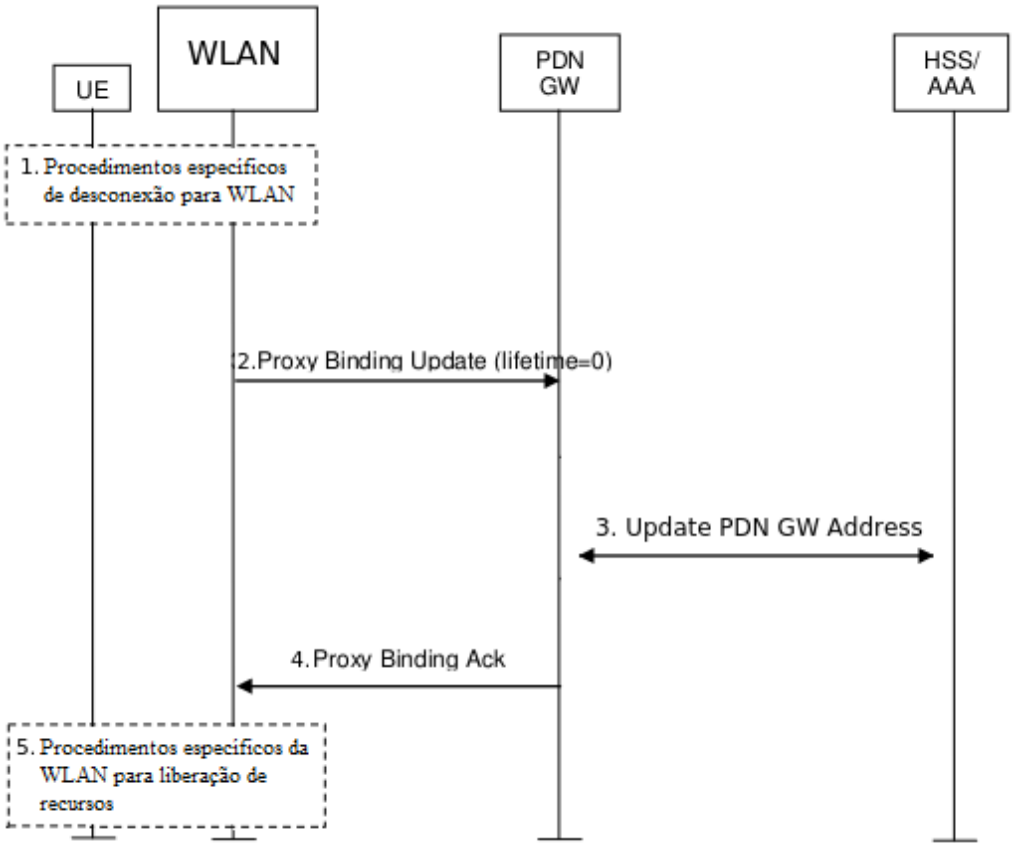

Figura 5.10 – Desconexão com a rede WLAN (Baseado em [9]).

Como a rede LTE é a rede caseira do móvel, não é necessária a autenticação do móvel com a rede 4G novamente, apenas são realizados os procedimentos de desconexão do móvel com a rede WLAN como mostrado na Figura 5.10. O MAG envia uma mensagem de PBU ao PDN-GW, setando o *lifetime* do pacote para zero, indicando uma mensagem de cancelamento de registro do UE. Logo após, o PDN-GW informa ao HSS/AAA da desconexão do UE a rede WLAN. O PDN-GW ao receber a mensagem de PBU, deleta a BCE (*Binding Cache Entry*) do UE e envia uma mensagem de PBA ao MAG da rede WLAN. Por fim, os procedimentos relativos à liberação de recursos da rede WLAN são executados.

5.10 – COMPARAÇÃO COM O FLUXO ORIGINAL DO PMIPV6

Para permitir o correto funcionamento do protocolo proposto, foi alterado o fluxo das mensagens de gerenciamento de mobilidade do PMIPv6, com o objetivode realizar o procedimento de preparação. A Figura 5.11 ilustra o fluxo de mensagens do protocolo PMIPv6:

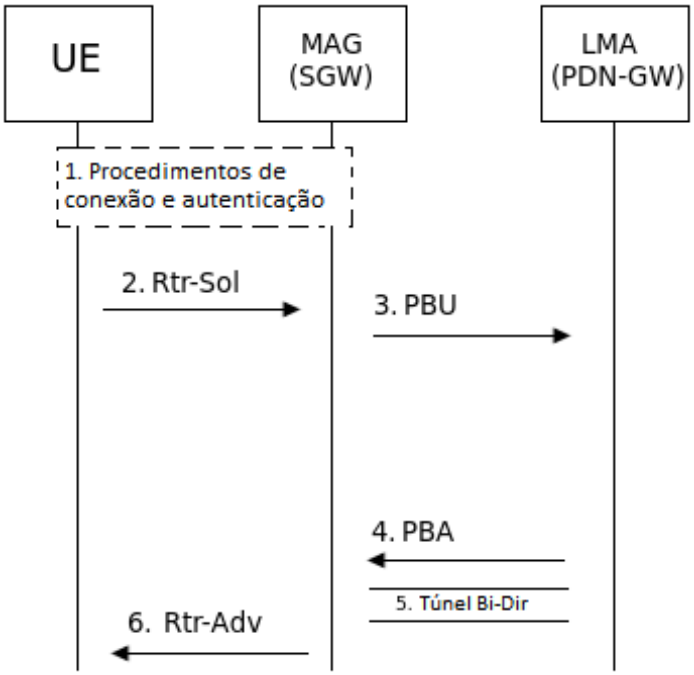

Figura 5.11 – Fluxo de mensagens do PMIPv6 (Baseado em [23]).

Comparando com as Figuras 5.2 e 5.3, pode-se notar que o PMIPv6 troca 8 mensagens a menos do que o protocolo proposto e nenhum procedimento de autenticação é realizado. Porém, durante o *handover* vertical LTE-WLAN, ilustrado na Figura 5.9, o UNAEN irá trocar 3 mensagens com a rede WLAN para o processo de autenticação, enquanto o protocolo EAP-AKA, recomendado para uso pelo 3GPP utiliza 16 mensagens para autenticar o móvel.

5.11 – COMPARAÇÃO DA PROPOSTA PRELIMINAR COM O UNAEN

A Figura 5.12 apresenta o fluxo de mensagens para a subfase de distribuição e os procedimentos relativos ao gerenciamento de mobilidade do PMIPv6 para o UNAEN.

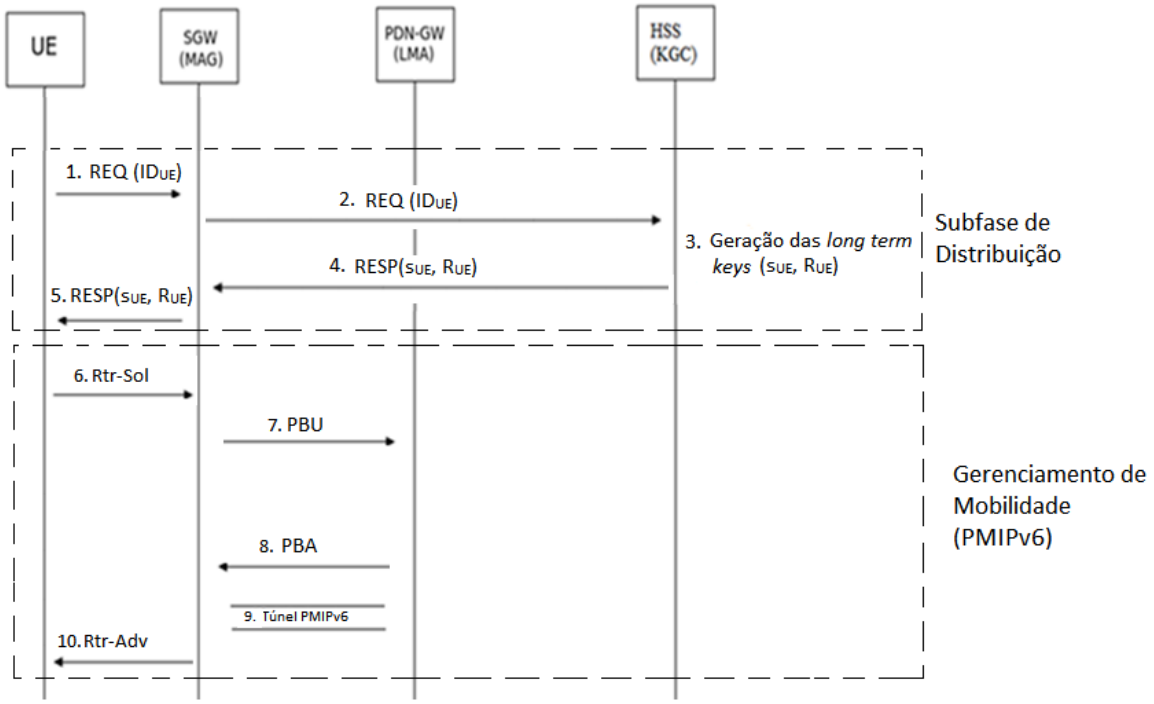

Figura 5.12 – Fluxo de mensagens da subfase de distribuição em conjunto com o PMIPv6 para o UNAEN.

A Figura 5.12 apresenta o fluxo de mensagens para o UNAEN para a subfase de Distribuição em conjunto com os procedimentos relativos ao gerenciamento de mobilidade do PMIPv6. Comparando com o fluxo de mensagens do protocolo proposto, apresentado na Figura 5.2, que une a subfase de Distribuição com os procedimentos relativos ao PMIPv6, o UNAEN troca 2 mensagens a mais do que o protocolo proposto. O ganho do protocolo proposto se deve no fato da realização em da subfase de distribuição em conjunto com o gerenciamento de mobilidade.

5.12 – GERENCIAMENTO DE CHAVES

O gerenciamento e distribuição de chaves do protocolo proposto é igual ao do protocolo UNAEN apresentado na Subseção 4.3.2.2. O diagrama de gerenciamento de distribuição de chaves do protocolo é mostrado na Figura 5.13:

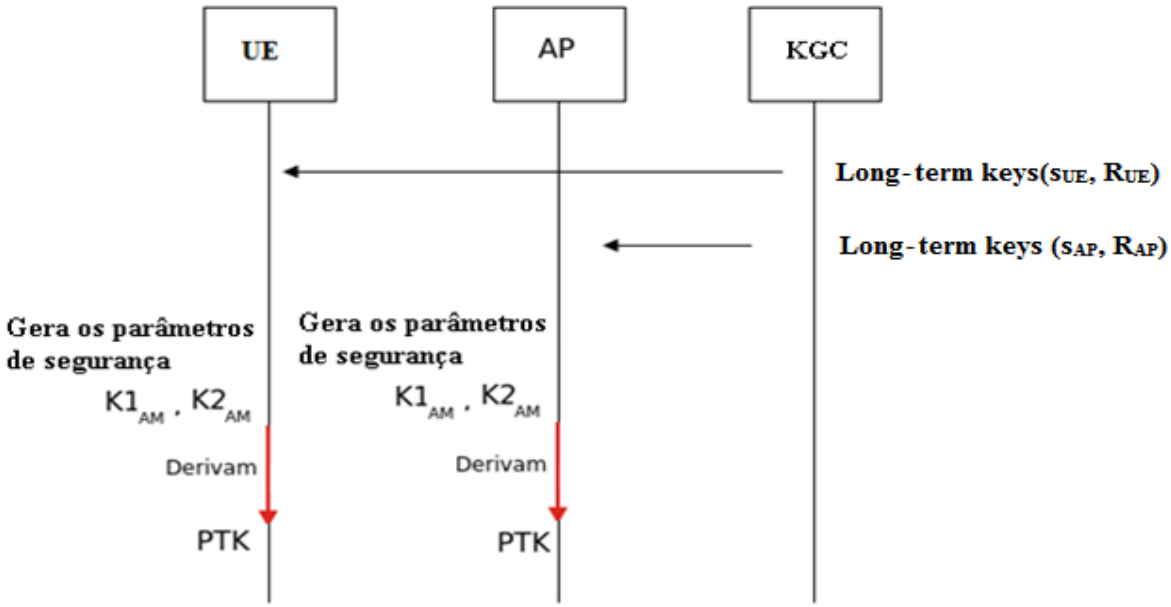

Figura 5.13 – Gerenciamento e distribuição de chaves do protocolo proposto.

Durante a fase de preparação, além de o KGC possuir seu par de chaves privada/pública x/PK, gera as chaves *long term* do móvel (s_{UE}, R_{UE}) e do AP (s_{AP}, R_{AP}).

Durante a fase de *handover*, são geradas as chaves $K1_{AM}$ e $K2_{AM}$ que são utilizadas para autenticação mútua do móvel e a rede WLAN. Por fim, o móvel e o AP geram a chave *Parwise Transient Key* (PTK), derivada de $K1_{AM}$ e $K2_{AM}$.

5.13 – CONSIDERAÇÕES FINAIS

Neste Capítulo foi apresentado o protocolo proposto, cuja finalidade é fornecer um processo ágil e prático de preparação para um futuro *handover* ao protocolo UNAEN e também os procedimentos necessários à realização do gerenciamento de mobilidade

baseado no PMIPv6. Apesar do protocolo proposto ter sido desenvolvido com base no protocolo UNAEN, ele pode ser adaptado para prover a pré-autenticação ou preparação para um futuro *handover* para protocolos que utilizam estes procedimentos, com base no PMIPv6. Assim como o protocolo UNAEN, o protocolo proposto pode ser utilizado para uma integração entre uma rede do padrão 3GPP e outra que não seja do padrão 3GPP, não especificando qual deve ser as redes de acesso utilizadas, pois as mensagens de preparação para um futuro *handover* são trocadas entre os elementos da rede de núcleo EPC (*Evolved Packet Core*).

6 – AVALIAÇÃO DE DESEMPENHO DOS PROTOCOLOS

Neste Capítulo, será realizada a avaliação de desempenho do protocolo proposto e dos protocolos estudados anteriormente, com base em três estudos de caso. No primeiro estudo de caso será avaliada a latência de *handover*, em um cenário de *handover* vertical no sentido LTE → WLAN. No segundo estudo de caso será avaliada a latência e a sinalização de *handover* em um cenário de *handover* horizontal entre redes WLANs em que a rede LTE é a rede caseira do móvel. No terceiro estudo de caso utilizou-se o mesmo cenário do segundo estudo de caso, mas considerando outros aspectos relativos à modelagem analítica.

Por fim, será feita uma comparação entre os protocolos em termos das propriedades de segurança a que atendem ou não.

6.1 – PRIMEIRO ESTUDO DE CASO

Trata-se aqui de cenário de *handover* no sentido LTE → WLAN, cuja relevância se prende, por exemplo., à possível implementação futura de estratégias de *data offloading*, passíveis de utilização para tratar problemas de congestão na LTE. Será considerado as retransmissões na interface aérea e será utilizado um modelo com base na teoria de filas para modelar os atrasos em cada elemento da rede, permitindo avaliar a latência de *handover*.

6.1.1 – Arquitetura Alvo

A Figura 6.1 ilustra a arquitetura alvo utilizada para a análise de dados:

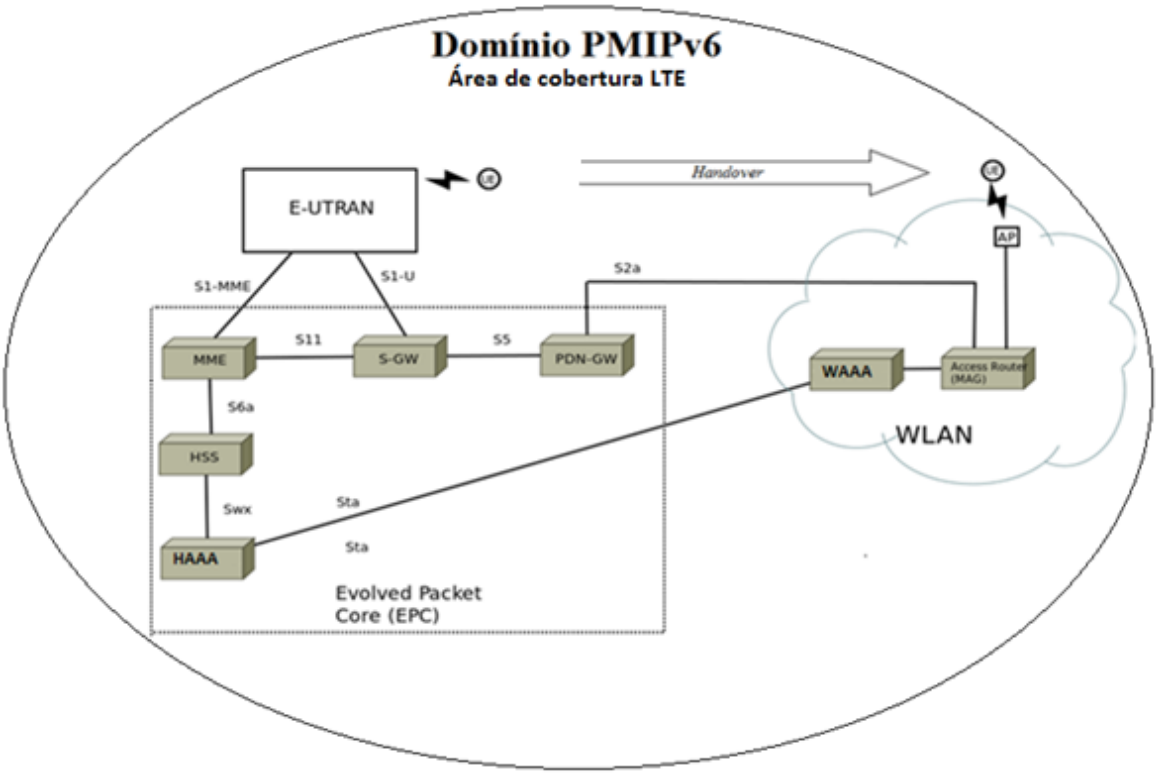

Figura 6.1 – Arquitetura alvo utilizada (Baseada em [9]).

A arquitetura alvo apresentada na Figura 6.1 é composta de uma rede LTE e uma rede WLAN interligadas por uma rede de núcleo do tipo EPC e contidas em um mesmo domínio PMIPv6. Neste cenário, a área de cobertura da rede LTE compõe todo o domínio PMIPv6, enquanto a área de cobertura da rede WLAN é limitada e interna à área de cobertura da rede LTE. Nesse caso, o *Access Router* exercerá o papel de MAG e o PDN-GW executará as funções de LMA no protocolo PMIPv6.

O fluxo de mensagens utilizado para todos os métodos de autenticação durante o *handover* vertical no sentido LTE → WLAN é ilustrado na Figura 3.9, com a realização dos procedimentos de autenticação do móvel na rede WLAN e posteriormente o uso do PMIPv6 para prover o gerenciamento de mobilidade. Nesse caso, como o móvel já possuía um endereço IP no domínio PMIPv6, durante o *handover* não será necessário a realização de nenhum procedimento para configurações de endereço de camada 3.

Quando se fizer o uso do protocolo proposto, será considerado que os procedimentos relativos a pré-autenticação e/ou preparação para o futuro *handover*, discutidos na Seção 5,

já foram realizados e nesse caso apenas os procedimentos relativos a autenticação durante o *handover* deverão ser feitos.

Nesta arquitetura alvo, a rede WLAN será do tipo *trusted* e a rede LTE será a rede caseira do móvel.

Como as redes LTE e WLAN estão contidas no mesmo domínio PMIPv6 e a WLAN é do tipo *trusted*, será considerado que as duas redes estarão geograficamente próximas, dessa forma os servidores de AAA das duas redes e o PDN-GW estarão co-localizados e a interconexão com o AR será feita diretamente, evitando que o tráfego entre os elementos dessas duas redes seja repassado através da internet.

6.1.2 – Modelagem para o atraso de interface aérea em redes WLANs

Será considerado o modelo proposto por [38] para modelar os atrasos em uma interface aérea para redes WLANs. Essa modelagem é utilizada por recentes trabalhos, como em [39 – 41].

Para um protocolo que possui controle de retransmissões e o atraso de propagação fim a fim igual a T', o atraso médio para se transmitir um pacote na em "n" retransmissões é dado por:

$$T = T' + RTO_1 + RTO_2 + ... + RTO_n . \quad \text{Eq. (6.1)}$$

Considerando que o valor do atraso de retransmissão inicial é RTO_0 e o valor de RTO_i é multiplicado por um constante c a cada retransmissão para se ter um aumento exponencial do tempo de retransmissão, ou seja, $RTO_{i+1} = c*RTO_i$, então o atraso de retransmissão dado pela Equação (6.1) pode ser expresso por:

$$T = T' + cRTO_0 + c2RTO_0 + ...+ c_nRTO_0 ,$$

$$T = T' + cRTO_0 \sum_{i=0}^{n-1} c^i ,$$

$$T = T' + cRTO_0 . \frac{(1-c^n)}{(1-c)}. \quad \text{Eq. (6.2)}$$

Sendo p, a probabilidade de um quadro (*frame*) estar com erro no enlace aéreo e k, o número de quadros do enlace aéreo contidos no pacote, então a taxa de perda de pacotes "q" é dada por (6.3):

$$q = 1 - (1-p)^k. \qquad \text{Eq. (6.3)}$$

Após definir "q" através da Equação (6.3), a probabilidade de se transmitir um pacote com sucesso em não mais do que "Nm" retransmissões é dada por (6.4):

$$(1-q) + (1-q)q + (1-q)q^2 + ... + (1-q)q^{Nm} = 1 - q^{Nm} . \qquad \text{Eq. (6.4)}$$

Combinando as equações (6.2) e (6.4), o atraso médio para transmitir um pacote com sucesso sobre a interface WLAN é dado pela expressão (6.5):

$$D' = (1-q)[D+(k-1)\,\tau] + ... + (1-q)q^{Nm}[D+(k-1)\,\tau + cRTO_0\frac{(1-c^n)}{(1-c)}] ,$$

$$D' = [D+(k-1)\tau]\,[1 - q^{Nm}\,] + cRTO_0\frac{1-q}{1-c}]\,[\frac{1-q^{Nm}}{1-q} - \frac{1-q^{Nm}c^{Nm}}{1-qc}\,], \qquad \text{Eq. (6.5)}$$

em que D é o atraso de propagação fim a fim, τ é o tempo entre os quadros e (k-1) é a quantidade de tempos inter-quadros existentes. Como as mensagens trocadas na interface aérea da WLAN possuem comprimento máximo menor do que 1023 bytes, o valor de k será igual a 1, pois o padrão IEE 802.11 especifica que o tamanho máximo do *payload* é 1023 bytes.

Considerando k = 1 e c = 2, como utilizado em [17], a Equação (6.5) é expressa por (6.6):

$$D' = D[1 - q^{Nm}\,] + 2RTO_0(1-q)[\frac{1-q^{Nm}2^{Nm}}{1-2q} - \frac{1-q^{Nm}}{1-q}\,] . \qquad \text{Eq. (6.6)}$$

O número de retransmissões máximas de um pacote na interface WLAN irá variar para cada protocolo e este valor normalmente é sugerido pela RFC do protocolo em questão, por exemplo, como no protocolo EAP (RFC 3748 [14]) em que este número é igual a 5.

6.1.3 – Modelagem Analítica

Nesta subseção, será feita a modelagem analítica que será utilizada para a avaliação da latência de *handover* considerando a utilização de filas do tipo M/M/1 nos elementos de redes, semelhante à modelagem feita em [17].

Para a análise da latência do *handover* utilizando a teoria clássica de filas, será tomada como base a Figura 6.4, que ilustra o modelo sentido terminal → rede e rede → terminal:

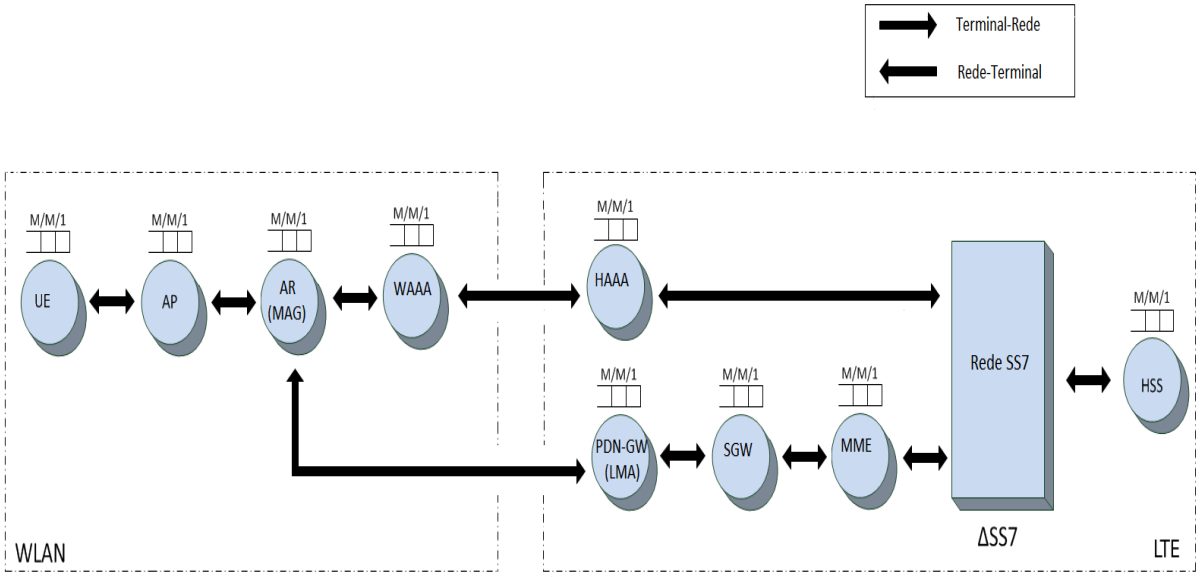

Figura 6.2 - Modelo de filas para análise da latência de *handover* (Baseada em [17]).

Será feita uma análise com base na Figura 6.2, considerando que cada elemento da rede é formado por uma fila do tipo M/M/1, e o atraso de processamento para cada nó da rede é descrito pela Equação (6.7):

$$D_{elemento} = \frac{a}{\mu t\_n + \lambda t\_n} + \frac{b}{\mu n\_t + \lambda n\_t}, \qquad \text{Eq. (6.7)}$$

em que μ_{t_n} é a taxa média de processamento para um determinado elemento no sentido terminal → rede; μ_{n_t} é a taxa média de processamento para um determinado elemento no sentido rede → terminal; λ_{t_n} é a taxa média de chegada para um determinado elemento no sentido terminal → rede; λ_{n_t} é a taxa média de chegada para um determinado elemento no sentido rede→ terminal; "a" e "b" indicam o número de mensagens trocadas no sentido terminal → rede e rede → terminal, respectivamente.

Seguindo o proposto pelo Teorema de Burke [46], o atraso total de cada rede de fila em um sistema aberto pode ser calculado como a soma dos atrasos individuais de cada nó, e considerando que o processo de autenticação envolve troca de sinalização bidirecional com os elementos da rede, a latência de *handover* para os protocolos de autenticação tratados até aqui é dada pela Equação (6.8):

$$D_{Prot\text{-}Aut} = D_{EAP} + D_{UE} + D_{AP} + D_{AR} + D_{AAA\_WLAN} + D_{AAA\_LTE} + D_{HSS} + D_{PDN\text{-}GW} + D_{S\text{-}GW} + D_{MME,} \quad \text{Eq. (6.8)}$$

em que os atrasos D_{UE}, D_{AP}, $D_{AR,}$ $D_{AAA\_WLAN,}$ D_{AAA_LTE}, $D_{PDN\text{-}GW,}$ $D_{S\text{-}GW}$ e D_{MME} são dados pela Equação (6.7); D_{EAP} é o atraso de propagação de mensagens EAP através da interface WLAN. Este atraso é dado por M_{wl}.D', em que M_{wl} é o número de mensagens trocadas através da interface WLAN e D' é dado pela Equação (6.6); e o atraso relativo a uma consulta ao HSS (D_{HSS}) é dado por (6.9):

$$D_{HSS} = \Delta HSS + 2\Delta SS7 \quad \text{Eq. (6.9)}$$

6.1.4 – Avaliação da Latência de *Handover*

Nesta subseção, será feita a avaliação da latência de *handover* em função da taxa de erro de quadros (FER) apresentada na Eq. (6.6).

Para auxiliar a avaliação de desempenho, a Tabela 6.1 mostra a quantidade de mensagens relativas à autenticação, trocadas entre cada elemento durante o procedimento de *handover* para cada protocolo de autenticação:

Tabela 6.1 - Troca de mensagens relativas à autenticação entre elementos.

Método de autenticação	**UE←→AP**	**AP←→AR**	**AR←→WAAA**	**WAAA ←→HAAA**	**HAAA←→HSS**	**WAAA ←→HSSS**
UNAEN [30] / Prot. Proposto	3 mensagens	-	-	-	-	-
EAP-FAKA [31]	6 mensagens	4 mensagens	4 mensagens	4 mensagens	2mensagens	-
EAP-FLAKA [32]	6 mensagens	4 mensagens	4 mensagens	-	-	-
EAP-LUTLS [33]	9 mensagens	7 mensagens	7 mensagens	2 mensagens	2 mensagens	-

Proposto por Hassanein, A., H., et al. [35]	6 mensagens	4 mensagens	4 mensagens	-	-	2 mensagens
EAP-CRA [36]	5 mensagens	4 mensagens	4 mensagens	2 mensagens	-	-
Reauten. EAP-CRA [37]	5 mensagens	2 mensagens	2 mensagens	-	-	-

A Tabela 6.2 mostra a quantidade de mensagens relativas ao gerenciamento de mobilidade, trocadas entre cada elemento durante o procedimento de *handover*:

Tabela 6.2 - Troca de mensagens relativas ao gerenciamento de mobilidade.

Método de autenticação	**AR←→PDN-GW**	**PDN-GW ←→SGW**	**SGW←→MME**	**MME←→HSS**	**HSS←→HAAA**
UNAEN [30] / Prot. Proposto	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
EAP-FAKA [31]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
EAP-FLAKA [32]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
EAP-LUTLS [33]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
Proposto por Hassanein, A., H., et al. [35]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
EAP-CRA [36]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens
Reauten. EAP-CRA [37]	2 mensagens	2 mensagens	2 mensagens	2 mensagens	2 mensagens

Foi feito um mapeamento, mostrado na Tabela 6.3, dos parâmetros contidos em [42] com os contidos nos métodos de autenticação estudados [30] – [34] e [35] - [37], para o auxílio da modelagem de dados.

Tabela 6.3 – Mapeamento dos parâmetros contidos em [42].

Parâmetros contidos Tabela 3.1 de [42]	**Parâmetros utilizados nos métodos de autenticação**	**Tamanho (Bytes)**	**Tipo**
TL-ID	[30] - ID_{UE}, ID_{AP}; [31] – ID_{TE}, ID_{NTE}; [32] - ID_{NTE}; [33] – TID [36] – re-ID [37] - re-ID	16	Identificadores temporários
HN	[30] - R_{UE}, T_{UE} , R_{AP}, T_{AP}; [31] – RAND, XRES, AUTN; [32] – $RAND_w$, R_W; [35] – $AUTH_{HSS}$, N_{HSS}, b	16	*Nonces* gerados pelo HAAA/HSS
-	[30] - $H_1(.)$, $H_2(.)$, $H_3(.)$ [33] – H(.)	16	Funções de *Hash*
MN	[31] – R_{UE} [33] - R_{MS} , n_{MS}, ChainC-CA [35] – N_{UE}, $AUTH_{UE}$, b	16	*Nonces* gerados pelo móvel
CK	[31] – CK	16	Chave de ciframento
IK	[31] – IK	16	Chave de integridade
TEK	[31] – TK_{UH} [32] – TK_{WU}	32	Chave transitória
-	[31] – MAC [32] – MAC_w [36] – MAC [37] – MAC	8	Código de autenticação de mensagens
-	[33] – (SK_{MS}, PK_{MS}) [36] - (SK_{HAAA}, PK_{HAAA}), (SK_{WAAA}, PK_{WAAA})	32	Par de chaves privada/pública
MSK	[33] - SK [35] – MSK [36] – EMSK, MSK, CRA-MSK, CRA-EMSK [37] - CRA-EMSK	64	Chave de sessão
HOK	[33] - K_{MH} [35] – K_{TEMP}	32	Chave de *handover*
ID	[35] – Id_{enc}, ID_{AP}, ID_{HSS}	16	ID permanente
-	[33] - T [35] – TU	8	*Timestamp*
WN	[35] – N_{AAA}, a	16	*Nonces* gerados pelo WAAA
C_{HHO}	[36] – SEQ	4	Número de

	[37] SEQ		sequencia/ Contador
-	[36] – Host Name, MSK Name, EMSK Name, Foreign Realm [37] - Kname-NAI	50	Nomes para identificação

Com o auxílio da Tabela 6.3 e estimando um tamanho médio para as mensagens do PMIPv6 em 90 bytes (com base em [49] e [9]), foi calculado o tamanho médio das mensagens (Avg M_{prot}) de cada protocolo de autenticação com o uso do PMIPv6 para prover o gerenciamento de mobilidade, mostrado na Tabela 6.4. Como apresentado em [42], no meio sem fio os pacotes possuem além dos seus dados de informação, 28 bytes do frame IEEE 802.11, 6 bytes do EAPoL *header* e 4 bytes do EAP *header.* Na rede cabeada as mensagens possuem 18 bytes do frame IEEE 802.3, 20 bytes do *header* IP, 8 bytes do UDP *header*, 22 bytes do *header* do protocolo Radius e 4 bytes do EAP *header*.

Tabela 6.4 – Tamanho médio das mensagens.

Protocolo	**Tamanho médio das mensagens relativas à autenticação (Bytes)**	**Tamanho médio das mensagens relativas ao gerenciamento de mobilidade (PMIPv6) (Bytes)**
Protocolo Proposto	86	90
UNAEN [30]	86	90
EAP-FAKA [31]	97	90
EAP-FLAKA [32]	84	90
EAP-LUTLS [33]	109	90
Proposto por Hassanein, A., H., et al. [35]	102	90
EAP-CRA [36]	110	90
Reaut. EAP-CRA [37]	91	90

A Tabela 6.5 ilustra os valores numéricos das taxas médias de chegada e das taxas médias de processamento nos sentidos terminal → rede e rede → terminal para os elementos apresentados na Figura 6.2:

Tabela 6.5 – Valores numéricos das taxas de chegada e processamento.

Parâmetros	Valor	Referência(s)	Formas de Obtenção
μ_{UE}; $\mu_{AP'}$	14,42 Mbps	[43]	{1}
$\mu_{UE'}$	100 Mbps	[17]	{2}
μ_{AP}	94,34 Mbps	[17]	{3}
μ_{HAAA}; μ_{WAAA}; $\mu_{HAAA'}$	160,14 pacotes/s	[17]	{6}
$\mu_{WAAA'}$	79,761 pacotes/s	[17]	{6}
μ AR; μ AR'	5000 pacotes/s	[44]	{12}
μ PDN-GW; μ PDN-GW'	2000 pacotes/s	[44]	{12}
μ S-GW; μ S-GW'	2000 pacotes/s	-	Estimado
μ MME; μ MME'	2000 pacotes/s	-	Estimado
λ_{UE}	15,22 Kbps	[17]	{4}
$\lambda_{UE'}$	14,42 Mbps	[43]	{1}
λ_{AP}; $\lambda_{AP'}$	100 Kbps	[17]	{5}
λ_{WAAA}	124,27 pacotes/s	[17]	{6}
$\lambda_{WAAA'}$	43,89 pacotes/s	[17]	{6}
λ_{HAAA}	124,27 pacotes/s	[17]	{6}
$\lambda_{HAAA'}$	43,89 pacotes/s	[17]	{6}
$\lambda_{AR;}$ $\lambda_{AR'}$	200 pacotes/s	-	Valor atribuído com base em [44]
$\lambda_{PDN\text{-}GW;}$ $\lambda_{PDN\text{-}GW'}$	200 pacotes/s	-	Valor atribuído com base em [44]
$\lambda_{S\text{-}GW;}$ $\lambda_{S\text{-}GW'}$	200 pacotes/s	-	Valor atribuído com base em [44]
$\lambda_{MME;}$ $\lambda_{MME'}$	200 pacotes/s	-	Valor atribuído com base em [44]
ΔSS7	37,07 ms	[17]	{7}
ΔHSS	66,20 ms	[17]	{8}

{1} - Calculado de acordo com metodologia desenvolvida por Bianchi [43] (utilizada em [47] e [48]) e considerando 10 terminais utilizando simultaneamente o mesmo canal 802.11.

{2} - Valor estimado para velocidade do barramento interno do terminal móvel.

{3} - Valor efetivo (*goodput*) de taxa para interface 100 BASE-T (*Fast Ethernet*) com MTU=1500 bytes, considerando o overhead devido ao protocolo TCP/IP e *Ethernet*.

{4} - Calculado pelo tamanho total das mensagens de EAP trocados pelo terminal, conforme calculado pelo autor.

{5} – Tráfego de internet estimado para um *Access Point* com 10 terminais conectados – dado histórico para dimensionamento de acesso WLAN.

{6} - Valor obtido por meio de medidas realizadas em servidor AAA em rede real de produção, conforme obtidas pelo autor.

{7} - Valor medido em rede de sinalização em operação comercial do atraso médio de transmissão, conforme indicado pelo autor.

{8} - Valor medido em elemento em operação comercial do tempo gasto pela consulta ao elemento HSS/AuC, conforme indicado pelo autor.

{12} - Valor estimado pelos autores em [44].

Para o atraso de *handover*, será considerado o tempo de retransmissão inicial (RTO_0), expresso pela Equação (6.6), como sendo igual a 200 milissegundos [26] para as mensagens de EAP na interface WLAN. O número de retransmissões máximas (N_m), também expressas na Equação (6.6), é configurado para 5 retransmissões para os métodos EAPs como sugerido pela RFC 3748 [14]. O atraso médio de propagação fim a fim do canal WLAN (D) é igual a 0,4 milissegundos para uma WLAN do padrão IEEE 802.11g (um canal de 54 Mbps), de acordo com [43].

A Figura 6.3 foi gerada a partir da Eq. (6.8) e ilustra a latência de *handover* no sentido LTE → WLAN em função da taxa de erro de quadro (FER, do inglês *Frame Error Rate*) para os protocolos de autenticação considerando a utilização de filas nos elementos e uma rede WLAN 802.11 g.

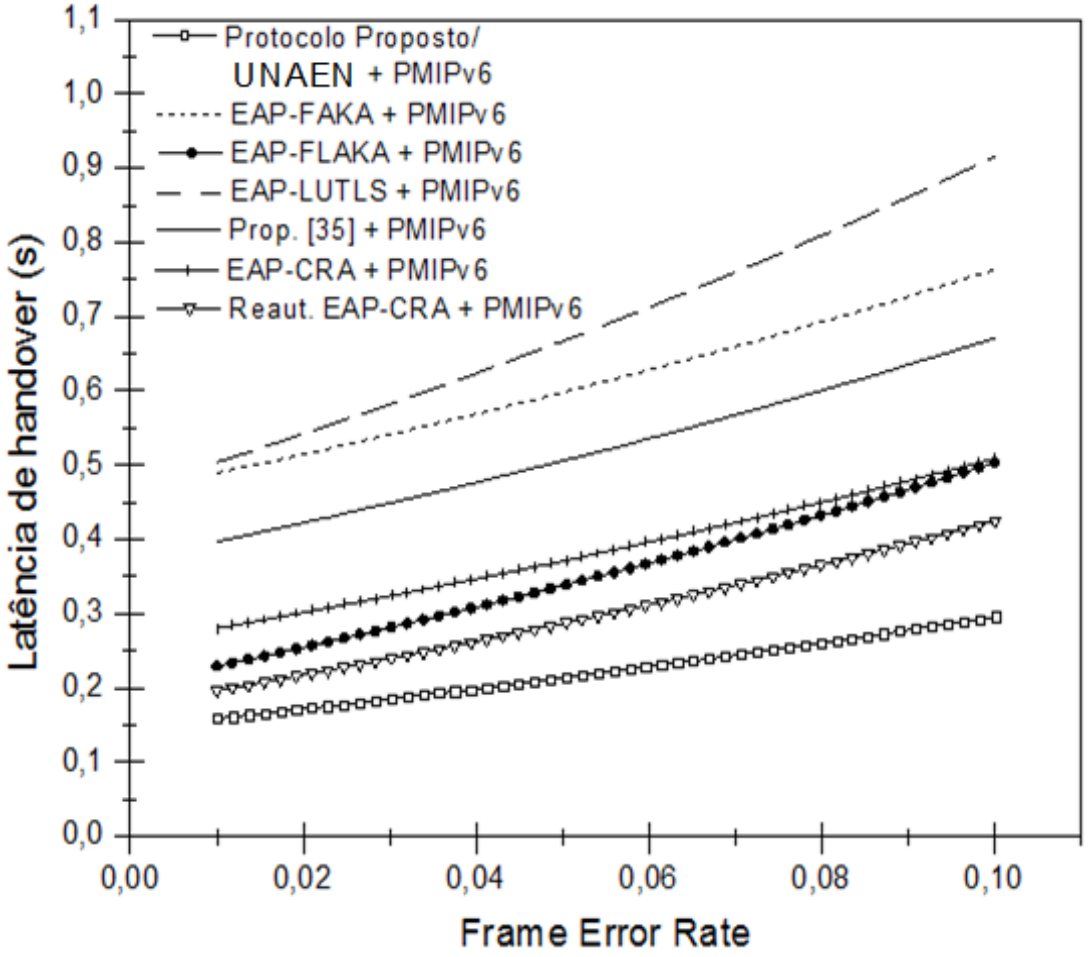

Figura 6.3 – Latência de *handover* vs Taxa de Erro de Quadro.

A partir da Figura 6.3, pode-se observar o comportamento da latência de *handover* em função da taxa de erro de quadro. Para todos os protocolos, pode-se notar que ocorre um aumento da latência de *handover* com o aumento da FER, porém alguns protocolos, como o EAP-LUTLS, são mais sensíveis a este aumento devido à troca de um número maior de mensagens através da interface WLAN.

O UNAEN e o protocolo proposto foram os métodos que apresentaram a menor latência de *handover* dentre todos os apresentados. Estes métodos trocam apenas 3 mensagens na interface WLAN para autenticar o móvel, enquanto as outras mensagens de sinalização para a autenticação do móvel são trocadas em uma fase anterior ao *handover*.

Pode-se também observar que os métodos de reautenticação, EAP-FLAKA e Reaut. EAP-CRA possuem uma menor latência de *handover* se comparado aos protocolos que

utilizam processo de autenticação completa. Comparando esses dois métodos, o EAP-FLAKA é mais afetado pela variação da taxa de erro de quadro se comparado a reautenticação do EAP-CRA, devido a troca de 1 mensagem a mais na interface WLAN, como apresentado na Tabela 6.1. A latência de *handover* do EAP-FLAKA também é a maior em relação aos dois protocolos, pois este para realizar seu processo de autenticação troca um número maior de mensagens.

Dentre os protocolos que utilizam o processo de autenticação completa, o EAP-LUTLS foi o protocolo que apresentou a maior latência de *handover*. O protocolo proposto por Hassanein, A., H., et al. apresentou uma latência levemente maior do que a do EAP-FAKA, porém o método proposto por Hassanein, A., H., et al. necessita de uma pequena alteração da arquitetura SAE, com a ligação direta entre o WAAA e o HSS, alteração que pode não ser viável em redes celulares comerciais. O EAP-CRA apresenta a menor latência de *handover* se comparado aos seus concorrentes, isso se deve principalmente ao fato deste protocolo não realizar nenhuma consulta ao HSS, processo este muito oneroso.

6.1.5 - Avaliação de Mensagens de Autenticação, MM e Consultas ao HSS

A Tabela 6.6 apresenta uma avaliação do somatório de mensagens de autenticação, MM e consultas ao HSS, junto com o respectivo tamanho em bytes

Tabela 6.6 – Mensagens de Autenticação, MM e Consultas ao HSS.

Método de autenticação	**Número de mensagens relativas à autenticação**	**Número de mensagens relativas à autenticação trocadas na interface aérea**	**Número de mensagens relativas ao MM**	**Número de consultas ao HSS durante a autenticação**
Protocolo Proposto	- Fase Preparação: 12 msgs de 90 bytes (Subfase de Distribuição + PMIPv6). - Fase Autenticação: 3 msgs de 86 bytes	3 msgs de 86 bytes	10 msgs de 90 bytes	0
UNAEN [30]	- Fase Preparação: 8 msgs de 100 bytes (Subfase de Distribuição). - Fase Autenticação: 3 msgs de 86 bytes	3 msgs de 86 bytes	10 msgs de 90 bytes	0
EAP-FAKA [31]	20 msgs de 97 bytes	6 msgs de 97 bytes	10 msgs de 90 bytes	1

EAP-FLAKA [32]	14 msgs de 84 bytes	6 msgs de 84 bytes	10 msgs de 90 bytes	0
EAP-LUTLS [33]	27 msgs de 109 bytes	9 msgs de 109 bytes	10 msgs de 90 bytes	1
Proposto por Hassanein, A., H., et al. [35]	16 msgs de 102 bytes	6 msgs de 102 bytes	10 msgs de 90 bytes	1
EAP-CRA [36]	15 msgs de 110 bytes	5 msgs de 110 bytes	10 msgs de 90 bytes	0
Reauten. EAP-CRA [37]	9 msgs de 91 bytes	5 msgs de 91 bytes	10 msgs de 90 bytes	0

6.1.6 – Discussão dos resultados

No cenário de *handover* vertical no sentido LTE → WLAN aqui tratado, considerou-se que a rede LTE é a rede caseira do móvel. Para auxílio na discussão dos resultados deste estudo de caso, será utilizado como base a Tabela 6.6 e a Figura 6.3.

Conforme descrito anteriormente, o prototocolo proposto apresenta duas fases: preparação de *handover* e autenticação. Na fase de preparação de *handover*, assim que o móvel entra no domínio PMIPv6 e se conecta com a rede LTE, são realizados os procedimentos relativos ao gerenciamento de mobilidade e preparação para um futuro *handover*. Nesta fase, verifica-se que são trocadas 12 mensagens com um tamanho médio estimado de 90 bytes para cada mensagem do PMIPv6. Na fase de autenticação ao ser realizado o *handover* vertical no sentido LTE → WLAN, é feita a autenticação do móvel com a troca de 3 mensagens com tamanho médio de 89 bytes através da interface aérea. Adicionalmente são trocadas 10 mensagens com um tamanho médio de 90 bytes no meio cabeado, relativas aos procedimentos de gerenciamento de mobilidade do PMIPv6.

Em termos de mensagens trocadas para autenticação do UE na rede alvo, o protocolo proposto e o UNAEN trocam 3 vezes menos mensagens do que o protocolo de reautenticação do EAP-CRA, que é o protocolo que apresenta o melhor desempenho após o protocolo proposto e o UNAEN.

O aumento da FER é prejudical a um protocolo, pois aumenta a probabilidade de um pacote ser perdido na interface aérea, fazendo com que acarrete aumento da latência de *handover*, pois o pacote deverá ser retransmitido. A partir da Figura 6.3, pode-se observar que os protocolos que trocam um maior número de mensagens no meio sem fio são mais afetados com o aumento da taxa de erro de quadro. Este comportamento pode ser visualizado entre os protocolos EAP-CRA e o EAP-FLAKA, que trocam 5 e 6 mensagens através da interface WLAN respectivamente. Para uma FER de 0,01 a diferença da latência de *handover* fica em torno de 0,05 segundos. A medida que a FER aumenta a latência de *handover* tende a diminuir, sendo que para uma FER igual a 0,1 a latência de *handover* para os dois protocolos é praticamente a mesma. A partir da Tabela 6.6, pode-se observar que o protocolo proposto e o UNAEN apresentaram o menor número de mensagens trocadas através da interface WLAN, sendo estes os protocolos que são menos afetados pela taxa de erro de quadro. Por outro lado, o EAP-LUTLS é o protocolo mais afetado pela taxa de erro de quadro, devido a troca de 9 mensagens através da interface WLAN.

Em relação às mensagens trocadas para o gerenciamento de mobilidade do protocolo PMIPv6, todos os protocolos apresentaram o mesmo desempenho, sendo trocadas 10 mensagens de 90 bytes como pode ser visto na Tabela 6.6.

A cada consulta feita ao HSS no processo de autenticação adiciona-se um atraso de 0,14034 segundos, de acordo com medição feita em rede comercial por [17]. Este atraso pode se tornar oneroso para aplicações que possuem requisitos mínimos de QoS. Para ilustrar como este atraso é alto, para uma FER de 0,01, o atraso de uma consulta ao HSS para o protocolo proposto por Hassanein, A., H., et al. representa 35% da latência total de *handover* para o protocolo. Nesse sentido, os protocolos que apresentam as menores latências de *handover* são aqueles que não efetuam uma consulta ao HSS, como o protocolo proposto, UNAEN, EAP-CRA, EAP-FLAKA e a reautenticação do protocolo EAP-CRA.

6.2 – SEGUNDO ESTUDO DE CASO

O segundo estudo de caso envolve *handover* horizontal entre duas WLANs, gerenciadas por uma rede de núcleo LTE. A modelagem analítica utilizada nesta subseção é semelhante à apresentada no trabalho de doutorado de [42].

6.2.1 – Arquitetura alvo

Neste cenário, busca-se avaliar o impacto de protocolos de autenticação durante um *handover* horizontal entre redes WLANs, em que a rede LTE será a rede caseira do móvel e as redes WLANs serão as redes visitadas. A rede LTE possui área de cobertura em todo domínio PMIPv6, enquanto as redes WLANs possuem área reduzida. Neste cenário, a rede 4G será a rede caseira do dispositivo móvel, enquanto este pode realizar o procedimento de *handover* para qualquer rede WLAN pertencente ao domínio PMIPv6. Neste modelo, cada célula WLAN terá área de cobertura hexagonal. Neste cenário, um servidor de AAA e um AR central responsável por todas as WLANs contidas no domínio das redes WLANs; portanto, tratar-se-á redes WLANs gerenciadas por um mesmo AR (*handover* horizontal intra-AR).

As mensagens trocadas para o procedimento de autenticação são as mesmas apresentadas na Tabela 6.1 e já discutidas na Seção 4.3. Para a realização dos procedimentos relativos ao gerenciamento de mobilidade, primeiramente é feito a desconexão com a rede WLAN atual, apresentada nos passos de 2 - 4 do fluxo de mensagens da Figura 3.10, e logo após são feitos os procedimentos relativos à conexão com a rede alvo, apresentada nos passos 4 – 7 do fluxo de mensagens da Figura 3.9. A Tabela 6.7 mostra a quantidade de mensagens relativas ao gerenciamento de mobilidade, trocadas entre cada elemento de rede durante o procedimento de *handover*:

Tabela 6.7 - Troca de mensagens relativas ao gerenciamento de mobilidade entre elementos.

Método de autenticação	**AR←→PDN-GW**	**PDN-GW ←→SGW**	**SGW←→MME**	**MME←→HSS**	**HSS←→HAAA**
UNAEN [30] / Prot. Proposto	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens
EAP-FAKA [31]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens
EAP-FLAKA [32]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens
EAP-LUTLS [33]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens
Proposto por Hassanein, A., H., et al. [35]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens

EAP-CRA [36]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens
Reauten. EAP-CRA [37]	4 mensagens	4 mensagens	4 mensagens	4 mensagens	4 mensagens

A Figura 6.4 apresenta o cenário utilizado para avaliação dos protocolos considerando aspectos de mobilidade do UE:

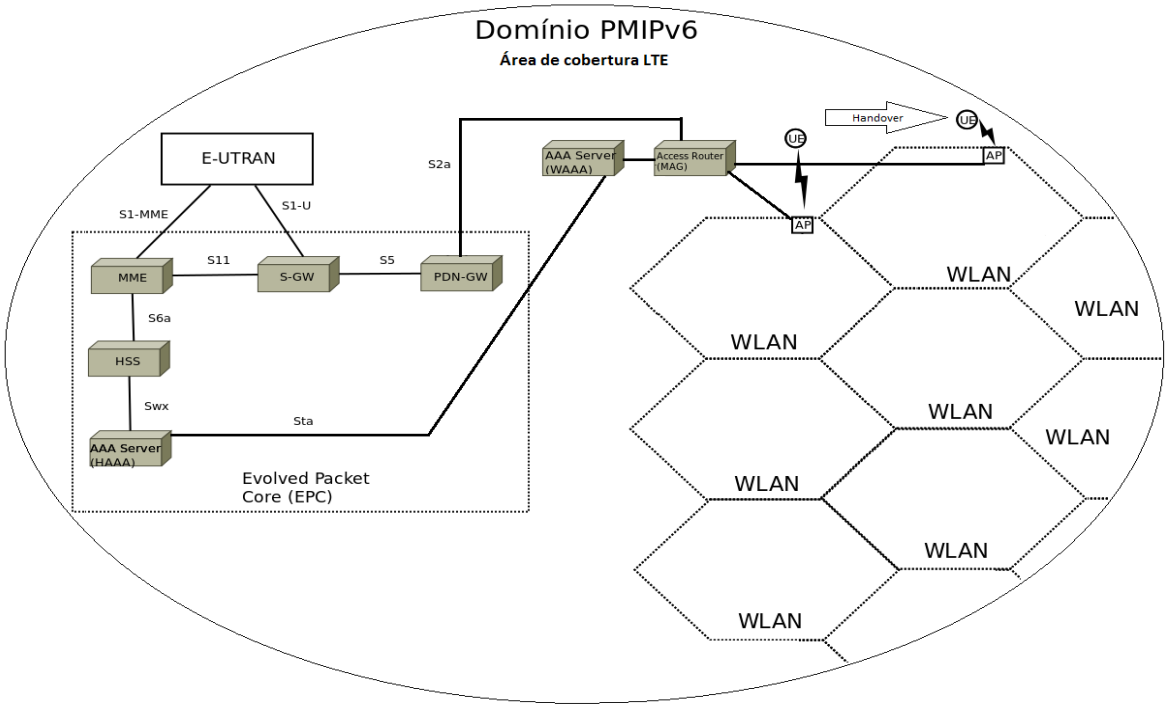

Figura 6.4 – Cenário utilizado para avaliação dos protocolos.

6.2.2 – Modelagem analítica

Neste modelo, cada célula WLAN será do tipo hexagonal e irá representar sua área de cobertura. *B* é o número de células no domínio das redes WLANs e R simboliza um círculo virtual representando o domínio WLAN como mostrado na Figura 6.5:

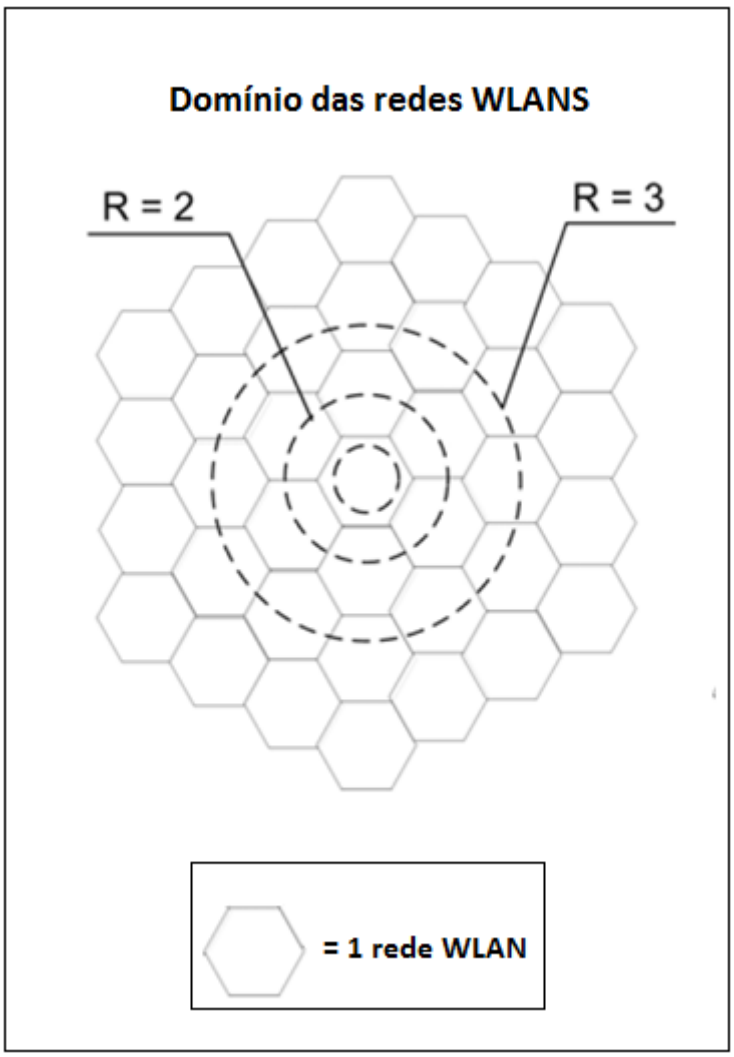

Figura 6.5 – Estrutura de rede.

Uma única célula existe no domínio WLAN quando R=1. Quando R=2, 7 células estão contidas no domínio. Para esse cenário, B é calculado da seguinte forma:

$$B = \sum_{n=1}^{R} 6.(n-1) + 1 = 3.R.(R-1) + 1 \qquad \text{Eq. (6.10)}$$

A área de uma célula é dada por:

$$A_{célula} = 1{,}5.a^2 . \sqrt{3}\ , \qquad \text{Eq. (6.11)}$$

em que "a" é o lado do hexágono.

A área do domínio WLAN é dada por:

$A_{Dom\text{-}WLAN} = 1{,}5.a^2 . \sqrt{3} . [3.R.(R-1)+1]$ Eq. (6.12)

E o perímetro do domínio é:

$L_{Dom\text{-}WLAN} = 6.a.(2.R-1)$ Eq. (6.13)

A taxa de *handover* dada para "n" usuários por célula e que se movem com velocidade média "v" é dada por (6.14):

$$HO_{Rate} = \frac{n.v.\mathrm{LDom-WLAN}}{\pi.\mathrm{ADom-WLAN}}$$ Eq. (6.14)

A taxa de *handover* para um domínio em que existam $n.B$ usuários é:

$$HO_{Rate\text{-}Dom} = \frac{n.B.v.\mathrm{LDom-WLAN}}{\pi.\mathrm{ADom-WLAN}}$$ Eq. (6.15)

6.2.3 – Avaliação da sinalização de *handover*

Esta subseção irá apresentar a análise do tráfego causado na rede devido as trocas de mensagens durante um *handover* no domínio WLAN, causado por n.B usuários. Nesta análise, serão consideradas as mensagens trocadas relativas à autenticação e ao gerenciamento de mobilidade do móvel.

A sinalização de *handover* trocada na rede pelos móveis quando $n.B$ usuários existem no domínio PMIPv6 é dada pela Eq. (6.16), utilizada em [42]:

$$SC = S_{prot} . HO_{Rate\text{-}Dom} = \frac{\mathrm{Sprot}.n.B.v.\mathrm{LDom-WLAN}}{\pi.\mathrm{ADom-WLAN}},$$ Eq. (6.16)

em que S_{prot}, denota o tamanho total das mensagens trocadas no *handover* de um determinado protocolo de autenticação. S_{prot} é dado por:

$S_{prot} = N_{msg\text{-}tot}.$ Avg $M_{prot,}$ Eq. (6.17)

em que $N_{msg\text{-}tot}$ é o número de mensagens totais trocadas por determinado protocolo para a realização do *handover* e Avg M_{prot} é o tamanho médio das mensagens.

Como as mensagens relativas à autenticação e gerenciamento de mobilidade possuem valores diferentes, S_{prot} será dividido em $S_{prot\text{-}aut}$ e $S_{prot\text{-}MM}$, em que $S_{prot\text{-}aut}$ representa

tamanho total das mensagens trocadas relativas a autenticação e $S_{prot-MM}$ representa as mensagens trocadas realativas ao gerenciamento de mobilidade. Desta forma, S_{prot} pode ser expresso por:

$$S_{prot} = S_{prot-aut} + S_{prot-MM,} \quad \text{Eq. (6.18)}$$

em que $S_{prot-aut}$ é dado por:

$$S_{prot-aut} = N_{msg-aut-tot}. \text{ Avg } M_{prot-aut,} \quad \text{Eq. (6.19)}$$

em que $N_{msg-tot-aut}$ é o número de mensagens totais trocadas relativas a autenticação durante o *handover* e Avg $M_{prot-aut}$ é o tamanho médio das mensagens relativas a autenticação.

Desta forma, $S_{prot-MM}$ é dado por:

$$S_{prot-aut} = N_{msg-MM-tot}. \text{ Avg } M_{prot-MM,} \quad \text{Eq. (6.20)}$$

em que $N_{msg-tot-}$ é o número de mensagens totais trocadas relativas a autenticação durante o *handover* e Avg $M_{prot-aut}$ é o tamanho médio das mensagens relativas a autenticação.

A Tabela 6.8 ilustra os valores de $S_{prot-aut}$ e $S_{prot-MM}$ para cada protocolo. Os valores de $N_{msg-aut-tot}$ para cada protocolo são apresentados na Tabela 6.6 e os valores de $N_{msg-MM-tot}$ podem ser obtidos por meio da Tabela 6.7 e são trocadas 20 mensagens relativas ao gerenciamento de mobilidade para todos os protocolos. Os valores de Avg $M_{prot-aut}$ e Avg $M_{prot-MM}$ são apresentados na Tabela 6.4.

Tabela 6.8 – $S_{prot-aut}$, $S_{prot-MM}$ e S_{prot} para cada protocolo.

Protocolo	$S_{prot-aut}$ (Bytes)	$S_{prot-MM}$ (Bytes)	$S_{prot} = S_{prot-aut} + S_{prot-MM}$(Bytes)
Protocolo Proposto	267	1800	2067
UNAEN[30] + PMIPv6	267	1800	2067
EAP-FAKA[31] +PMIPv6	1692	1800	3492
EAP-FLAKA[32] + PMIPv6	1316	1800	3116
EAP-LUTLS[33] + PMIPv6	2943	1800	4743
Proposto por Hassanein, A., H., et al. [35] +	1632	1800	3432

PMIPv6			
EAP-CRA[36] + PMIPv6	1650	1800	3450
Reaut. EAP-CRA[37] + PMIPv6	819	1800	2619

Com base na Eq. (6.16) foi gerada a Figura 6.6 que ilustra a sinalização de *handover* (KByte) quando n.B usuários se movimentam a uma velocidade média v (m/s). Neste caso, a = 100 metros, R=2 e n = 10 usuários.

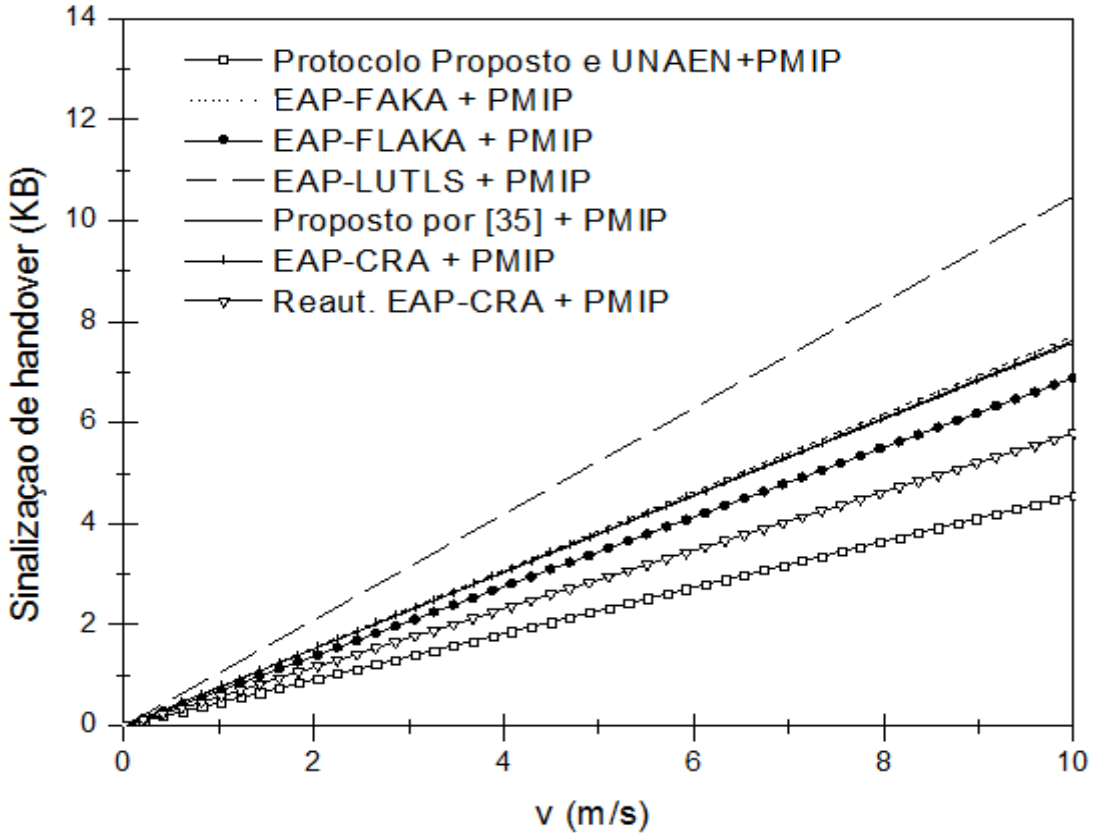

Figura 6.6 – Sinalização de *handover* vs velocidade média.

A partir da Eq. (6.16), pode-se observar que a sinalização de *handover* depende de 6 variáveis diretamente ou inversamente proporcionais que são elas:

- Diretamente proporcionais:

- S_{prot}: tamanho total das mensagens trocadas durante o *handover* e expresso pelas Eqs (6.17) e (6.18);
- n: número de usuários por célula;
- B : número de células contidas no domínio das redes WLANs e expresso pela Eq. (6.10);
- $L_{Dom\text{-}WLAN}$: perímetro do domínio das redes WLANse expresso pela Eq. (6.13);
- v : velocidade média de deslocamento do móvel.

- <u>Inversamente proporcionais</u>:

- $A_{Dom\text{-}WLAN}$: área do domínio das redes WLANs e expresso pela Eq. (6.12).

Para a avaliação da sinalização de *handover* vs velocidade média do UE, considera-se que a = 100 metros, R=2 e n = 10 usuários, desta forma $A_{Dom\text{-}WLAN}$ = 18186532 m^2, B = 7 células e $L_{Dom\text{-}WLAN}$ = 1800 metros. Incluindo esses valores na Eq. (6.16), a sinalização de *handover* vs velocidade média do UE é dado por:

$$SC = v \,.S_{prot}\,.\,0{,}00221 = v\,.\,(S_{prot\text{-}aut} + S_{prot\text{-}MM}).\,0{,}0021 \qquad \text{Eq. (6.21)}$$

A partir da Tabela 6.8, pode-se observar que o valor $S_{prot\text{-}MM}$ é o mesmo para todos os protocolos, então a Eq. (6.21) pode ser expressa por:

$$SC = v.(S_{prot\text{-}aut} + 1800).\,0{,}00221 \qquad \text{Eq. (6.22)}$$

A equação acima justifica o comportamento linear observado na Figura 6.6, a partir da qual pode-se observar também que o protocolo proposto e o UNAEN obtiveram o melhor desempenho se comparados aos demais protocolos (estes protocolos trocam apenas 3 mensagens relativas à autenticação, cada mensagem de tamanho médio de 89 Bytes e um $S_{prot\text{-}aut}$ igual a 267 bytes. O protocolo que mais se aproximou do desempenho do protocolo proposto foi o EAP-CRA em modo de reautenticação, sendo trocadas 9 mensagens com um tamanho médio de 91 bytes cada e um $S_{prot\text{-}aut}$ de 819 bytes.

Dentre os protocolos que não utilizam métodos de preparação para o futuro *handover* e nem reautenticação, o EAP-FAKA, o EAP-CRA e o proposto por Hassanein, A., H., et al.

apresentaram uma sinalização de *handover* muito semelhantes, sendo o $S_{prot-aut}$. igual a 1692 para o EAP-FAKA, 1650 para o EAP-CRA e 1632 para o proposto por Hassanein. Dentre todos os protocolos, o EAP-LUTLS foi o protocolo que apresentou o pior desempenho, sendo trocadas 27 mensagens com tamanho médio de 109 bytes cada e um $S_{prot-aut}$ de 2943 bytes.

Pela Figura 6.6, à medida que a velocidade dos móveis aumenta a sinalização de *handover* também aumenta, face à ocorrência de um maior número de *handovers*.

A Figura 6.7 baseia-se na Eq. (6.16) e mostra o efeito na sinalização de *handover* em relação ao parâmetro R. Neste caso, tem-se que a = 100 m, v=1 m/s e n = 10 usuários.

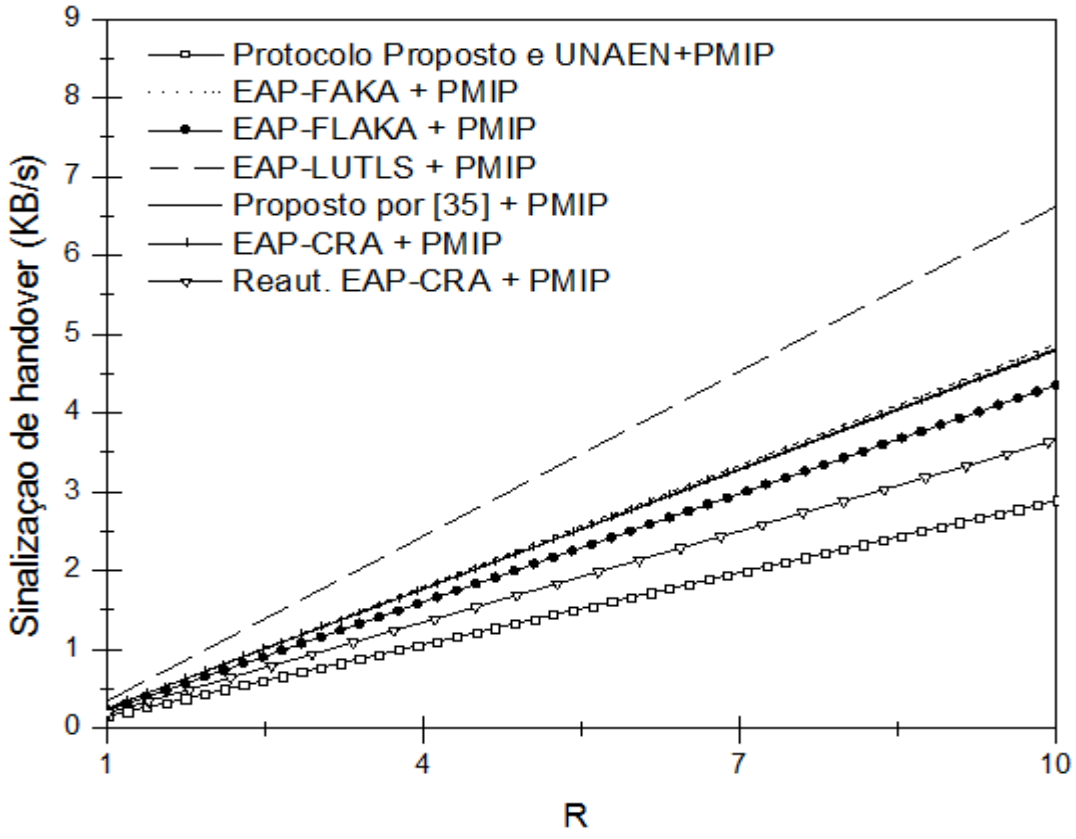

Figura 6.7 – Sinalização de *handover* vs R.

Aplicando o mesmo raciocínio feito para a Figura 6.6, na avaliação da sinalização de *handover* vs R, considerando que a = 100 m, v=1 m/s e n = 10 usuários, então $A_{Dom-WLAN}$ =

$1{,}5.100^2 . \sqrt{3} . [3.R.(R-1)+1]$, $L_{Dom\text{-}WLAN} = 6.100.(2.R-1)$ e $B = 3.R.(R-1)+1$. Incluindo esses valores na Eq. (6.16), a sinalização de *handover* vs R em bytes é dado por:

$$SC = \frac{Sprot.10.1.[6.100.(2.R-1)].[3.R.(R-1)+1]}{\pi.1{,}5.100^2 . \sqrt{3} .[3.R.(R-1)+1]} = \frac{Sprot.[6.10^3.(2.R-1)]}{\pi.1{,}5.10^4 . \sqrt{3}} = \frac{Sprot.(12.R-6)}{81{,}58} \quad \text{Eq. (6.23)}$$

Como o gráfico da Figura 6.7 é dado em KB a Eq. (6.23) pode ser expressa por:

$$SC = \frac{Sprot.(12.R-6)}{81{,}58.10^3} \quad \text{Eq. (6.24)}$$

Como $S_{prot} = S_{prot\text{-}aut} + S_{prot\text{-}MM}$ e de acordo com a Tabela 6.8, o valor $S_{prot\text{-}MM}$ é o mesmo para todos os protocolos e igual a 1800 bytes, a Eq. (6.24) pode ser expressa por:

$$SC = \frac{(Sprot-aut + 1800).(12.R-6)}{81{,}58.10^3} \quad \text{Eq. (6.25)}$$

A equação acima justifica o comportamento linear observado na Figura 6.7. Para essa situação o comportamento foi muito semelhante ao apresentado na Figura 6.6, o protocolo proposto e o UNAEN foram os protocolos que apresentaram o melhor desempenho, sendo trocadas 3 mensagens com um tamanho médio de 89 Bytes e um $S_{prot\text{-}aut}$ igual a 267 bytes. O protocolo que obteve o pior desempenho foi o EAP-LUTLS sendo trocadas 27 mensagens com um tamanho médio de 109 bytes cada e um $S_{prot\text{-}aut}$ de 2943 bytes. Em relação aos métodos que utilizam reautenticação, o EAP-CRA em modo de reautenticação possui um desempenho superior se comparado com o EAP-FLAKA. O EAP-CRA em modo de reautenticação trocou 9 mensagens com um tamanho médio de 91 bytes cada e um $S_{prot\text{-}aut}$ de 819 bytes para o procedimento de autenticação do móvel, enquanto o EAP-FLAKA trocou 14 mensagens de 84 bytes e um $S_{prot\text{-}aut}$ de 1316 bytes. Assim como na Figura 6.6, o EAP-FAKA, o EAP-CRA e o proposto por Hassanein, A., H., et al. apresentaram uma sinalização de *handover* muito semelhantes, sendo o $S_{prot\text{-}aut}$. igual a 1692 para o EAP-FAKA, 1650 para o EAP-CRA e 1632 para o proposto por Hassanein, A., H., et al.

6.2.4 – Avaliação da latência de *handover*

Nesta subseção será feita a análise da latência de *handover* em função de R e da velocidade média de cada usuário no domínio PMIPv6.

A latência de *handover* em todo o domínio quando n.B usuários existem no domínio PMIPv6 é dada pela Eq. (6.26), utilizada em [42]:

$$LC = T_{prot} \cdot HO_{Rate\text{-}Dom} = \frac{\mathrm{Tprot}.n.v.L.B}{\pi.A}, \quad \text{Eq. (6.26)}$$

em que $T_{prot,}$ é o atraso causado a um móvel quando este realiza o *handover*. T_{prot} é dado pela Eq. (6.27), utilizada em [42]:

$$T_{prot} = (M_{wl}.(D_{t(wl)} + D_{pp(wl)} + 2D_{pc})) + (M_{wd}.H_{wd}(D_{t(wd)} + D_{pp(wd)} + 2D_{pc})) + TE_{prot}, \quad \text{Eq. (6.27)}$$

em que M_{wl} e M_{wd} indicam o número de mensagens trocadas nos meios sem e com fio, respectivamente. H_{wd} denota o número de *hops* na rede cabeada. Foi assumido que entre o WAAA e o HAAA possuem 3 *hops* e entre o HAAA e o HSS possuem 2 *hops*. Os demais nós representam um *hop* cada nó. $D_{t(wl)}$ e $D_{t(wd)}$ são os atrasos de transmissão dos meios sem e com fio, respectivamente. $D_{t(wl)}$= Avg $M_{prot\text{-}sem\text{-}fio.}$ /W_{wl} e $D_{t(wd)}$=Avg $M_{prot\text{-}com\text{-}fio}$/$W_{wd}$, em que Avg $M_{prot\text{-}sem\text{-}fio.}$ e Avg $M_{prot\text{-}com\text{-}fio}$ é o tamanho médio (bytes) das mensagens de determinado protocolo nos meios sem e com fio, respectivamente, W_{wl} e W_{wd} são as taxas de dados dos meios sem e com fio e são setadas para 11 Mbps e 100Mbps, respectivamente. $D_{pp(wl)}$ e $D_{pp(wd)}$ são os atrasos de propagação dos meios sem e com fio e são setados para 2 ms e 0,5 ms, respectivamente. D_{pc} é o atraso de processamento em cada nó e é configurado para 1 μs. TE_{prot} são os atrasos adicionais causados no protocolo e é dado por:

$$TE_{prot} = e_{prot} \cdot h, \quad \text{Eq. (6.28)}$$

em que h e e_{prot} são linhas de uma matriz. h é definido como:

$$h = [D_{AV}, D_{ED}, D_{MAC}, D_{KEY}, D_{ID}], \quad \text{Eq. (6.29)}$$

em que D_{AV} é o atraso gerado pelo HSS para geração dos vetores de autenticação, D_{ED} é o atraso relacionado à encriptação/decriptação, D_{MAC} é o atraso causado pelo cálculo e verificação de um código de autenticação de mensagem, D_{KEY} é o atraso introduzido na derivação de chaves e D_{ID} é o atraso relacionado na geração de identificadores (ID). e_{prot} é a matriz que indica a quantidade de vezes em que ocorre os atrasos contidos na matriz h:

$e_{prot.\ proposto} = [0,2,2,7,1]$

$e_{UNAEN\ [30]\ +\ PMIP} = [0,2,2,7,1]$

$e_{EAP\text{-}FAKA[31] + PMIPv6} = [1,2,2,5,2]$

$e_{EAP\text{-}FLAKA[32] + PMIPv6} = [0,0,2,3,2]$ Eq. (6.30)

$e_{EAP\text{-}LUTLS[33] + PMIPv6} = [1,1,3,2,1]$

$e_{proposto\ por\ Hassanein,\ A.,\ H.,\ et\ al.\ [35] + PMIPv6} = [1,4,6,10,0]$

$e_{EAP\text{-}CRA\ [37] + PMIPv6} = [0,7,6,4,1]$

$e_{Reaut.\ EAP\text{-}CRA\ [37] + PMIPv6} = [0,0,5,0,1]$

A Tabela 6.9 contém Avg $M_{prot\text{-}sem\text{-}fio}$, Avg $M_{prot\text{-}com\text{-}fio}$, M_{wl}, M_{wd} e H_{wd}. A Tabela 6.10 contém os valores relativos à matriz h. Como na interface sem fio trafegam apenas mensagens relativas à autenticação, os valores de Avg $M_{prot\text{-}sem\text{-}fio}$ são os mesmos apresentados na Tabela 6.4. No meio cabeado, trafegam mensagens relativas à autenticação e ao gerenciamento de mobilidade, então se chegar a um valor aproximado do tamanho médio de uma mensagem no meio cabeado, foi feita uma média ponderada entre as mensagens de autenticação e gerenciamento de mobilidade. Como exemplo, pode-se citar o protocolo EAP-FAKA, em que são trocadas 14 mensagens de 97 bytes (de acordo com a Tabela 6.1 e 6.4) relativas à autenticação e mais 20 mensagens de 90 bytes (de acordo com a Tabela 6.2 e 6.4) relativas ao gerenciamento de mobilidade. Neste exemplo o Avg $M_{prot\text{-}com\text{-}fio} = \frac{(14.97)+(20.90)}{(14+20)}$ = 93 bytes. Esse mesmo raciocínio pode ser aplicado para os demais protocolos.

Tabela 6.9 – Parâmetros utilizados na análise de dados.

Protocolo	**Avg $M_{prot\text{-}sem\text{-}fio}$ (Bytes)**	**Avg $M_{prot\text{-}com\text{-}fio}$ (Bytes)**	**M_{wl}**	**M_{wd}**	**H_{wd}**
Protocolo Proposto	89	90	3	20	13
UNAEN [30] + PMIPv6	89	90	3	20	13
EAP-FAKA[31] +PMIPv6	94	93	6	34	13
EAP-FLAKA[32] + PMIPv6	84	88	6	28	13
EAP-LUTLS[33] + PMIPv6	109	99	9	38	13
Proposto por	102	94	6	30	13

Hassanein, A., H., et al. [35] + PMIPv6					
EAP-CRA[36] + PMIPv6	110	97	5	30	13
Reaut. EAP-CRA[37] + PMIPv6	91	90	5	24	13

Tabela 6.10 – Valores contidos na matriz h. [42].

Parâmetro	D_{AV}	D_{ED}	D_{MAC}	D_{KEY}	D_{ID}
Valor	12 μs	5 μs	3 μs	12 μs	3 μs

A Figura 6.8 foi gerada com base na Eq. (6.26) e ilustra a latência de *handover* (s) quando n.B usuários se movimentam a uma velocidade média v (m/s). Neste caso, considera-se que a = 100 m, R=2 e n = 10 usuários.

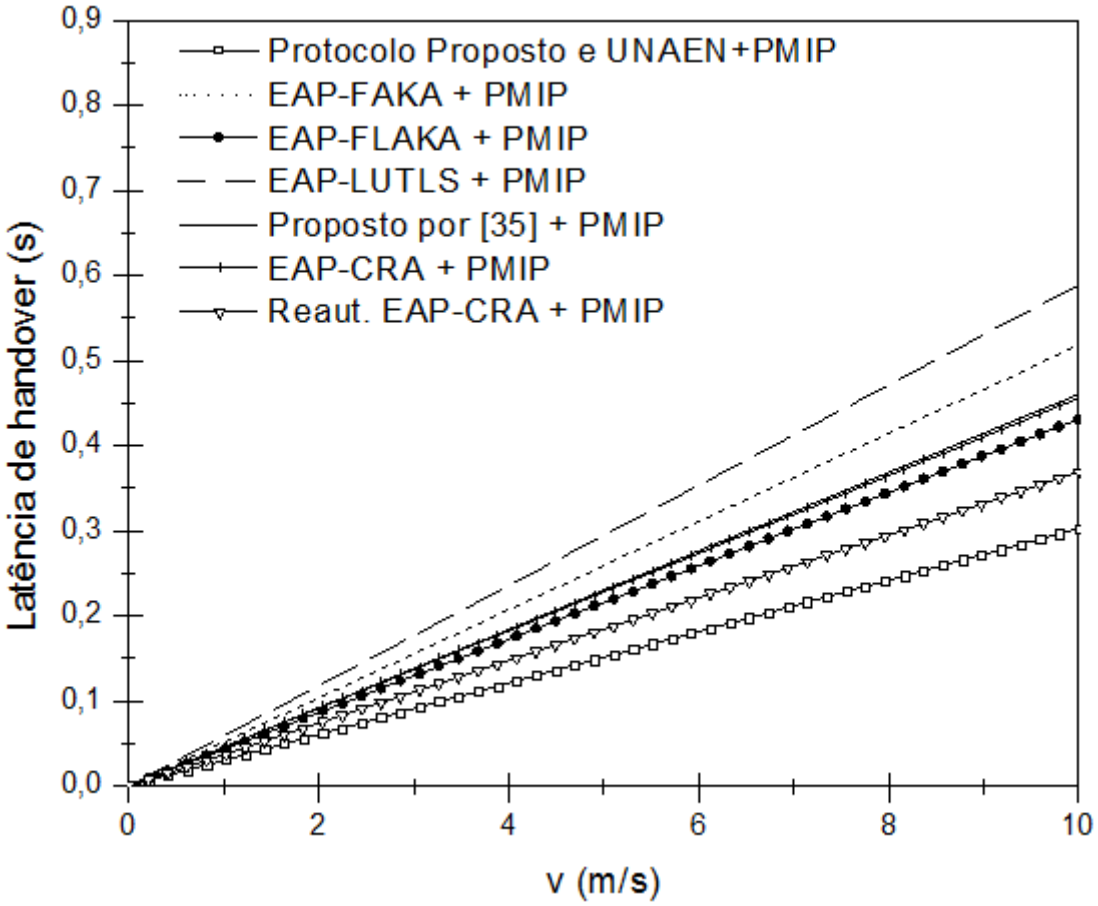

Figura 6.8 – Latência de *handover* vs velocidade média.

A partir das Eqs. 6.27 – 6.30 pode-se observar que a sinalização de *handover* depende de diversas variáveis diretamente ou inversamente proporcionais que são elas:

- Diretamente proporcionais:

- T_{prot}: atraso expresso pela Eq. (6.27) e composto por:
    - M_{wl} e M_{wd} - número de mensagens trocadas nos meios sem e com fio, respectivamente.
    - H_{wd} - número de *hops* na rede cabeada.
    - $D_{t(wl)}$ e $D_{t(wd)}$ - atrasos de transmissão dos meios sem e com fio, respectivamente. $D_{t(wl)}$ e $D_{t(wd)}$ são os atrasos de transmissão dos meios

sem e com fio, respectivamente. $D_{t(wl)}$ = Avg $M_{prot\text{-}sem\text{-}fio.}$ /W_{wl} e $D_{t(wd)}$=Avg $M_{prot\text{-}com\text{-}fio}$/$W_{wd}$, em que Avg $M_{prot\text{-}sem\text{-}fio.}$ e Avg $M_{prot\text{-}com\text{-}fio}$ é o tamanho médio (bytes) das mensagens de determinado protocolo nos meios sem e com fio, respectivamente, W_{wl} e W_{wd} são as taxas de dados dos meios sem e com fio, respectivamente.

- $D_{pp(wl)}$ e $D_{pp(wd)}$ são os atrasos de propagação dos meios sem e com fio, respectivamente.
- D_{pc} é o atraso de processamento em cada nó.
- TE_{prot} são os atrasos adicionais causados para geração dos vetores de autenticação pelo HSS, processos de encriptação/decriptação, cálculo e verificação de um código de autenticação de mensagem (MAC, do inglês *message authentication code*), derivação de chaves e geração de identificadores.

- n: número de usuários por célula;
- B : número de células contidas no domínio das redes WLANs e expresso pela Eq. (6.10);
- $L_{Dom\text{-}WLAN}$: perímetro do domínio das redes WLANs e expresso pela Eq. (6.13);
- v : velocidade média de deslocamento do móvel.

- <u>Inversamente proporcionais</u>:

Para a avaliação da latência de *handover* vs velocidade média do UE, considerando que a = 100 metros, R=2 e n = 10 usuários, então $A_{Dom\text{-}WLAN}$= 18186532 m^2, B =7 células e $L_{Dom\text{-}WLAN}$ = 1800 metros. Incluindo esses valores na Eq. (6.26), a latência de *handover* vs velocidade média do UE é dado por:

$$LC = T_{prot}.v.\ 0{,}00221 \qquad \text{Eq. (6.31)}$$

Com base em [42], $D_{t(wl)}$ = Avg $M_{prot\text{-}sem\text{-}fio}$/11 Mbps, $D_{t(wd)=}$ Avg $M_{prot\text{-}com\text{-}fio}$/100Mbps, $D_{pp(wl)}$ = 2 ms, $D_{pp(wd)}$ = 0,5 ms e Dpc = 1 μs. Adicionalmente, H_{wd} é igual a 13 *hops* no

meio cabeado para todos os protocolos como pode ser visto na Tabela 6.9. O atraso T_{prot} é dado por:

$$T_{prot} = (M_{wl}.(\text{Avg } M_{prot\text{-}sem\text{-}fio}/11 \text{ Mbps} + 2.10^{-3} + 2.10^{-6})) + (M_{wd}.13.(\text{Avg } M_{prot\text{-}com\text{-}fio}/100\text{Mbps} + 0{,}5.10^{-3} + 2.10^{-6}{}_{c})) + TE_{prot}, \quad \text{Eq. (6.32)}$$

O protocolo proposto e o UNAEN trocam o menor número de mensagens no meio sem fio M_{wl}.= 3 e com fio M_{wd} = 20, como pode ser visto na Tabela 6.9. Para a média do tamanho das mensagens trocadas através do meio sem fio (Avg $M_{prot\text{-}sem\text{-}fio}$) o protocolo EAP-FLAKA apresentou o melhor desempenho com Avg $M_{prot\text{-}sem\text{-}fio}$ = 84 bytes. O protocolo proposto e o UNAEN também apresentaram um bom resultado com Avg $M_{prot\text{-}sem\text{-}fio}$ = 90 bytes. O EAP-FLAKA também apresentou o melhor resultado para o tamanho médio das mensangens trocadas através do meio com fio, sendo Avg $M_{prot\text{-}com\text{-}fio}$ = 88 bytes.

Em relação ao atraso TE_{prot}, o protocolo de reautenticação do EAP-CRA apresentou o melhor desempenho com TE_{prot} = 18 μs, porém este atraso influencia pouco na latência de *handover* final por ser da ordem de microssegundos. O protocolo que apresentou o maior atraso relativo ao TE_{prot} foi o proposto por Hassanein, A., H., et al., com um TE_{prot} = 170 μs. Para uma velocidade v = 10 m/s, o atraso TE_{prot} corresponde a aproximadamente 0,038% do atraso total do protocolo proposto por Hassanein, A., H., et al.

Analisando a Figura 6.8, tem-se que no desempenho final, o protocolo proposto e o UNAEN apresentaram a menor latência de *handover* em função da velocidade média do móvel dentre todos os protocolos estudados.

A Figura 6.9 foi gerada a partir da Eq. (6.26) e mostra o efeito da latência de *handover* quando se varia o parâmetro R. Considera-se que a = 100 m, v=1 m/s e n = 10 usuários.

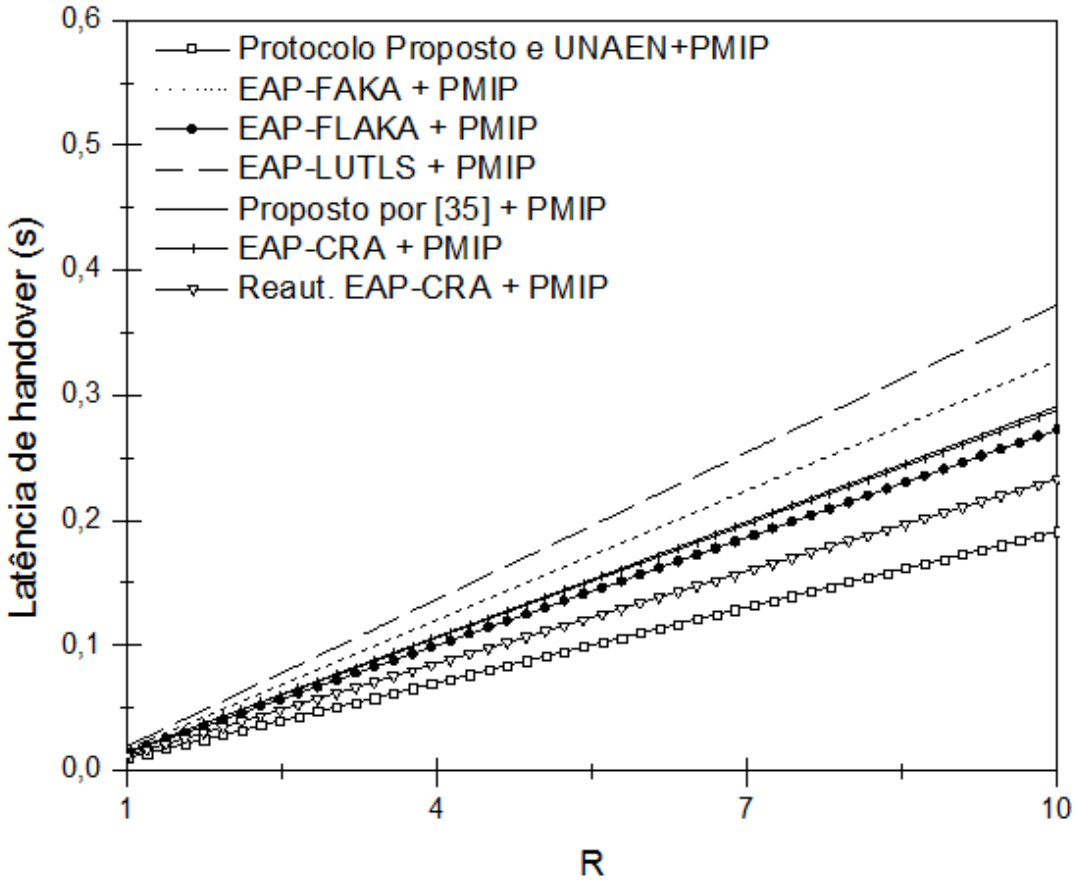

Figura 6.9 – Latência de *handover* vs R.

Aplicando o mesmo raciocínio feito para a Figura 6.8, na avaliação da latência de *handover* vs R, considerando que a = 100 m, v=1 m/s e n = 10 usuários, então $A_{Dom\text{-}WLAN} = 1{,}5.100^2 .\sqrt{3} .[3.R.(R-1)+1]$, $L_{Dom\text{-}WLAN} = 6.100.(2.R-1)$ e $B = 3.R.(R-1)+1$. Incluindo esses valores na Eq. (6.26), a latência de *handover* vs R em bytes é dado por:

$$LC = \frac{Tprot.10.1.[6.100.(2.R-1)].[3.R.(R-1)+1]}{\pi.1{,}5.100^2 .\sqrt{3} .[3.R.(R-1)+1]} = \frac{Tprot.\left[6.10^3.(2.R-1)\right]}{\pi.1{,}5.10^4 .\sqrt{3}} = \frac{Tprot.(12.R-6)}{81{,}58}, \quad \text{Eq. (6.33)}$$

sendo o T_{prot} o mesmo atraso apresentado na Eq. (6.32), então o número de mensagens trocadas no meio sem fio (M_{wl}) e com fio (M_{wd}) é o principal fator para a diminuição ou aumento da latência de *handover*, pois estes elementos entram como multiplicadores de outros atrasos. O M_{wl} multiplica a expressão ($D_{t(wl)} + D_{pp(wl)} + 2D_{pc}$) e o M_{wd} multiplica a expressão $H_{wd}(D_{t(wd)} + D_{pp(wd)} + 2D_{pc})$. O número de *hops* na rede cabeada (H_w) também entra como um termo multiplicador da expressão M_{wd} ($D_{t(wd)} + D_{pp(wd)} + 2D_{pc}$), porém esta

variável apresenta o mesmo valor para todos os protocolos. Os demais termos entram na expressão do T_{prot} somando-se a outros tipos de atrasos. O atraso TE_{prot} pouco influencia no atraso do T_{prot}, pois o TE_{prot} é da ordem de microssegundos.

Assim como na Figura 6.8, o protocolo proposto também apresentou a menor latência de *handover* se comparado aos demais protocolos. Como já foi dito, isso se deve ao fato do protocolo trocar apenas 3 mensagens para o procedimento de autenticação.

6.2.5 – Discussão dos resultados

Neste estudo de caso, tem-se um cenário de *handover* horizontal entre redes WLANs em que a rede LTE é a rede caseira do móvel e faz o gerenciamento do *handover* entre as redes WLANs.

Primeiramente, foi avaliada a sinalização durante o *handover* horizontal em função da velocidade média do UE e de R, simbolizando um círculo virtual representando o domínio das redes WLANs. Nesta avaliação, pode-se concluir que o $S_{prot\text{-}aut}$ é o parâmetro que mais influencia para o aumento da latência de *handover* em cada protocolo. Este parâmetro é dado pela Eq. (6.19). A Figura 6.10 é derivada da Tabela 6.8 e apresenta o $S_{prot\text{-}aut}$ para cada protocolo.

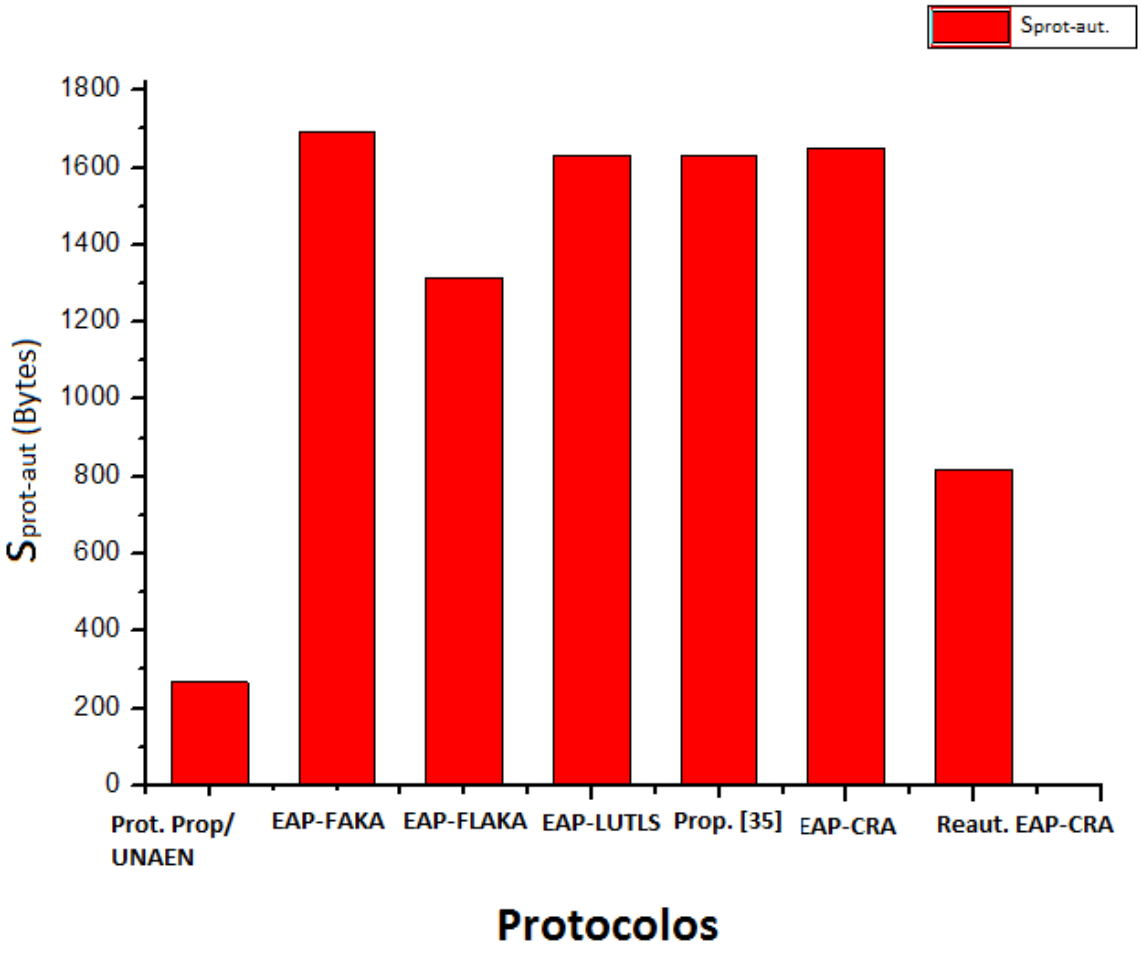

Figura 6.10 – $S_{prot\text{-}aut}$ para cada protocolo.

A partir da Figura 6.10, pode-se observar que o protocolo proposto e o UNAEN apresentam o menor valor para o $S_{prot\text{-}aut}$. O protocolo proposto e o UNAEN apresentaram o $S_{prot\text{-}aut}$ mais de 3 vezes menor do que o protocolo de reautenticação do EAP-CRA, que é o segundo protocolo com o menor $S_{prot\text{-}aut}$ após o protocolo proposto/UNAEN.

Também pode-se observar que a sinalização de *handover* é diretamente proporcional à velocidade do móvel e e ao parâmetro R.

Por fim, face à relevante contribuição das mensagens trocadas nos meios sem fio e com fio para o aumento da latência de *handover* em cada protocolo (conforme Eq. (6.18)), as Figuras 6.11 e 6.12 apresentam o número de mensagens trocadas nos meios com e sem fio, respectivamente, permitindo ratificar discussões anteriores.

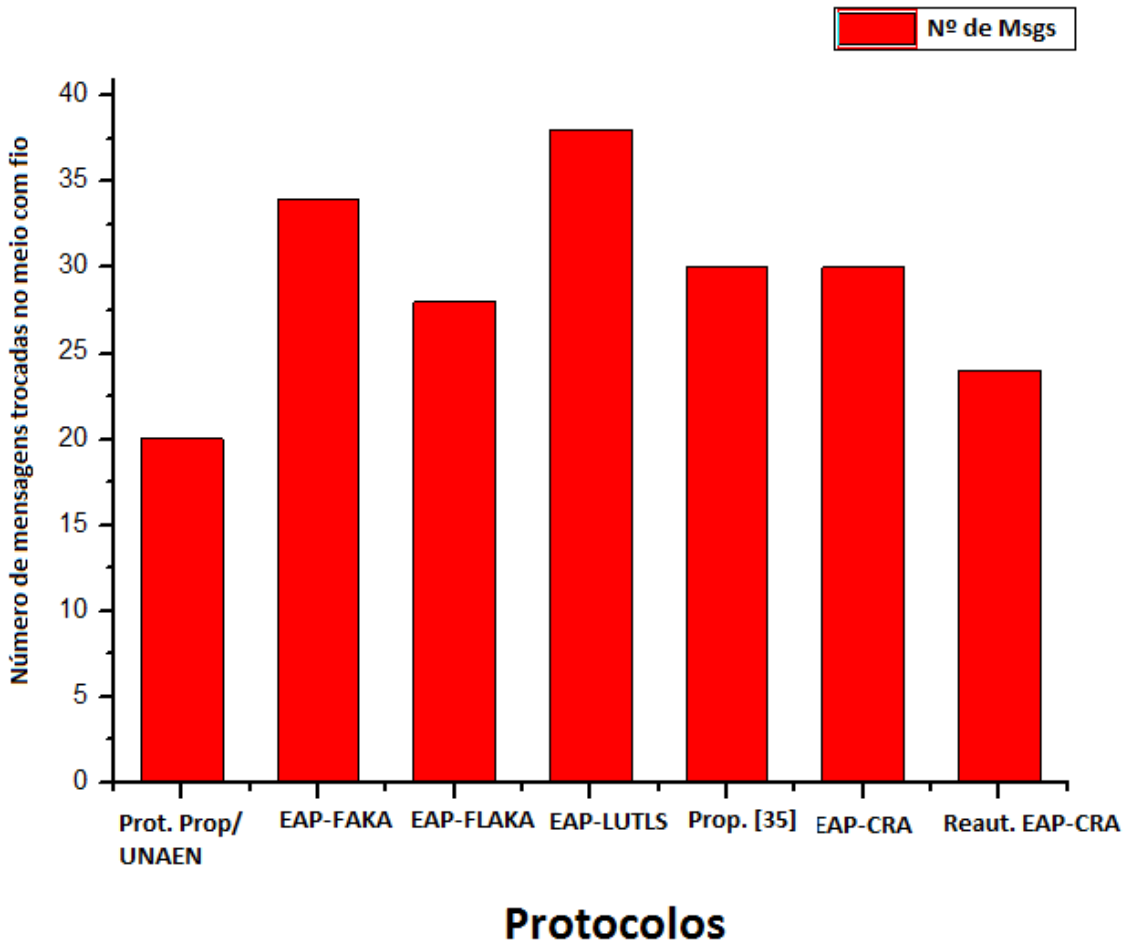

Figura 6.11 – Número de mensagens trocadas no meio com fio para cada protocolo.

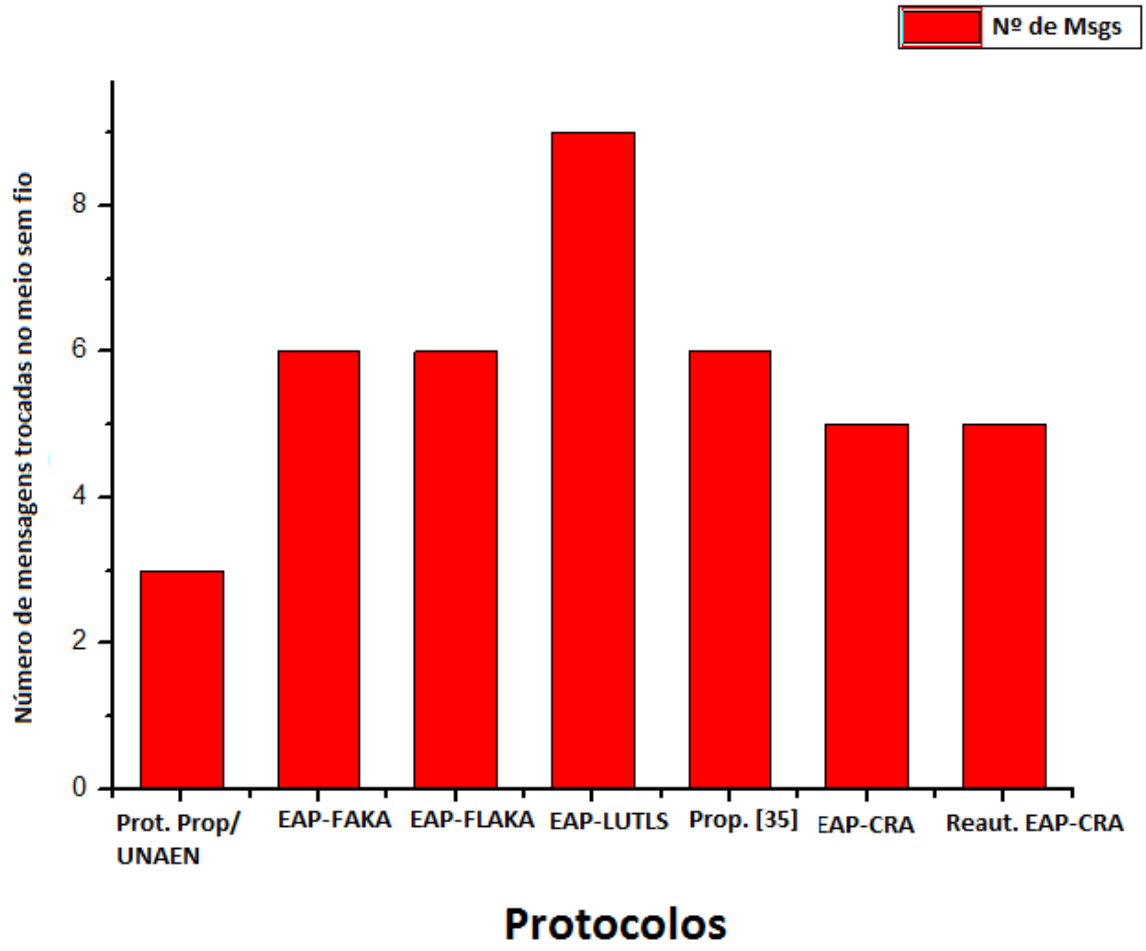

Figura 6.12 – Número de mensagens trocadas no meio sem fio para cada protocolo.

6.3 – TERCEIRO ESTUDO DE CASO

Neste estudo de caso, o cenário é o mesmo do estudo de caso anterior (*handover* horizontal entre WLAN´s controladas por uma LTE), tendo sido aplicada modelagem adotada por [42] e [17].

De acordo com [45], em um modelo de redes de comunicações de dados, os principais atrasos experimentados por um pacote ao viajar de um nó a outro são:

- Atraso de processamento nodal: Tempo requerido para examinar o cabeçalho do pacote e determinar para onde direcioná-lo [45].

- Atraso de fila: Tempo do pacote enquanto espera na fila para ser transmitido no enlace [45].

- Atraso de transmissão: Quantidade de tempo requerida para transmitir todos os bits do pacote para o enlace [45].

- Atraso de propagação: tempo necessário para propagar o bit desde o início até o fim do enlace [45].

Em [42] os atrasos de filas não são considerados no modelo. Adicionalmente, as retransmissões decorrentes da perda de quadros na interface aérea não são tratadas, sendo os atrasos na interface aérea tratados com base em valores fixos (estimativas).

Esta subseção irá apresentar um modelo analítico que considera os 4 tipos principais de atrasos apresentados em [45], com uma taxa de perda de quadros na interface aérea e considerando também os aspectos relativos a mobilidade do móvel.

6.3.1 – Modelagem analítica

A Equação (6.34) será utilizada para modelar os atrasos referentes à interface aérea:

$$T_{prot\text{-}sem\text{-}fio'} = (M_{wl}.D_{t(wl)}) + D_{UE} + D_{AP} + D_{EAP,} \quad \text{Eq. (6.34)}$$

em que M_{wl} indica o número de mensagens trocadas no meio sem fio; $D_{t(wl)}$ é o atraso de transmissão do meio sem fio, sendo $D_{t(wl)} = Avg\ M_{prot.} / W_{wl}$ em que $Avg\ M_{prot}$ é o tamanho médio das mensagens de determinado protocolo e W_{wl} é a taxa de dados do meio sem fio; os atrasos D_{UE} e D_{AP} são dados pela Equação (6.7); e o atraso D_{EAP} é o atraso de propagação referente à troca de mensagens EAP através da interface WLAN, dado pela Equação (6.6).

Os atrasos relativos ao meio com fio são dados pela Equação (6.35):

$$T_{prot\text{-}com\text{-}fio'} = M_{wd}.H_{wd}(D_{t(wd)} + D_{pp(wd)}) + D_{AR} + D_{AAA\_WLAN} + D_{AAA\_LTE} + D_{HSS} + D_{PDN\text{-}GW} + D_{S\text{-}GW} + D_{MME} + TE_{prot'}, \quad \text{Eq. (6.35)}$$

em que M_{wd} indica o número de mensagens trocadas no meio com fio; H_{wd} denota o número de *hops* na rede cabeada. Foi assumido que entre o WAAA e o HAAA possuem 3

hops e entre o HAAA e o HSS possuem 2 *hops*. Os demais nós representam um *hop* cada nó; $D_{t(wd)}$ é o atraso de transmissão do meio com fio, sendo que $D_{t(wd)=}$Avg M_{prot}/W_{wd} , em que Avg M_{prot} é o tamanho médio das mensagens de determinado protocolo e W_{wd} é a taxa de dados do meio com fio; $D_{pp(wd)}$ é o atraso de propagação com fio; D_{AR}, D_{AAA_WLAN}, D_{AAA_LTE}, D_{PDN-GW}, D_{S-GW} e D_{MME} são dados pela Equação (6.7); e o atraso relativo a uma consulta ao HSS (D_{HSS}) é dado pela Equação (6.36).

$$D_{HSS} = \Delta HSS \qquad \text{Eq. (6.36)}$$

Na Equação (6.24) não foi considerado o atraso causado pela rede SS7 (ΔSS7), pois já se considera 2 *hops* entre o HAA e o HSS e o atraso de propagação do meio com fio.

TE_{prot} é dado pela Equação (6.28) e neste caso a matriz h, apresentado na Equação (6.29), não irá conter o atraso para geração de vetores de autenticação D_{AV}, pois o atraso D_{HSS} já considera o atraso para geração dos vetores de autenticação do HSS. A matriz h será dada por:

$$h' = [D_{ED}, D_{MAC}, D_{KEY}, D_{ID}], \qquad \text{Eq. (6.37)}$$

A matriz $e_{prot'}$ apresentada na Equação (6.30) é dada por (6.38):

$$e_{prot.\ proposto'} = [2,2,7,1]$$

$$e_{UNAEN\ [30]\ +\ PMIP'} = [2,2,7,1]$$

$$e_{EAP\text{-}FAKA[31]\ +\ PMIPv6'} = [2,2,5,2]$$

$$e_{EAP\text{-}FLAKA[32]\ +\ PMIPv6'} = [0,2,3,2] \qquad \text{Eq. (6.38)}$$

$$e_{EAP\text{-}LUTLS[33]\ +\ PMIPv6'} = [1,3,2,1]$$

$$e_{proposto\ por\ Hassanein,\ A.,\ H.,\ et\ al.\ [35]\ +\ PMIPv6'} = [4,6,10,0]$$

$$e_{EAP\text{-}CRA\ [37]\ +\ PMIPv6'} = [7,6,4,1]$$

$$e_{Reaut.\ EAP\text{-}CRA\ [37]\ +\ PMIPv6'} = [0,5,0,1]$$

A latência de *handover* em todo o domínio quando n.B usuários existem no domínio PMIPv6 é dada por:

$LC' = (T_{prot\text{-}sem\text{-}fio} + T_{prot\text{-}com\text{-}fio}).HO_{Rate\text{-}Dom} = \frac{(T_{prot-sem-fio} + T_{prot-com-fio}).n.v.L.B}{\pi.A}$, Eq. (6.39)

os atrasos M_{wl}, M_{wd}, Avg $M_{prot.}$ e H_{wd} são dados pela Tabela 6.9 e os atrasos D_{ED}, D_{MAC}, D_{KEY} e D_{ID} são dados pela Tabela 6.10. W_{wl} e W_{wd} são setadas para 11 Mbps e 100Mbps, respectivamente e $D_{pp(wd)}$ é setados para 0,5 ms.

As taxas de chegadas e processamentos do UE, AP, AR, WAAA, HAAA, PDN-GW, S-GW, MME e o atraso ΔHSS são dados pela Tabela 6.5.

Em relação ao atraso da interface aérea causado pelas trocas de mensagens do protocolo EAP, será considerado o tempo de retransmissão inicial (RTO_0), expresso pela Equação (6.6), como sendo igual a 200 milissegundos, o número de retransmissões máximas (Nm) é configurado para 5 retransmissões e o atraso médio de transmissão fim a fim do canal WLAN (D) é igual a 0,4 milissegundos para uma WLAN do padrão IEEE 802.11g.

A Tabela 6.11 classifica cada atraso utilizado na modelagem proposta em atraso de processamento nodal, de filas, de transmissão e de propagação:

Tabela 6.11 – Classificação dos atrasos utilizados na modelagem proposta.

Atraso	**Significado**	**Tipo**	**Meio**	**Utilizado na modelagem de**
$D_{t(wl)}$	Atraso de transmissão do meio sem fio	Transmissão	Sem fio	[42]
D_{UE}	Atraso de processamento/filas para o móvel	Processsamento e Filas	Sem fio	[17]
D_{AP}	Atraso de processamento/filas para o *Access Point*	Processsamento e Filas	Sem fio	[17]

D_{EAP}	Troca de mensagens EAP através da interface WLAN	Propagação	Sem fio	[17]
$D_{t(wd)}$	Atraso de transmissão do meio com fio	Transmissão	Com fio	[42]
$D_{pp(wd)}$	Atraso de propagação do meio com fio	Propagação	Com fio	[42]
D_{AR}	Atraso de processamento/filas para o *Access Router*	Processamento e filas	Com fio	[17]
D_{AAA_WLAN}	Atraso de processamento/filas para o servidor de AAA da rede WLAN	Processamento e filas	Com fio	[17]
D_{AAA_LTE}	Atraso de processamento/filas para o servidor de AAA da rede LTE	Processamento e filas	Com fio	[17]
D_{PDN-GW}	Atraso de processamento/filas para o PDN-GW	Processamento e filas	Com fio	[17]
D_{S-GW}	Atraso de processamento/filas para o S-GW	Processamento e filas	Com fio	[17]

D_{MME}	Atraso de processamento/filas para o MME	Processamento e filas	Com fio	[17]
D_{HSS}	Atraso de processamento/filas para o HSS	Processamento e filas	Com fio	[17]

6.3.2 – Avaliação da latência de *handover*

A Figura 6.13 foi gerada a partir da Eq. (6.39) e ilustra a latência de *handover* (s) quando n.B usuários se movimentam a uma velocidade média v (m/s). Neste caso, considera-se que a = 100 m , R=2, n = 10 usuários e a taxa de erro de quadro (FER) é igual a 0,05 (5%).

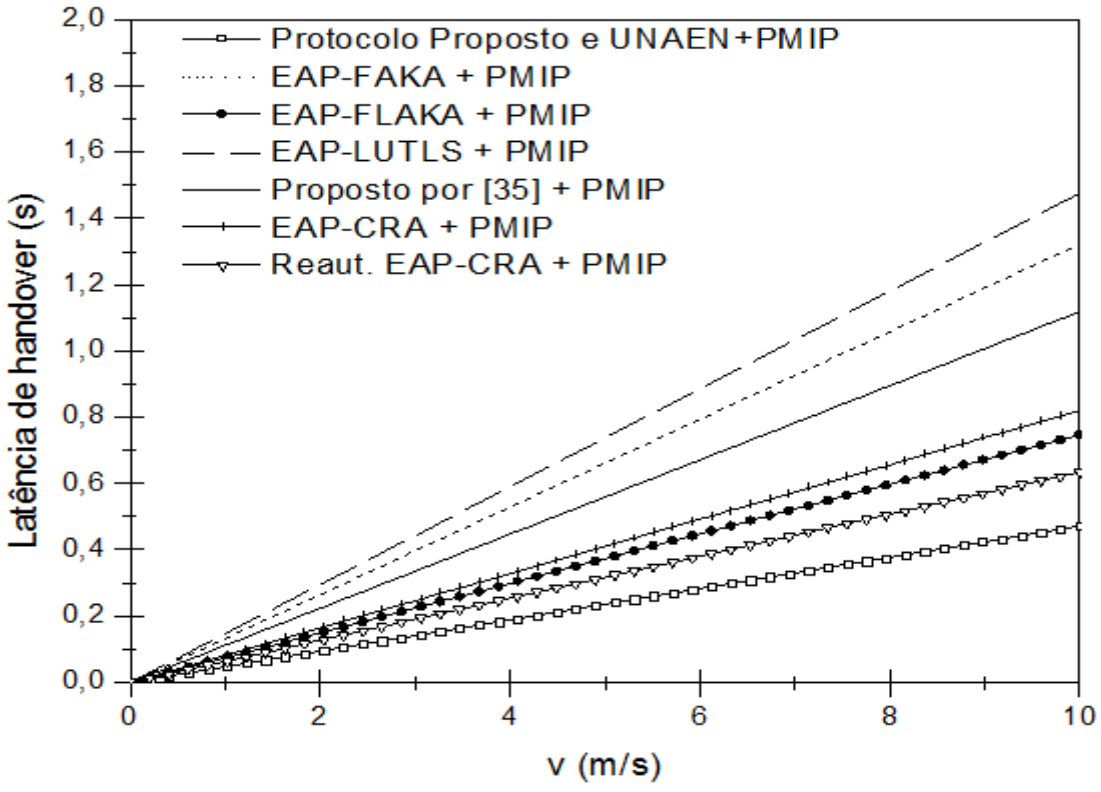

Figura 6.13 – Latência de *handover* vs velocidade média.

Com a inclusão do atraso de filas em cada nó e a taxa de erro de quadro na interface aérea, pode-se observar pela Figura 6.13 que ocorreu um significativo aumento na latência de *handover* comparado com a Figura 6.8. Além do aumento da latência de *handover*, outra diferença significativa entre as Figuras 6.8 e 6.13 foi em relação à latência de *handover* enre os protocolos EAP-CRA e o proposto por Hassanein, A., H., et al. Na Figura 6.8, esses protocolos apresentam a latência de *handover* muito semelhante, porém com a adição dos atrasos de filas o protocolo proposto por Hassanein, A., H., et al., apresentou um grande aumenta na latência devido o fato do atraso de processamento e o atraso de filas do HSS ser bastante elevado, o EAP-CRA por não fazer nenhuma consulta ao HSS, apresentou uma latência de *handover* abaixo do protocolo proposto por Hassanein, A., H., et al.

Assim como nos outros casos analisados, o protocolo proposto também apresentou o melhor desempenho em relação aos demais protocolos estudados, sendo o EAP-LUTLS o protocolo que apresentou a maior latência de *handover*.

A Figura 6.14 foi gerada a partir da Eq. (6.39) e mostra o efeito da latência de *handover* quando se varia o parâmetro R. Neste caso, considera-se que a = 100 m, v=1 m/s, n = 10 usuários e taxa de erro de quadro (FER) é igual a 0,05 (5%).

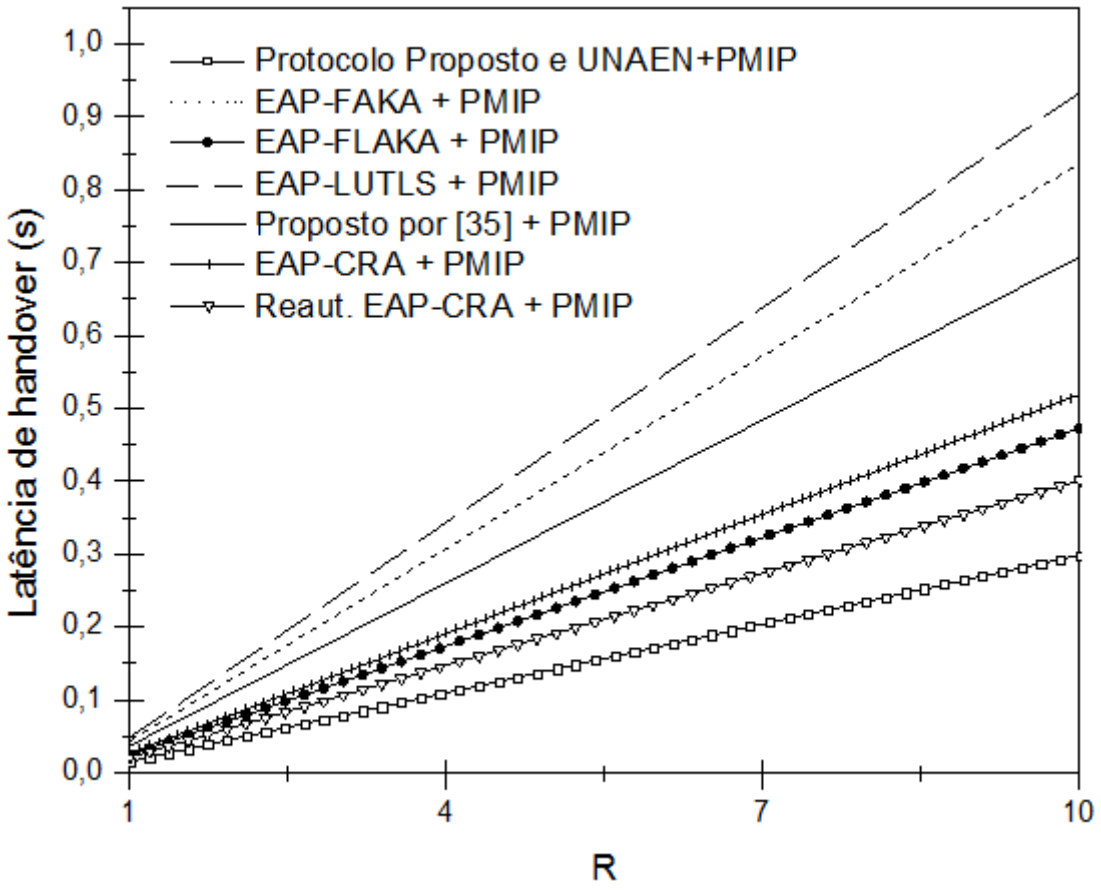

Figura 6.14 – Latência de *handover* vs R.

Assim como na análise da latência de *handover* x velocidade média (Figura 6.13), a adição dos atrasos de fila e a FER na interface sem fio trouxe um aumento significativo da latência de *handover* em todos os protocolos estudados comparando com as Figuras 6.16 e 6.11.

A partir da Figura 6.14, pode-se notar que os protocolos EAP-FAKA, EAP-LUTLS e o proposto por Hassanein, A., H., et al. apresentam uma latência de *handover* significativamente maior do que os demais protocolos, isso se deve ao fato do grande atraso ao se realizar uma consulta ao HSS.

Neste caso também, o protocolo proposto foi o método de autenticação que obteve a menor latência de *handover*.

A Figura 6.15 foi gerada a partir das Eq. (6.39) e mostra o efeito da latência de *handover* quando se varia a taxa de erro de quadro (FER). Neste caso, considera-se que a = 100 m , v = 5 m/s, n = 10 usuários e R = 2.

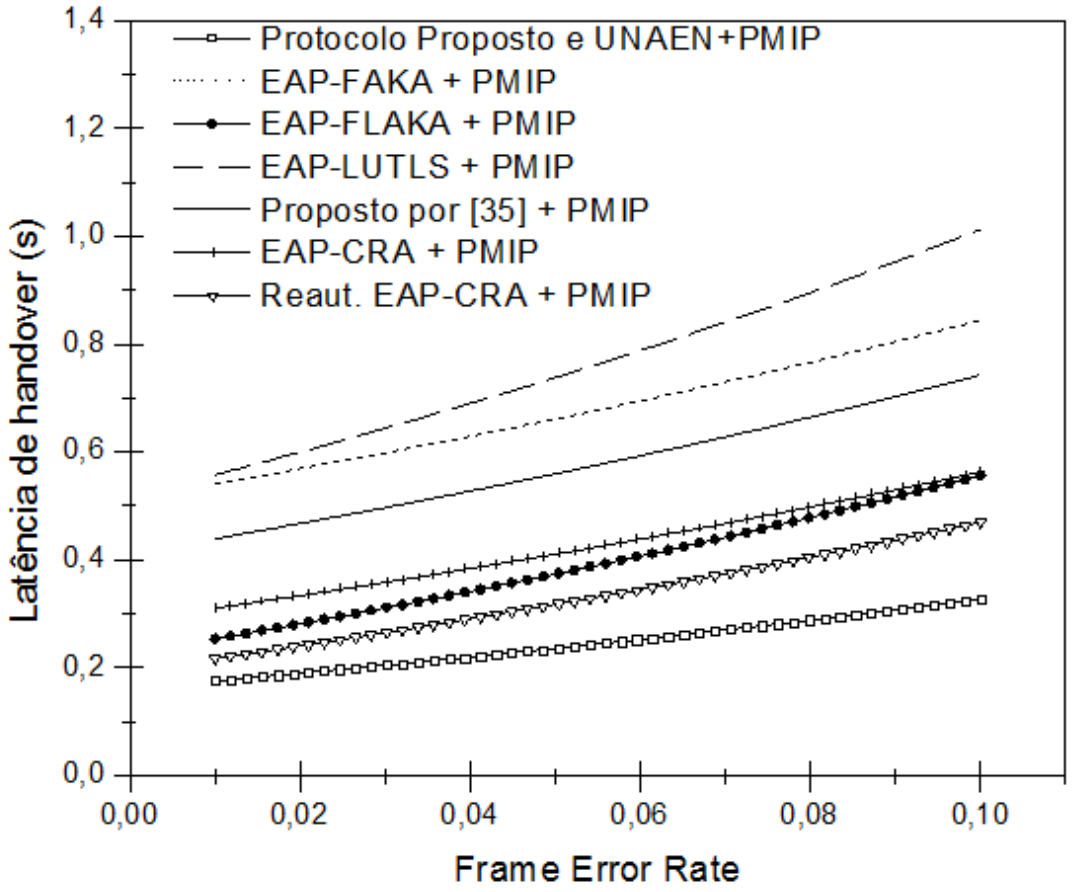

Figura 6.15 – Latência de *handover* vs Taxa de Erro de Quadro.

Pela Figura 6.15, pode-se observar o comportamento da latência de *handover* em função da taxa de erro de quadro para os protocolos de autenticação em um *handover* horizontal entre redes WLANs. Para todos os protocolos, pode-se notar que ocorre um aumento da latência de *handover* com o aumento da FER, pois todos os protocolos trocam mensagens através da interface WLAN. O protocolo proposto e o UNAEN foram os protocolos menos afetados pela FER, pois trocam apenas 3 mensagens através da interface WLAN, enquanto o EAP-LUTS é o protocolo mais afetado pela FER devido o fato deste protocolo trocar 9 mensagens através da interface WLAN, de acodo com a Tabela 6.1.

Em termos de latência de *handover,* o protocolo proposto apresentou a menor latência se comparado aos demais protocolos estudados, devido a troca das 3 mensagens para autenticar o móvel na rede alvo.

6.3.3 – Discussão dos resultados

Neste estudo de caso foi apresentada a avaliação de desempenho do protocolo proposto e dos protocolos estudados em um cenário de *handover* horizontal entre rede WLANs em que o a rede LTE é a rede caseira do móvel e faz o gerenciamento do *handover* entre as redes WLANs. O cenário utilizado foi o mesmo apresentado no segundo estudo de caso, porém o segundo estudo de caso avalia apenas os atrasos de processamento nodal, transmissão e propagação, não incluindo os atrasos relativos a formação de filas nos elementos de rede. O foco deste estudo de caso foi realizar a avaliação do cenário proposto pelo segundo estudo de caso considerando os 4 tipos de atrasos. Os dados relativos aos atrasos de filas foram retirados do primeiro estudo de caso, em que alguns desses valores foram coletados em uma rede real de produção.

Os autores ([42]) em que este trabalho se baseou para a construção do segundo estudo de caso fazem a estimativa de alguns valores para atrasos. Para se ter uma estimativa de latência de *handover* valores estimados são aceitáveis, porém valores obtidos em redes reais fornecem resultados mais próximos aos que são obtidos na realidade. Neste terceiro estudo de caso, além de serem adicionados os atrasos de filas nos elementos de rede, foram utilizados diversos valores obtidos em redes reais por [17] e apresentados no primeiro estudo de caso.

O atraso adicionado que mais impactou na latência de *handover* foi o atraso relativo a uma consulta no HSS. Enquanto que em [42] os autores estimaram um atraso para geração dos vetores de autenticação pelo HSS de 12 μs, em [17] foi feita uma medição em rede real com valor de 0,14034 segundos.

6.4 – PROPRIEDADES DE SEGURANÇA

Nesta seção, será feito a análise e comparação do protocolo proposto e dos diversos métodos de autenticação citados até aqui em termos de propriedades de segurança, como proteção contra ataques do tipo *Man in the middle*, *Replay*, autenticação mútua entre o móvel e a rede WLAN, dentre outras. Também serão detalhadas as propriedades de segurança do protocolo proposto.

6.4.1 – Proteção contra ataques do tipo *Man in the middle* (MitM)

Nos ataques do tipo MitM, o atacante se posiciona entre dois nós que se comunicam, interceptando as mensagens enviadas e depois se passa por uma das partes envolvidas.

Proteção contra esse tipo de ataque é feita protegendo o ID do dispositivo móvel (*User* ID) com uma chave secreta, normalmente de posse do UE e dos servidores de AAA, fazendo com que o atacante não consiga recuperar e modificar o *User* ID.

6.4.2 – Autenticação mútua

A autenticação mútua é a propriedade em que a rede alvo autentica o UE e este também verifica a autenticidade da rede alvo. Para garantir a autenticação mútua, normalmente são verificados os parâmetros de segurança tanto do móvel quanto da rede alvo.

6.4.3 – Proteção contra ataques do tipo *Replay*

Os ataques do tipo *Replay* são uma variação dos ataques do tipo MitM e consistem no reenvio de pacotes fora de ordem ou contexto para burlar alguma etapa do processo de autenticação.

O uso de um número sequencial nos pacotes de autenticação, são utilizados para proteção contra ataques do tipo *Replay*.

6.4.4 – Proteção do *User* ID

O furto do *User* ID é a base de diversos ataques de personificação, como no caso do ataque MitM. A proteção do *User* ID normalmente é feita atribuindo um ID temporário ao móvel a cada nova autenticação.

6.4.5 – *Perfect Forward Secrecy*

Esta propriedade assegura que se uma chave de sessão for derivada de um conjunto de parâmentros, ela não poderá ser comprometida caso um dos parâmetros de segurança sejam comprometidos no futuro.

6.4.6 – Verificação de integridade

A verificação de integridade assegura que o pacote não foi modificado de maneira maliciosa ou acidental. A verificação da integridade é feita normalmente utilizando códigos de autenticação de mensagem (MAC) e evitam principalmente ataques de negação de serviço (DoS).

6.4.7 – Derivação de um protocolo de reautenticação

Esta propriedade consiste na derivação de um método de reautenticação de protocolos de autenticação. Como já dito anteriormente, a reautenticação é utilizada nos casos em que o móvel se reassocia com uma mesma rede WLAN com frequência e auxilia na redução da latência de *handover.*

6.4.8 – Comparação entre os protocolos de autenticação

Nesta subseção, será feito a análise das propriedades de segurança para cada método de autenticação, como mostrado na Tabela 6.12.

Tabela 6.12 – Propriedades de segurança.

Método de autenticação	**Proteção Contra *Man in the middle***	**Autenticação mútua**	**Proteção contra ataques de *Replay***	**Proteção do *User ID***	***Perfect Forward Secrecy***	**Verificação de integridade**	**Possui reautenticação**
UNAEN / Protocolo Proposto	X	X	X	X	X	X	-
EAP-FAKA	X	X	X	X	-	X	x
EAP-FLAKA	X	X	X	X	-	X	Não se aplica
EAP-LUTLS	X	X	X	X	-	X	-
Proposto por Hassanein, A., H., et al. [35]	X	X	X	X	X	X	-
EAP-CRA	X	X	X	X	-	X	x
Reauten. EAP-CRA	X	X	X	X	-	X	Não se aplica

Com base na Tabela 6.12, todos os métodos de autenticação possuem proteção contra ataques do tipo *Man in the middle*. Para os protocolos citados na Tabela 6.12, a segurança contra este tipo de ataque se deve ao fato do *User ID* ser protegido por uma chave secreta, com isso o atacante não consegue recuperar e modificar o *User* ID.

Outra propriedade que todos os métodos de autenticação possuem é a autenticação mútua entre as entidades que participam do processo de autenticação. Neste caso entre o móvel e a rede alvo (rede WLAN).

Todos os métodos também possuem proteção contra ataques do tipo *Replay*. Esquemas que utilizam um número de sequencia nos pacotes de autenticação, como no EAP-CRA, são utilizados para proteção contra ataques do tipo *replay*.

Para evitar que atacantes possam descobrir o *User* ID, todos os métodos possuem abordagens que protegem a privacidade do *User* ID.

O protocolo proposto por Hassanein, A., H., et al. e o UNAEN proveem *Perfect Forward Secrecy*. Esta propriedade assegura que se uma chave de sessão for derivada de um conjunto de chaves *long term*, ela não poderá ser comprometida caso uma das chaves *long term* seja comprometida no futuro.

A verificação da integridade dos pacotes de autenticação é feita também por todos os métodos através do uso do Códico de Autenticação de Mensagem (MAC).

Por fim, apenas o EAP-FAKA e o EAP-CRA possuem esquemas com uma abordagem de reautenticação, que irádiminuir a latência de *handover* a usuários que retornam com frequência a uma mesma rede WLAN.

6.4.9 – Propriedades de segurança do protocolo proposto

Nesta subseção, será feito o detalhamento das propriedades de segurança do protocolo proposto apresentadas na Tabela 6.12.

6.4.9.1 – Autenticação mútua

Para o procedimento de autenticação mútua que será apresentado nesta subseção tem-se os seguintes parâmetros e chaves de segurança:

- ID_{UE} e ID_{AP}: Identificadores temporários do móvel e do AP, respectivamente;

- Par (s_{UE}, R_{UE}): Chaves *long term* do UE geradas pelo KGC.

- Par (s_{AP}, R_{AP}): Chaves *long term* do AP geradas pelo KGC.

- a: número aleatório gerado pelo UE.

- b: número aleatório gerado pelo AP.

- T_{UE}: Parâmetro de segurança gerado pelo UE a partir do número aleatório a.

- T_{AP}: Parâmetro de segurança gerado pelo AP a partir do número aleatório b.

-PK: Chave pública do UE.

- H1 e H2: Funções de *hash* seguras.

- $K1_{AM}$ e $K2_{AM}$: Parâmetros de segurança que são utilizados para a realização da autenticação mútua e geração da chave de sessão.

Assim como no caso do UNAEN, o protocolo proposto também provê autenticação mútua entre o móvel e o AP da rede WLAN alvo. Neste modelo, o UE e o AP verificam os valores de *hash* um do outro e verificam os seus parâmetros de segurança como mostrado abaixo:

$K1_{MA} = s_{UE}\, T_{AP} + a(R_{AP} + H_1\,(ID_{AP}\, R_{AP})PK)$

$= s_{UE}\, bP + as_{AP}\, P$

$= s_{AP}\, aP + b(R_{UE} + H_1\,(ID_{UE} \,||\, R_{UE})\, PK)$

$= s_{AP}\, T_{UE} + b(R_{UE} + H1\,(ID_{UE} \,||\, R_{UE})PK) = K1_{AM}$

$K2_{MA} = aT_{AP} = abP = baP = K2_{AM}$

Gerados os parâmetros $K1_{AM}$ e $K2_{AM}$, a chave de sessão para o uso do móvel e do AP pode ser gerada por:

$PTK = H2\,(ID_{UE} \,||\, ID_{AP} \,||\, T_{UE} \,||\, T_{AP} \,||\, K1_{MA} \,||\, K2_{MA})$

Apenas UEs e APs legítimos podem gerar os valores de *hashs* válidos obtidos pelo outro.

6.4.9.2 – Proteção contra ataques do tipo *Man in the Middle* (MitM)

Como a geração e distribuição de chaves é baseado em um esquema *Computational Diffie-Hellman* (CDH), um atacante não é capaz de derivar a chave de sessão PTK com base apenas nos parâmetros públicos, desse modo não podendo realizar um ataque de personificação.

6.4.9.3 – Proteção contra ataques do tipo *Replay*

O atacante pode capturar a mensagem REQ durante o *handover* e repassá-la. Como o atacante não tem acesso ao AP e ao UE, este não possui a correta PTK e assim não pode gerar as mensagens de REP e ACK válidas.

6.4.9.4 – Proteção do *User* ID

Como o ID do móvel é gerado a cada nova sessão, o atacante não pode associar um ID temporário a um determinado UE.

6.4.9.5 – *Perfect Forward Secrecy*

Esta propriedade assegura que se uma chave de sessão for derivada de um conjunto de parâmetros de segurança, ela não poderá ser comprometida caso um dos parâmetros de segurança sejam comprometidos. Nesse caso, se algum parâmetro de segurança for roubado, a chave de sessão PTK não poderá ser derivada.

6.5 – CONSIDERAÇÕES FINAIS

Com base em modelos analíticos, verificou-se que o protocolo proposto apresentou os melhores desempenhos, em termos de latência e sinalização de *handover*, nos três estudos de caso se comparado aos demais protocolos estudados. Com base neste Capítulo, tem-se uma boa estimativa da comparação entre o protocolo proposto e os demais protocolos

estudados nos cenários de *handover* vertical no sentido LTE → WLAN e no de *handover* horizontal entre redes WLANs em que a rede LTE é a rede caseira do móvel. Apesar do protocolo proposto ter apresentando um desempenho satisfatório, pretende-se validar este desempenho em trabalhos futuros com base em simulações e/ou medidas em protótipos.

Um aspecto importante, que permeia os 3 (três) estudos de caso e todos os protocolos considerados, envolve a geração e a distribuição de chaves, tanto de longo prazo (*long term*) quanto de sessão. Esse aspecto é aqui tratado face à ligação com o foco do trabalho e os resultados obtidos na avaliaçãoo de desempenho.

Para esse fim, servimo-nos da Tabela 4.1, onde pode-se observar que, em relação ao número de chaves e/ou parâmetros de segurança gerados durante o procedimento de *handover*, o protocolo de reautenticação do EAP-CRA apresentou o melhor desempenho, não gerando nenhuma chave ou parâmetro de segurança durante o procedimento de *handover*, pois este protocolo faz uso das chaves geradas anteriormente na autenticação completa do protocolo EAP-CRA. O protocolo proposto e o UNAEN apresentaram um bom desempenho, gerando apenas a chave de sessão PTK, como já apresentado na Subseção 4.2.2. Em contrapartida, o EAP-FAKA foi o protocolo que apresentou o pior desempenho, sendo geradas 6 chaves criptográficas durante o procedimento de *handover*.

Em relação às chaves de *long term* (geradas anteriormente ao processo de *handover*), todos os protocolos geram pelo menos 1 chave criptográfica de *long term* durante essa fase. Os protocolos que realizam a reautenticação, como o EAP-FLAKA e o EAP-CRA em modo de reautenticação, utilizam as chaves geradas nos procedimentos de autenticação completa. No protocolo proposto e no UNAEN, o KGC gera um par de chaves *long term* para UE e para o AP. O EAP-LUTLS e o proposto por Hassanein, A., H., et al. geram apenas 1 chave *long term* e esta é pré-compartilhada entre o móvel e o HSS, enquanto que o EAP-CRA gera 2 chaves *long term* e o EAP-FAKA gera um par de chaves que também são pré-compartilhados entre o móvel e o HSS.

Como o foco do trabalho é a avaliação do processo de *handover*, nas análises de desempenhos apresentadas nos três estudos de caso, foi considerado apenas os procedimentos realizados durante aquele processo, desta maneira, não foram considerados os atrasos relativos à preparação para o futuro *handover* do protocolo proposto e do

UNAEN e também a geração e o pré-compartilhamento das chaves *long term* nos protocolos EAP-FAKA, EAP-LUTLS, proposto por Hassanein, A., H., et al. e EAP-CRA.

7 – CONCLUSÕES E TRABALHOS FUTUROS

7.1 – CONCLUSÕES

Este trabalho apresentou uma proposta preliminar de um protocolo seguro e que apresente uma baixa latência de *handover* em uma arquitetura de integração LTE-WLAN. O protocolo proposto altera as mensagens do PMIPv6 com o objetivo de prover um procedimento de preparação para o futuro *handover* ao protocolo UNAEN. A escolha do UNAEN se deve ao fato deste protocolo trocar apenas 3 mensagens durante o *handover* para autenticar o móvel, porém para o correto funcionamento deste protocolo, deve-se fazer os procedimentos necessários de preparação para o futuro *handover*.

Em adição ao UNAEN, foram apresentadas outras 6 técnicas de autenticação para comparação com o protocolo proposto, que são os métodos de autenticação completa EAP-FAKA, EAP-LUTLS, método proposto por Hassanein, A., H., et al., EAP-CRA e os procedimentos de reautenticação EAP-FLAKA e a reautenticação do EAP-CRA. Foi utilizado uma arquitetura de integração LTE-WLAN do tipo SAE, apresentada na norma 3GPP TS 23.402 [9], para a realização da comparação entre os protocolos.

A avaliação de desempenho dos protocolos foi tratada em três estudos de caso. No primeiro, o móvel deslocava-se entre uma rede LTE e uma WLAN, sem considerar a possibilidade de o móvel escolher entre outras WLANs para se conectar. Para prover o gerenciamento de mobilidade foi utilizado o PMIPv6 modificado para o protocolo proposto e o PMIPv6 para os demais métodos de autenticação. Foi utilizado um cenário no qual ocorre a formação de filas nos dispositivos de rede, tendo assim um atraso relativo ao *buffer* e ao tempo de serviço dos elementos e enlaces. Para a modelagem das filas utilizou-se a teoria clássica de filas em que, em cada elemento, ocorre a formação de filas do tipo M/M/1.

Avaliou-se a latência de *handover* em função da taxa de erro de quadro (FER) e o protocolo proposto e o UNAEN apresentaram resultados satisfatórios, tendo a latência de *handover* um pouco menor do que os protocolos de reautenticação e consideravelmente menor do que os protocolos que utilizam autenticação completa.

No segundo estudo de caso, seguindo modelagem utilizada por [42], considerou-se aspectos de mobilidade do UE, utilizando um cenário de *handover* horizontal entre redes

WLANs em que a rede LTE é a rede caseira do móvel e as redes WLANs são as redes visitadas. A rede LTE possui área de cobertura em todo domínio PMIPv6, enquanto as redes WLANs possuem área reduzida. Neste cenário, o dispositivo móvel pode realizar o procedimento de *handover* para qualquer rede WLAN pertencente ao domínio PMIPv6.

Primeiramente foram avaliados os protocolos proposto em termos de trocas de sinalização em função da velocidade média do móvel e do tamanho do domínio PMIPv6. Por fim, a latência de *handover* foi avaliada também em função da velocidade média do móvel e do tamanho do domínio PMIPv6. Em ambos os casos, o protocolo proposto e o UNAEN apresentaram os melhores resultados.

No terceiro estudo de caso, fez-se uma modelagem considerando aspectos das modelagens tratadas por [17] e [42], com algumas alterações. No modelo proposto por [17], são considerados os atrasos de processamento nodal, de fila, o atraso de propagação no meio sem fio e a perda de quadro na interface sem fio da WLAN. Em [42] não foram considerados os atrasos de filas e a dependência da taxa de erro de quadro. No modelo analítico proposto, foram considerados a perda de quadros e os 4 principais atrasos em redes de comunicação: atraso de processamento nodal, atraso de fila, atraso de transmissão e o atraso de propagação. Neste modelo foi utilizado o mesmo cenário apresentado na segunda abordagem.

No modelo proposto, foi avaliada a latência de *handover* em termos da velocidade média, do parâmetro R e da taxa de erro de quadro, sendo que nos três casos o protocolo proposto e o UNAEN tiveram o melhor desempenho.

Por fim, foi feita a comparação entre os protocolos em termos das seguintes propriedades de segurança: proteção contra ataques do tipo *Man in the Middle* e *Replay*, proteção do *user* ID, autenticação mútua entre o móvel e a rede WLAN, *Perfect Forward Secrecy*, verificação de integridade e a existência de um método de reautenticação associado a determinado protocolo de autenticação. Dentre as propriedades de segurança, todos os métodos de autenticação avaliados possuíram proteção contra ataques *Man in the middle* e *Replay*, proteção do *user* ID, verificação de integridade das mensagens de autenticação e autenticação mútua entre o móvel e a rede alvo. O protocolo proposto em caráter preliminar, o UNAEN e o método proposto por Hassanein, A., H., et al., possuíam

a propriedade *Perfect Forward Secrecy*. O EAP-FAKA e o EAP-CRA foram os únicos protocolos que possuem métodos de reautenticação.

Apesar de o protocolo proposto apresentar excelentes resultados em relação à sinalização e latência de *handover,* ele apresenta algumas desvantagens como a obrigação do usuário em utilizar o PMIPv6 para prover o gerenciamento de mobilidade e a alteração do protocolo PMIPv6 para prover a pré-autenticação ou preparação para o futuro *handover* do móvel.

7.2 – SUGESTÕES DE TRABALHOS FUTUROS

Finalmente, são feitas propostas de alguns temas relevantes que não puderam ser abordados ou que não foram esclarecidos completamente no decorrer deste trabalho. Os temas sugeridos são listados abaixo:

- Avaliação da arquitetura utilizada por meio de simulações e/ou medidas em protótipos;
- Uso do protocolo proposto com outras abordagens que utilizam o esquema de pré-autenticação e/ou preparação para o futuro *handover*;
- Avaliação do uso do protocolo proposto em outras interconexões de redes sem fio, como LTE-Ad Hoc, LTE-WiMAx, WiMAx-WLAN, dentre outras;
- Avaliação da viabilidade de um método de reautenticação para o protocolo proposto;
- Uso do protocolo proposto com outras técnicas de gerenciamento de mobilidade derivadas do PMIPv6, como o PMIPv6 distribuido.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] 3GPP TS 33.402 V12.4.0 (2014-10): "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[2] http://www.3gpp.org/technologies/keywords-acronyms/98-lte, acessado em: 08 de março de 2015.

[3] ftp://ftp.3gpp.org/Inbox/2008_web_files/LTA_Paper.pdf, acessado em: 08 de março de 2015.

[4] *LTE for UMTS: Evolution to LTE-Advanced*, Second Edition. Edited by Harri Holma and Antti Toskala.© 2011 John Wiley & Sons, Ltd. Published 2011 by John Wiley & Sons, Ltd. ISBN: 978-0-470-66000-3.

[5] 3GPP TS 23.401 V13.1.0 (2014-12): "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[6] 3GPP TS 23.002 V13.1.0 (2014-12): "Network Architecture".

[7] *An introduction to LTE : LTE, LTE-advanced, SAE and 4G mobile communications*, First Edition, Christopher Cox. 2012 John Wiley & Sons, Ltd. Published 2012 by John Wiley & Sons, Ltd. ISBN: 978-1-119-97038-5.

[8] LTE Security. Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi . John Wiley & Sons, 26/10/2010 - 298 páginas

[9] 3GPP TS 23.402 V12.6.0 (2014-09): “Architecture enhancements for non-3GPP accesses”.

[10] http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core, acessado em: 13 de março de 2015.

[11] http://www.3gpp.org/technologies/keywords-acronyms/101-carrier-aggregation-explained, acessado em: 15/03/2015.

[12] *Heterogeneous Wireless Access Networks Architectures and Protocols*. Edited by Ekram Hossain.© 2009Springer US. ISBN: 978-0-387-09776-3

[13] Albuquerque, Silas Leite, and Paulo Roberto de Lira Gondim. "Applying Continuous Authentication to Protect Electronic Transactions." *Information Assurance and Security Technologies for Risk Assessment and Threat Management*: Advances: Advances (2011): 134.

[14] Aboba, Bernard, et al. "RFC 3748-Extensible authentication protocol (EAP)." Network Working Group (2004).

[15] Aboba, B., D. Simon, and P. Eronen. "RFC 5247-Extensible authentication protocol (EAP) key management framework." Network Working Group (2008)..

[16] Rigney, Carl, Steve Willens, and A. Rubens. W. Simpson," Remote Authentication Dial in User Service (RADIUS). RFC 2865, June, 2000.

[17] RIBEIRO JR, Sebastião Boanerges. Proposta de modelo de autenticação para interconexão de redes sem fio heterogêneas.2011. 227 p. Dissertação (Mestrado em Engenharia Elétrica) – Universidade Nacional de Brasília, Brasília, 2011. [Orientador: Prof. Dr. Paulo R. L. Gondim].

[18] J. Bannister, P. Mather, S. Coope, "*Convergence Technologies for 3G Networks: IP, UMTS, EGPRS and ATM*", John Wiley & Sons, 2004.

[19] Albuquerque, Silas Leite, Paulo Roberto de Lira Gondim, and Cláudio de Castro. "Aspectos de Segurança na Interconexão de Redes Celulares e WLANs.", Minicurso apresentado no *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacioanais (SBSeg)* 2010.

[20] Soliman, H. "RFC 5555: Mobile IPv6 support for dual stack hosts and routers." Request for Comments 5555 (2009).

[21] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[22] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[23] Gundavelli, S., et al. B. Patil," Proxy Mobile IPv6. RFC 5213, August, 2008.

[24] Zekri, Mariem, Badii Jouaber, and Djamal Zeghlache. "A review on mobility management and vertical *handover* solutions over heterogeneous wireless networks." *Computer Communications* 35.17 (2012): 2055-2068.

[25] Márquez-Barja, Johann, et al. "An overview of vertical *handover* techniques: Algorithms, protocols and tools." *Computer Communications* 34.8 (2011): 985-997.

[26] Gondim, Paulo RL, and Jose BM Trineto. "DSMIP and PMIP for mobility management of heterogeneous access networks: Evaluation of authentication delay." *Globecom Workshops (GC Wkshps)*, 2012 IEEE. IEEE, 2012.

[27] Chung, Jong-Moon, et al. "Enhancements to FPMIPv6 for improved seamless vertical *handover* between LTE and heterogeneous access networks." *Wireless Communications*, IEEE 20.3 (2013): 112-119.

[28] Gohar, Moneeb, Sang-Il Choi, and Seok-Joo Koh. "Load Balancing for Proxy Mobile IPv6 in SAE-based Mobile Networks.", 2014.

[29] Cao, Jin, et al. "A survey on security aspects for LTE and LTE-A networks." *Communications Surveys & Tutorials*, IEEE 16.1 (2014): 283-302.

[30] Jin Cao; Maode Ma; Hui Li, "An Uniform *Handover* Authentication between E-UTRAN and Non-3GPP Access Networks," *Wireless Communications*, IEEE Transactions on, vol.11, no.10, pp.3644,3650, October 2012.

[31] Idrissi, Y.E.H.E.; Zahid, N.; Jedra, M., "Security analysis of 3GPP (LTE) — WLAN interworking and a new local authentication method based on EAP-AKA," *Future Generation Communication Technology (FGCT)*, 2012 International Conference on, vol., no., pp.137,142, 12-14 Dec. 2012.

[32] El Hajjaji El Idrissi, Younes; Zahid, Noureddine; Jedra, Mohamed, "A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA," *Telecommunications (ICT), 2013 20th International Conference* on, vol., no., pp.1,5, 6-8 May 2013

[33] Chou-Chen Yang; Shin-Hao Lo; Lu, E.J., "A Universal Lightweight Authentication Scheme Based on Delegation Mechanism in Heterogeneous Networks," *Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC)*, 2012 9th International Conference on, vol., no., pp.963,966, 4-7 Sept. 2012.

[34] Bouabidi, I.E.; Daly, I.; Zarai, F., "Secure handoff protocol in 3GPP LTE networks," *Communications and Networking (ComNet), 2012 Third International Conference* on, vol., no., pp.1,6, March 29 2012-April 1 2012.

[35] Hassanein, Ahmed H., et al. "New Authentication and Key Agreement Protocol for LTE-WLAN Interworking." *International Journal of Computer Applications 61.19 (2013)*: 20-24.

[36] Sithirasenan, E.; Kumar, S.; Ramezani, K.; Muthukkumarasamy, V., "An EAP Framework for Unified Authentication in Wireless Networks," *Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011 IEEE 10th International Conference on, vol., no., pp.389,397, 16-18 Nov. 2011.

[37] Sithirasenan, E.; Ramezani, K.; Muthukkumarasamy, V., "Enhanced CRA protocol for seamless connectivity in wireless networks," *Communications and Information Technologies (ISCIT)*, 2012 International Symposium on, vol., no., pp.1075,1079, 2-5 Oct. 2012.

[38] S. K. Das, E. Lee, K. Basu, S.K. Sen, “Performance optimization of VoIP calls over wireless links using H.323 protocol”, *IEEE Transactions on Computers* 52 (6) (2003) pp. 742–752, Junho 2003.

[39] Edward, E. Prince, and V. Sumathy. "Performance analysis of a context aware cross layer scheme for fast handoff in IMS based integrated WiFi–WiMax networks." *Pervasive and Mobile Computing* (2014).

[40] Liao, Jianxin, et al. "A dual mode self-adaption handoff for multimedia services in mobile cloud computing environment." *Multimedia Tools and Applications* (2015): 1-26.

[41] Machado, Cristian Cleder, et al. "Towards SLA Policy Refinement for QoS Management in Software-Defined Networking." Advanced Information Networking and Applications (AINA), *2014 IEEE 28th International Conference on*. IEEE, 2014.

[42] Ali, A. S. “Authentication and Key management in heterogeneous wireless networks.” Electrical and Computer Engineering, The University of British Columbia (2010).

[43] - G. Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function”, *IEEE Journal on Selected Areas in Communications*, vol. 18, issue: 3, pp. 535–547, Março 2000.

[44] A. Diab, A. Mitschele-Thiel, K. Getov, and O. Blume, “Analysis of proxy MIPv6 performance compared to fast MIPv6,” in *IEEE Conference on Local Computer Networks (LCN)*, Oct. 2008, pp. 579–580.

[45] Kurose, James F. *Computer Networking: A Top-Down Approach Featuring the Internet*, 3/E. Pearson Education India, 2005. NBR 6023.

[46] Bose, Sanjay K. *An introduction to queueing systems*. Springer Science & Business Media, 2013.

[47] Weng, Chien-Erh, and Hsing-Chung Chen. "The performance evaluation of IEEE 802.11 DCF using Markov chain model for wireless LANs." *Computer Standards & Interfaces 44* (2016): 144-149.

[48] Ma, Xiaomin, and Kishor S. Trivedi. "Reliability and performance of general two-dimensional broadcast wireless network." *Performance Evaluation 95* (2016): 41-59.

[49] L. Tie, D. He, J. Li, and J.H. Tang, "Performance Analysis of Authentication Method for Proxy Mobile IP Protocol", *in Proc. BMEI*, 2009, pp.1-4.

APÊNDICE A – PUBLICAÇÕES

1 - TRINETO, J. B. L. ; Gondim, P.R.L. . DSMIP and PMIP for Mobility Management of Heterogeneous Access Networks: Evaluation of Authentication Delay. In: 1st International Workshop on Emergent Technologies for Smart Devices (GLOBECOM 2012), 2012, Anaheim, California (USA). Proceedings of the 1st International Workshop on Emergent Technologies for Smart Devices (ETSD - GLOBECOM 2012), 2012. p. 308-313.

2 - TRINETO, J. B. L. ; Gondim, P.R.L. . "Comparing Authentication Protocols for Heterogeneous Wireless Networks". Artigo publicado ao VII Congreso Internacional de Computación y Telecomunicaciones, COMTEL 2015.

DSMIP AND PMIP FOR MOBILITY MANAGEMENT OF HETEROGENEOUS ACCESS NETWORKS: EVALUATION OF AUTHENTICATION DELAY

Paulo R. L. Gondim[1]

José B. M. Trineto[2]

Universidade de Brasília – Departamento de Engenharia Elétrica

(1) pgondim@unb.br (2) jbenicio@unb.br

Abstract —**The evolution of wireless networks involves the development of several standards, considering different radio access technologies. In a scenario of integration of heterogeneous access technologies, the optimization of vertical *handover* involves the need of reduction of authentication delays. Int his paper, the authentication latency is evaluated by the utilization of an analytical model, considering the use of Proxy Mobile IPv6 (PMIPv6) and Dual Stack Mobile IPv6 (DSMIPv6) protocols for providing mobility management.**

Keywords – Heterogeneous Networks, Authentication, Interconnection.

I. INTRODUCTION

Due to the increase of portable terminals, e.g. notebooks and smart phones, wireless communication networks are into an increasing evolution. Several wireless networks (like GSM, UMTS, LTE and WLAN) were developed, and interconnecting all these networks is one of the greatest challenges in the area.

The convergence of these networks has appeared to unify and create an unique, intelligent and efficient infrastructure, based on the integration supplied by these heterogeneous access networks. Among the innumerous advantages of integrated heterogeneous networks we can cite as follows:

- Increasing of the service area of networks;
- Possible decreasing of service costs for users;
- Availability of new services by operators;
- Possibility of greater efficiency in terms of QoS (Quality of Service) for users;

One of the most critical questions in wireless communication networks interconnection is the handoff latency as well as the continuity of session when a mobile moves from one network to another.

The tendency is that, in a near future, the convergence of more and more wireless network technologies may occur, and some existing problems must be solved. Questions regarding mobility management, security, handoff latency, session continuity, among others, have been the focus of several papers with the purpose of development of more efficient and robust networks.

Some types of services such as internet video transmissions and VoIP (Voice over IP) have determined acceptable levels of QoS for services to work properly with a good quality for the user. For these levels of QoS to be reached, the handoff latency must be as minimum as possible and session discontinuity must not happen.

In a handoff between different access networks, mobile authentication on target network is one of the most onerous processes. For this authentication process to succeed the exchange of several messages by network elements usually occur.

One of the strategies to have session continuity and decreasing of handoff latency is the use of protocols which have the finality of supplying mobility management, like Proxy Mobile IPv6 (PMIPv6) and Dual Stack Mobile IPv6 (DSMIPv6). An important part of the handoff latency is due to the use of authentication protocols. In this paper, authentication latency between a UMTS and a WLAN network using PMIPv6 and DSMIPv6 protocols will be evaluated.

This paper is organized as follows: sections II and III present the basic concepts about PMIPv6 and DSMIPv6 protocols respectively; section IV presents related papers; section V presents the case study with the adopted target architecture; section VI shows the analytical modeling which was performed; section VII presents the results and its respective analysis, and section VIII shows the conclusions.

II. DUAL STACK MOBILE IPv6

The Dual Stack Mobile IPv6 (DSMIPv6) is a protocol that operates with IPv6 and IPv4, being the Home Agent (HA) the entity that stores the Home Address (HoA) and the Care of Address (CoA).

For mobile communication with acorresponding node (CN), the packets are intercepted by HA and passed onto their final destination. However, if IPv6 is being used, the route optimization can be used, thus the mobile can exchange messages directly with the CN, without the need of the messages passing through HA.

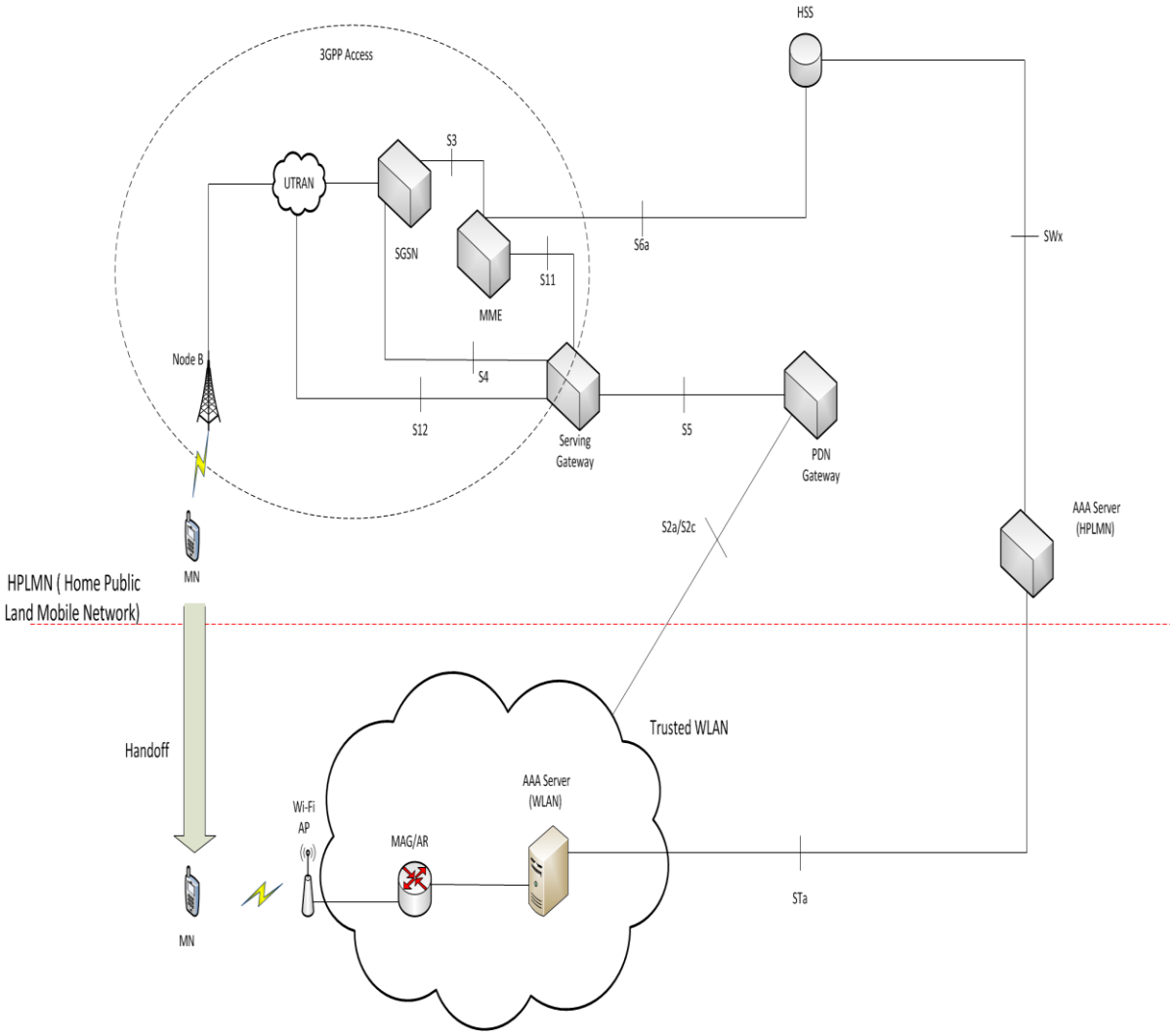

Fig. 1. Target Architecture

DSMIP has some problems such as the high latency handoff, due to the high number of messages exchanged in that process of handoff. Moreover, it is amobility management protocol that requires modification of the protocol stack of the mobile node.

III. Proxy Mobile IPv6

In order to solve the problems related to high latency handoff and the modification of the protocol stack of the mobile, it was developed a protocol in which the mobilitybased on the network, called Proxy Mobile IPv6 (PMIPv6).

Mobility in PMIPv6 is concentrated on an administrative domain, called PMIPv6 domain. ThePMIPv6 defines two new entities, the LMA(Local Mobility Anchor) and the MAG (Mobile Access Gateway). The LMA is similar to Home Agent in DSMIPv6, intercepting packets destined to the mobile terminal and tunneling for the MAG, which after passes them to the mobile station. The MAG works as a proxy, being responsible for the detection of the association point of MN and on its behalf performs the necessary procedures to provide mobility.

IV. Related Work

In [1], it is made a comparison of handoff latency between PMIPv6, MIPv6 and HMIPv6 protocols in a homogeneous networks scenario. From ananalytical model that deemed delays as being deterministic, the authors deduced the expressions of handoff latency between MAG/AR of each protocol, taking into account the delay on mobile authentication by the Authentication, Authorization and Accounting (AAA) server. From this analytical model, acomparison of handoff latency protocols is accomplished, considering the propagationdelay of wireless medium, the delay between the mobile and the corresponding node and the delay related to motion detection. For the three scenarios, the PMIPv6 was the protocol that presented the lowest handoff latency.

In [2], the authors evaluated the handoff latency between MAGs/ARs for MIPv6 and PMIPv6 protocols in a homogeneous network scenario, similar to the one used in [1]. The authors considered the delays relating to mobile authentication by AAA server and the delay of wireless medium as given by reference [5]. The mentioned latency was evaluated on the basis of frame error rate (FER) and the PMIPv6 was less affected by the protocol, showing its lowest handoff latency.

In [3], the author used a scenario where a MN moves from a GSM network to a WLAN andEAP-SIMfortheprovision of security. Ananalytical model based on the queueing theory was developed for the analys is of handoff latency, with M/M/1 model adopted for each network element. The author also proposes an architecture to achievead ecreased latency handoff, that introduces an element called theKey Distribution Server (KDS), responsible for performing the early distribution of temporary authentication keys for the mobile terminal in the next handoff.

In [4], the authors make an analysis of handoff latency when a mobile node moves from a 3G network to a WLAN. The EAP-AKA protocol is considered for authentication, authorization and accounting for MN; a DHCP server is used for addressing purposes, and MIPv4 is used for mobility management. For the handoff latency evaluation the OPNET simulator was used.

This paper evaluates the authentication latency of PMIPv6 protocol in a heterogeneous network scenario, while the papers [1] and [2] evaluate this protocol in a homogeneous network. The works [3] and [4] use a heterogeneous network scenario, but do not use the PMIPv6 to provide the mobility management.

V. Case Study

The architecture shown in Figure 1 is derived from standard 3GPP TS 23,402 [7] and illustrates a handoff between UMTS network and a WLAN 802.11 g. The 3G network has a core architecture of type System Architecture Evolution (SAE), being this architecture an evolution of GPRS. To provide the mobility management and session continuity, PMIPv6 and DSMIPv6 protocols are used.

In this scenario the PDN Gateway shall exercise the function of LMA or HA when PMIPv6 protocol or DSMIPv6, respectively, are used.

The message flow with the use of handoff protocols PMIPv6 and DSMIPv6 is presented in Chapter 6 of the standard 3GPP TS 23,402 [7].

Mobile authentication in WLAN network is done through the EAP-AKA [8], which is based on symmetric key encryption, using the challenge-response paradigm to authenticate the mobile. The architecture of EAP-AKA has a supplicant (being represented by the mobile terminal, using the keys and algorithms of USIM card), an authenticator in 3GPP network and an EAP remote server, implementing AAA and able to request authentication vectors HSS (Home Subscriber Services) database.

The WLAN network is assumed to be reliable, i.e., it is managed by the operated 3G, therefore, it is assumed a prior security association between the elements of the UMTS and WLAN networks.

For the case in which the DSMIPv6 is being used, in addition to mobile authentication to the WLAN, occurs a security association between the mobile and the PDN Gateway (represented by HA) through the IKEv2 protocol, described in [8]. This procedure has the purpose of creating a more secure environment for the exchange of information, with the negotiation of protocols and algorithms that will be used between the partners for the creation of secure means.

For the case in which the PMIPv6 is used, a previous security association between MAG and LMA (PSN Gateway) is presumed.

In the target architecture, the policy and charging control (PCC) is realized in static mode and provided by AAA infrastructure of the WLAN network, as specified in Section 4.10.4 standard 3GPP TS. 402 [7].

VI. Analytical Modeling

Considering that the handoff involves procedures related to authentication of the mobile terminal, this article evaluates authentication latencyinavertical handoff.

The latency related to authentication is due to message exchanges of EAP-AKA and also to message exchanges concerning the Security Association in the case of DSMIPv6.

For the analysis of authentication latency, theclassical theory ofqueues will be taken as a basis. The Figure 2 illustrates the model for terminal-network and network-terminal directions to the PMIPv6 and DSMIPv6.

Considering each element as represented by a M/M/1 queue, the delay of processing for each element can be described by:

$$D_{element} = \frac{a}{\mu_{t\_n} + \lambda_{t\_n}} + \frac{b}{\mu_{n\_t} + \lambda_{n\_t}} \quad (1)$$

Where $\mu_{t_n}$is the average rate for a given element processing towards terminal-network; μ_{n_t} is the average rate for a given element processing towards network-terminal; λ_{t_n} is the average rate of arrivals to a particular element in the terminal-network sense; λ_{n_t} is the average rate of arrivals to a particular element in the network-terminal sense; *a* and *b* indicate the number of

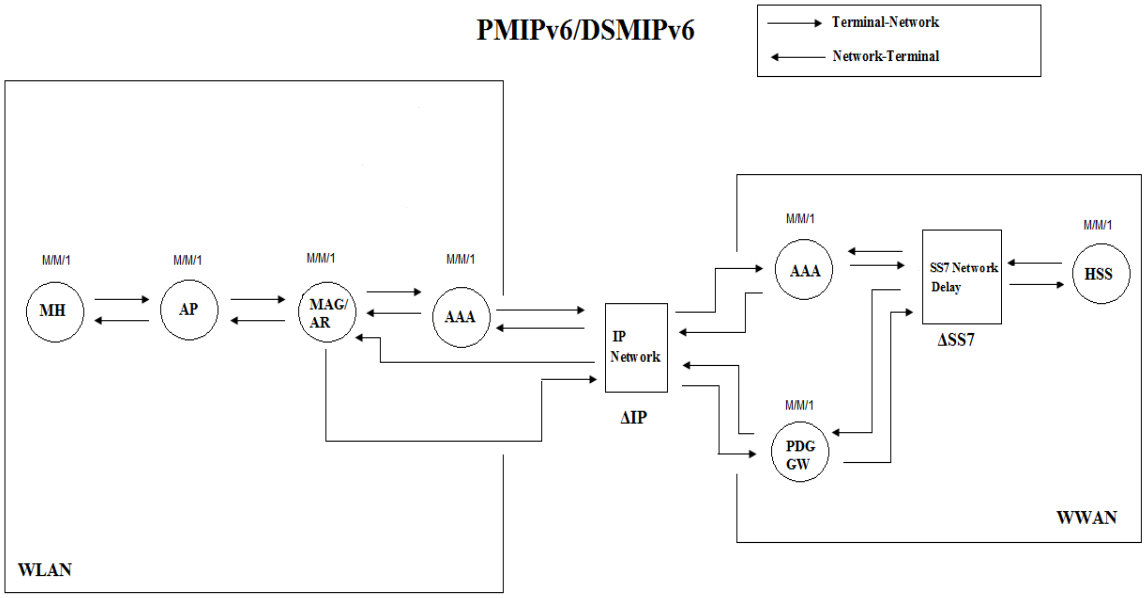

Fig. 2. Queueing model for analysis of delay in network-terminal and terminal-network ways for PMIPv6 and DSMIPv6 (Based on [3]).

messages exchanged in the terminal-network and network-terminal ways respectively.

The expression for the delay of WLAN interface delay model was obtained on the basis of an analytical modeling from [5] and is given by:

$$D' = D[1 - q^{Nm}] + 2RTO_0(1-q)[\frac{(1-q^{Nm}2^{Nm})}{(1-2q)} - \frac{1-q^{Nm}}{1-q}] \quad (2)$$

Where D is the end-to-end propagation delay; RTO_0 is the initial timer relay for every erroneouspackage; q is the frame error rate; and N_m is the maximum number of retransmissions for a particular protocol.

Following Burke's theorem, the total delay of each queue network, in an open system, can be calculated as the sum of the individual delays for each node. Thus, the expression of PMIPv6 authentication latency is given by:

$$D_{AUT} = D_{MH} + D_{EAP} + D_{AP} + D_{MAG/AR} + D_{AAA\_WLAN} + D_{AAA\_WWAN} + D_{HSS} + z \times \Delta IP \quad (3)$$

Where z is a positive integer and indicates the number of messages exchanged between the WLAN and WWAN; the delays D_{MH}, D_{AP}, $D_{MAG/AR}$, D_{AAA_WLAN} and D_{AAA_WWAN} are given by equation (1); the D_{EAP} delay refers to exchange of EAP messages via WLAN interface and is given by the equation (2); the ΔIP delay is relative to the IP network;

The delay on a query to the HSS (D_{HSS}) is given by:

$$D_{HSS} = \Delta HSS + 2\Delta SS7 \quad (4)$$

Thus, DSMIPv6 authentication latency is given by:

$$D_{AUT} = D_{MH} + D_{IKE} + D_{EAP} + D_{AP} + D_{MAG/AR} + D_{LMA/HA} + D_{AAA\_WLAN} + D_{AAA\_WWAN} + D_{HSS} + j \times \Delta IP \quad (5)$$

Where j is an integer and positive and indicates the number of messages exchanged between the WLAN and WWAN; the delays D_{MH}, D_{AP}, D_{AAA_WLAN}, D_{AAA_WWAN}, $D_{MAG/AR}$ and $D_{LMA/HA}$ are given by equation (1); D_{EAP} and D_{IKE} delays are related to message flow of EAP and IKEv2, respectively, through the WLAN interface and are given by equation (2).

The authentication process and the mobiles ecurity association involves two queries to the HSS (a query fort he acquisition of authentication and other one involving the obtention of the profile of mobile terminal).When using the PMIPv6 protocol, two queries to the HSS arenecessary, whereas in DSMIPv6 four queries to HSS are required considering two queries on mobile authentication process with the EAP-AKA and two more queries with the mobile security association withthe PDN Gateway.

Table I illustrates the numeric values of the average rates of arrivals and the average rates of processing in terminal- network and network-terminal directions, considering the elements of Figure 2:

TABLE I. NUMERIC VALUES OF ARRIVALS AND PROCESSING RATES

Terminal-network parameter	802.11 g	Network-terminal parameter	802.11 g	Reference
μ_{MH}	14,42 Mbps	$\mu_{MH'}$	100 Mbps	[3]
μ_{AP}	94,34 Mbps	$\mu_{AP'}$	14,42 Mbps	[3]
$\mu_{MAG/AR}$	5000 packages /s	$\mu_{MAG/AR'}$	5000 packages/s	[6]
$\mu_{LMA/HA}$	2000 packages/s	$\mu_{LMA/HÁ'}$	2000 packages/s	[6]
μ_{AAA_WLAN}	160,14 packages/s	$\mu_{AAA'\_WLAN}$	79,761 packages/s	[3]
μ_{AAA_WWAN}	160,14 packages/s	$\mu_{AAA'\_WWAN}$	160,14 packages/s	[3]
λ_{MH}	15,22 Kbps	$\lambda_{MH'}$	14,42 Mbps	[3]
λ_{AP}	100 Kbps	$\lambda_{AP'}$	100 Kbps	[3]
$\lambda_{MAG/AR}$	200 packages/s	$\lambda_{MAG/AR'}$	200 packages/s	Estimated
$\lambda_{LMA/HA}$	200 packages/s	$\lambda_{LMA/HÁ'}$	200 packages/s	Estimated
λ_{AAA_WLAN}	124,27 packages/s	$\lambda_{AAA'\_WLAN}$	43,89 packages/s	[3]
λ_{AAA_WWAN}	124,27 packages/s	$\lambda_{AAA'\_WWAN}$	43,89 packages/s	[3]

Table II presents the numeric value of the delays on IP networks (ΔIP) and SS7 (ΔSS7) and the delay for the HSS (ΔHSS).

TABLE II. NUMERIC VALUES USED IN DATA ANALYSIS

Parameter	802.11 g	Reference
ΔSS7	37,07 ms	[3]
ΔHSS	66.20 ms	[3]
ΔIP	20 ms	Estimated

ANALYSIS OF AUTHENTICATION LATENCY

In this section we will evaluate the behavior of authentication latency as a function of FER in a vertical handoff between UMTS and WLAN 802.11 g networks, using PMIPv6 and DSMIPv6 protocols to provide mobility management and session continuity.

Figure 3 illustrates the authentication latency in a WLAN based on IEEE 802.11 g (54 Mbps) varying the frame error rate up to a maximum value of 0.1, and considering queue in effect in the network elements. It may be noted that the reis an increase in authentication latency with the increase of FER; this was expected, due to the PMIPv6 and DSMIPv6 exchange messages through the WLAN interface.

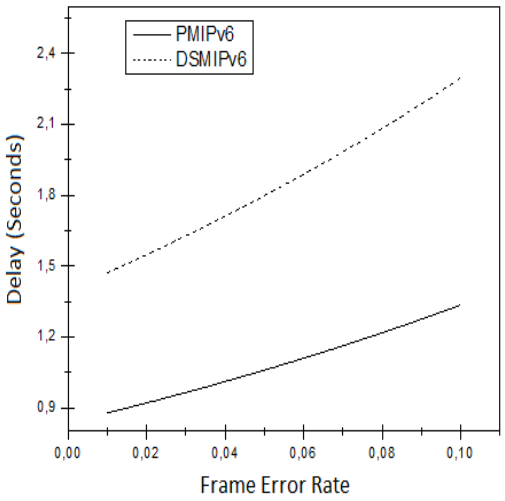

Fig. 3. Authentication delay vs frame Error rate (FER)

The DSMIPv6 is the most affected protocol, because it returns agreater number of messages via the WLAN interface, 18 messages in total. On the other hand, in the PMIPv6 Exchange the reare almost half of messages over WLAN interface when compared to DSMIPv6.

We can also observe in Figure 3, that the delay of DSMIPv6 authentication is much greater than that of PMIPv6, this is due to the fact that in addition to the mobile authentication DSMIPv6 inWLAN, done by EAP, it is necessary the security association between the mobile and the PDNGW, while inPMIPv6 it is done only on mobile authentication to the WLAN. The process for the realization of the Security Association is so onerous that this corresponds to approximately 40% of the total time for mobile authentication on DSMIPv6 and, the other 60% are referring to delay mobile authentication to the WLAN, done by EAP-AKA.

VII. CONCLUSIONS

This paper evaluated the authentication latency in a vertical handoff between UMTS and WLAN networks using PMIPv6 and DSMIPv6 protocols to provide mobility management and session continuity.

On the evaluation of authentication delays, PMIPv6 protocol presented a better performance when compared to DSMIPv6. This is mainly due to the utilization of agreater numberof ExchangeDSMIPv6messages, when compared to PMIPv6. Moreover, PMIPv6 is less affected by frame errors.

REFERENCES

[1] Ki-Sik Kong, Youn-Hee Han, Myung-Ki Shin, HeungRyeol Yoo, and Wonjun Lee, "Mobility

Management for All-IP Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6," IEEE Wireless Communications (Special Issue on Architectures and Protocols for Mobility Management in All-IP Mobile Networks), Vol.15, No.2, pp.36-45, April 2008.

[2] L. Tie, D. He, J. Li, and J.H. Tang, "Performance Analysis of Authentication Method for Proxy Mobile IP Protocol", in Proc. BMEI, 2009, pp.1-4.

[3] RIBEIRO JR, Sebastião Boanerges. Proposalofauthenticationmodelfor interconnection of heterogeneous wireless networks.2011. 227 p. Dissertation(Master's degreeinElectricalEngineering)– Universidade deBrasília,Brasília,2011. [Advisor:PauloR.L. Gondim].

[4] Abdul-Aziz Al-Helali, Ashraf Mahmoud, Talal Al-Kharobi, Tarek Sheltami, "Analysis of *Handoff* Delay Components for Mobile IP-Based 3GPP UMTS/WLAN Interworking Architecture," waina, pp.798-803, 2009 International Conference on Advanced Information Networking and Applications Workshops, 2009;

[5] S. K. Das, E. Lee, K. Basu, S.K. Sen, "Performance optimization of VoIP calls over wireless links using H.323 protocol", IEEE Transactions on Computers 52 (6) (2003) pp. 742–752, Junho 2003.

[6] A. Diab, A. Mitschele-Thiel, K. Getov, and O. Blume, "Analysis of proxy MIPv6 performance compared to fast MIPv6," in IEEE Conference on Local Computer Networks (LCN), Oct. 2008, pp. 579–580.

[7] 3GPP TS 23.402 V11.0.0 (2011-09): "Architecture enhancements for non-3GPP accesses".

[8] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

COMPARING AUTHENTICATION PROTOCOLS FOR HETEROGENEOUS WIRELESS NETWORKS

José B. M. Trineto, Paulo R. L. Gondim

Electrical Engineering Department - Faculty of Technology - Universidade de Brasilia

jbenicio@unb.br, pgondim@unb.br

Abstract: **Nowadays, there are several technologies of wireless networks such as GSM, HSPA, LTE, WIMAX and WLAN, among others, and a major trend in the telecommunications world is the interconnection of these networks, aiming to provide better coverage and other services to mobile users. For such interconnection, it is of crucial importance to consider authentication protocols able to provide security without compromising session continuity and consuming small bandwidth. This article, considering LTE and WLAN networks, describes and compares the impact of the use of authentication protocols for heterogeneous networks, considering their characteristics, the number of generated messages and the respective security properties.**

Keywords—Heterogeneous Network, Authentication, Vertical Handover.

1. INTRODUCTION

A major trend in the telecommunications world is the interconnection of wireless networks, based on a set of standards and technologies. Some examples are HSPA and LTE networks (standardized by 3GPP), WiMAX (standardized as IEEE 802.16) and WLAN (standardized as IEEE 802.11). These networks offer different coverage and capabilities, sometimes use different portions of electromagnetic spectrum and obey specific medium access control.

The convergence movement involving these heterogeneous networks aims to create and provide a unique intelligent infrastructure. Several aspects need to be tretaed for the creation of this infrastrucuture, in special those related to the consequences of the mobility of people and their terminals.

Moreover, with the recent evolution of the wireless communication networks, the demand for new services has been grown exponentially. Among these services, the real time multimedia communications impose requirements that are difficult to be met. In special, QoS (*Quality of Service*) and QoE (*Quality of Experience*) are aspects that need to be adequately treated.

The adequate provisioning of QoS and QoE levels in heterogeneous networks depends on efficient authentication mechanisms, considering that the authentication process in a vertical *handover* can lead to a great number of messages, thus reflecting on the *handover* latency and bandwidth consumption and influencing the flow of data and the continuity of sessions between terminals.

EAP-AKA is the protocol adopted by 3GPP for the interconnection of heterogeneous networks. It is based on symmetric key cryptography and uses the challenge-response paradigm for authenticating the mobile terminal. However, in this protocol the great number of messages between the network elements makes it inneficient for certain applications.

This paper aims to describe and compare authentication protocols, in a context of vertical *handover* involving LTE and WLAN networks. It is organized as follows: Section 2 describes the System Architecture Evolution, as proposed and adopted by 3GPP; Section 3 presents a set of methods for authentication in heterogeneous wireless networks; in Section 4, a comparison between the mentioned methods is made; Section 5 contains the conclusions and outlines some future work.

2. System Architecture Evolution (SAE)

In this section we give a brief description of the architecture SAE (System Architecture Evolution) architecture, which enables the integration of networks of different wireless standards, and is used as a basis for various authentication methods.

SAE, as defined by 3GPP in Release 8, is a core network designed to have a simplified architecture, ie, with few elements, optimization of network performance, support for multiple types of wireless networks such as LTE, WLAN, UMTS, and mobility support across heterogeneous access networks.

In this architecture we have the following elements:

- PDN Gateway (P-GW): Provides mobile connectivity to any external data network. Has an important role in the use of mobility management in IP networks.

- Serving Gateway (S-GW): Routes and forwards the packets and also acts as a mobility

manager during the handoff between LTE networks or between network LTE and other 3GPP.

- Mobility Management Entity (MME): This element has functions for managing user profile, connection and service authorization, interception of signaling traffic, transfer of control messages among other functions.,- Home Subscriber Server (HSS): A database that contains information relating to subscribers and users of the network.

- AAA Server: responsible for the functions of authentication, authorization and accounting server.

3. AUTHENTICATION METHODS

In this section, we present a set of proposals recently published for the the sake of authenticating (or re- authenticating or pre-authenticating) mobile terminals in heterogeneous networks.

3.1 UNAEN Method

In [1], it is proposed a technique for fast and secure authentication for handoffs between LTE and non-3GPP networks (WLAN, WiMax, CDMA 2000, etc.). The SAE architecture (System Architecture Evolution) was used with the access networks 3GPP and non-UTRAN connected by the same core architecture of the EPC (Evolved Packat Core). The proposed scheme, named UNAEN, consists on two phases, a pre-authentication of the mobile call "preparatory phase handoff" and another consisting of authentication for mobile during the handoff call "authentication phase handoff".

The "preparatory phase handoff" aims to make the preparation for future handoff authentication. In this step the first Access Points (APs) and mobile devices (ME) receive a distribution center keys (KCG) function provided by the HSS, their private keys, and only authenticated APs and mobile devices can receive private keys KCG. This phase is subdivided into two other phases, initialization and key distribution. In the sub-step boot KCG generating the data security of the system and the master key. The sub-phase for key distribution will only be done the first time that the AP and ME register themselves on the network or your private key expires. For the acquisitionof the private key, each mobile/AP sends a message containing its ID to KCG via AAA server using the pre secret key negotiated between the elements.

The "authentication phase handoff" process consists of mutual authentication between the mobile and the target AP based on a challenge response method, consisting in the replacement of only four messages between the mobile network and the target AP.

The proposed scheme can be applied to all types of mobility scenarios between LTE networks and networks that are not standard 3GPPP considering that networks are not 3GPP can be trusted and untrusted type.

Some types of services such as video streams over the Internet and VoIP (Voice over IP), have certain acceptable levels of QoS for services work with a good quality to the user. In particular, to achieve these levels of QoS, latency handoff should be as small as possible and the advantage of this authentication method is that there is little exchange of authentication messages to the handoff process, thereby reducing latency authentication. However, the main disadvantage is that all APs and mobile devices connected to a network that is part of the SAE architecture must perform at least once the pre-authentication with key distribution center, may occurring the overloading of the server.

3.2 EAP-FAKA Method

In [2], a method of authentication in a LTE - WLAN handoff has been proposed, called EAP-FAKA. The method simplifies the authentication process, reduces the authentication delay and offers a flexible method to reauthenticate the terminal. It is based on EAP-AKA and makes use of the combination of symmetric and asymmetric key systems.

In this approach the authors use an integration architecture of LTE and SAE WLAN networks with a EPC core network.

For this protocol some assumptions were made:

- A secure channel between the elements Access Point (AP) of WLAN (WAAA) AAA server, AAA server of the home network (HAAA) and HSS;
- A WAAA is responsible for multiple APs;
- The mobile device (UE) can identify the ID AAA and AP;
- All HAAA has a known public key;
- Each UE has a pair of pre-shared secret key with the HSS server.

The operation of the protocol is described by the message flow shown in Figure 1.

Upon detection of the UE by the network, the AP requests the mobile its handle and passes them to the HSS via the AAA servers for obtaining authentication vectors, which will be used to process authentication challenge-response. After receiving the authentication vectors, the WAAA sends a challenge message to the AP to be transferred to the mobile device. The UE on receiving the challenge message verifies it with your security settings. If the verification is

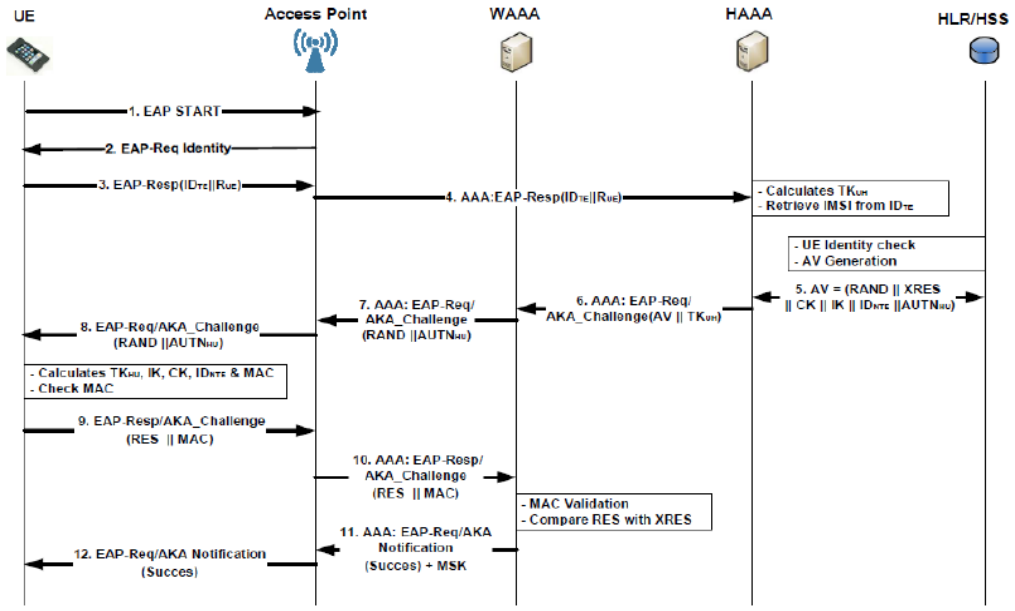

Fig. 3. Message Flow - EAP-FAKA ([2])

successful, the mobile sends the challenge response to WAAA. Possession of the challenge response message, WAAA will do the validation of this message and if this is successful a message to the mobile notifying that the authentication was successful sends.

The main advantage of this protocol is the use of the WLAN AAA server (WAAA) to authenticate the mobile, unlikely EAP-AKA using the HAAA for this procedure. With this four messages are exchanged in comparison to less EAP-AKA, so that there is a reduction in the handoff latency and a decrease in bandwidth consumption.

However, this protocol by not presenting a pre-authentication-based approach still has a high number of messages exchanged during handoff compared to [1]. Another disadvantage of this method is the fact that this is limited to use in WLAN or those with architecture similar to WLAN, unlike EAP-AKA that enables its use for any type of networks other than 3GPP networks.

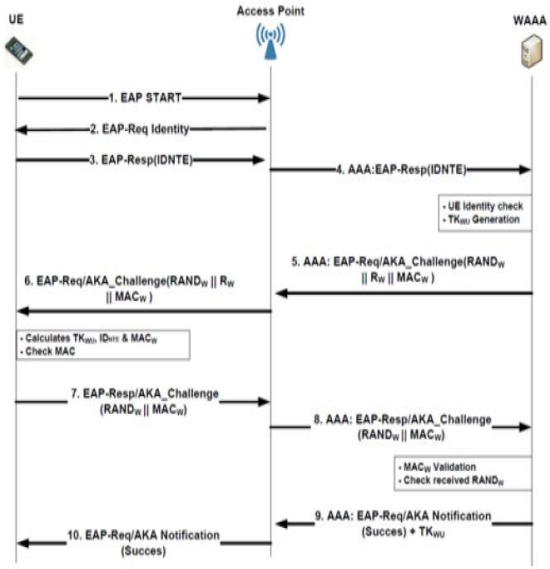

Fig. 4. EAP -FLAKA re-authentication protocol ([3])

3.3 EAP-FLAKA Method

EAP-FLAKA described in [3], is a method of re-authentication based on EAP-AKA, used in cases where the mobile reassociate itself with a single AP or a new AP on the same area of the WLAN. The same assumptions and architectural aspects for EAP-FAKA [2] were considered in its the proposal.

In this method, WAAA authenticates the mobile on behalf of HAAA using the key previously received on the full authentication protocol EAP-FAKA.

The operation of the protocol is described by the message flow shown in Figure 2:

In the fast re-authentication scheme, after detection of a mobile, WLAN network requests the identification of the first mobile ID that has been previously delivered to the mobile node authentication process overall EAP-FAKA. After that are made the procedures of re-authentication mobile using keys derived from the previous full authentication. The procedure for challenge-response authentication is performed and if this is successful, the AAA server sends a WLAN network (REQ-EAP / AKA-Notification) message notification to mobile stating that authentication was successful.

The use of EAP-FLAKA brings lower latency handoff, due to lower messaging and no need to do any type of query to the HSS, because the process of generation of authentication vectors by HSS is quite costly. But the use of EAP-FLAKA is restricted to cases of users who return frequently to the same WLAN.

3.4 EAP-LUTLS Method

Was proposed in [4] an authentication protocol, called EAP-LUTLS for heterogeneous networks without wire, where the architecture consisted of interconnecting a WLAN to a cellular network.

In this protocol is assumed a pre sharing a secret key between the HSS and mobile cellular network. The proposed scheme utilizes certificates between the elements for the mutual authentication and authenticating the mobile entity.

Next, the flow of protocol messages is displayed. In this scheme we have that W-AS, is the authentication server of the WLAN network, represented by WAAA, and C-AS is the authentication server over the cellular network represented by the AAA server and the HSS.

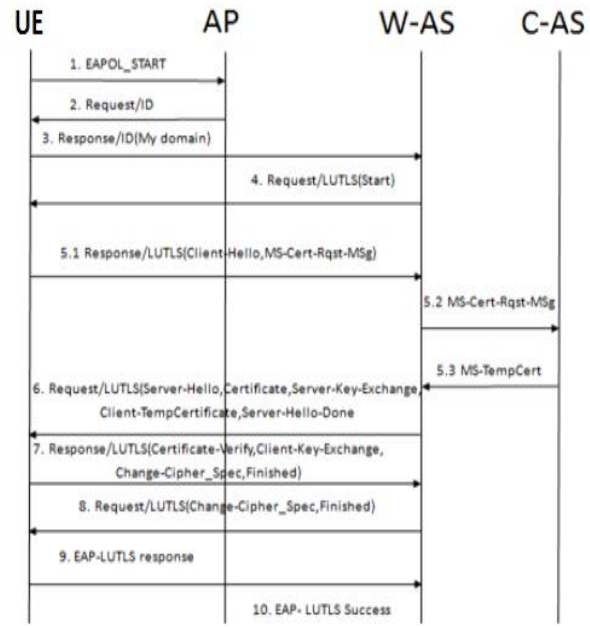

Fig. 5. Message Flow for EAP-LUTLS Protocol ([4])

In EAP-LUTLS, after the detection of the WLAN mobile network, the mobile authentication process is performed. Then the AP requests the ID of the mobile and this sends a Temporary Identifier (TID) to be replaced by your actual ID, thus ensuring privacy protection EU. After these steps the W-AS requests the certificate from the EU, and this sends a few parameters with encrypted pre-shared key with the AS-C. Upon receiving the message, the W-AS passes to the C-AS and this gives the certificate. If this certificate is valid, means that the EU is legitimate. Finally, the W-AS sends its certificate to the EU, and this certificate is validated by mobile, the authentication procedure is successful.

The use of EAP-LUTLS, besides reducing handoff latency because it uses the WAAA as authenticating entity, as well as in EAP-FAKA also provides security to impersonation attacks due to the use of pre-shared key with HSS has mutual authentication between the EU and WAAA and ensuring user privacy with the use of a temporary ID.

Moreover, EAP-LUTLS has some problems such as the increase of the handoff latency compared to protocols that use pre-authentication schemes and there is still a pre-shared secret key between the mobile device and the HSS cellular network.

3.5 Authentication Method by Hassanein et al. [6]

In this work the authors proposed a protocol for authentication in heterogeneous networks, aiming at improving EAP-AKA.

The SAE architecture was used in a LTE-WLAN handoff, but in this case not used a AAA server over the cellular network, with the assumption a secure channel established between the WLAN network AAA and HSS cellular network.

The Figure4 illustrates the message flow of the proposed protocol. After the UE to detect the target network, the AP requests some information from EU and sends its ID encrypted with a temporary key (KTEMP) which was derived from a pre-shared key with the HSS, Timestamp, the AP ID and the ID HSS. The HSS in possession of the data generates parameters that will be used for mutual authentication between the mobile and WAAA. Soon after, WAAA sends a message containing an authentication code (MACWAAA) and MACHSS with encrypted KTEMP. Are also sent parameters that will be used to generate the secret key shared between the EU and WAAA (KUE-WAAA) by exchanging keys Elliptic Curve Diffie Hellman (ECDH). Possession of message authentication codes, the UE is able to authenticate the HSS and WAAA and generates a message authentication code (MACUE) using KUE-WAAA and sends it to WAAA. Upon receiving the MACUE the WAAA be able to authenticate the mobile device. If authentication of the EU by the WAAA succeeds, it sends a message to the mobile notifying you that the authentication was successful.

This protocol introduces improvements compared to EAP-AKA as the protection of EU ID, mutual authentication between entities and the reduction of authentication latency with fewer messages.

Despite a decrease in the latency of authentication, with the removal of the HAAA in the authentication process, the method requires a small change in the SAE architecture, with the direct link between the HSS and WAAA, a change that may not be feasible in commercial mobile networks.

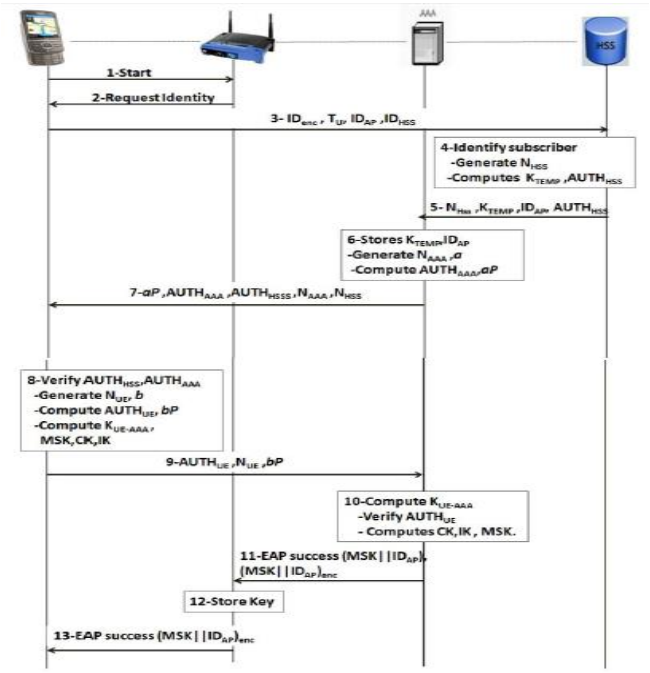

Fig. 6. Message Flow in Hassanein [6]

4. COMPARING AUTHENTICATION METHODS

In this section we will compare the authentication methods described in [1] - [4] in relation to exchange messages during the handoff between WLAN and cellular network. Was not included in the proposed [5] method because its architecture differs from the others (with the inclusion of the element HIU) and due to the fact that the EAP method has not been specified by the authors.

Table 1 shows the number of messages exchanged between each element during the handoff procedure for authentication methods [1] - [4]:

TABLE 1 EXCHANGE OF MESSAGES IN AUTHENTICATION METHODS

Method	UE-AP	AP-WAAA	WAAA-HAAA	HAAA-HSS	WAAA-HSS
UNAEN	3 msgs	-	-	-	-
EAP-FAKA	6 msgs	4 msgs	2 msgs	2 msgs	-
EAP-FLAKA	6 msgs	4 msgs	-	-	-
EAP-LUTLS	9 msgs	7 msgs	2 msgs	2 msgs	-
Hassanein [6]	6 msgs	4 msgs	2 msgs	-	2 msgs

From table 1 it follows that the method that has the least number of messages exchanged among the elements, and therefore has the lowest authentication latency during handoff is the UNAEN, due to the fact this method perform the pre-authentication procedure before completion of the handoff.

Additional work has been done for the sake of enlarging the comparison here initiated, involving management (including distribution) of cryptographic keys, energy consumption and security properties (e.g. protection against man-in-the-middle replay attacks). Moreover, the influence of security and mobility management functions in the latency as well as in the quality of experience related to the use of multimedia applications (e.g. VoIP, videoconference,) in a context of vertical *handover* represents an important issue to be considered, where the several options for authentication protocols as well as some options for mobility management protocols (for example, DSMIP and PMIP) must be jointly considered.

5. CONCLUSION AND FUTURE WORK

This article described and compared recent proposals for authentication during vertical handoff LTE-WLAN, considering a core architecture based on SAE.

The advantages and disadvantages of each authentication technique were discussed, considering easiness of imlementation and number of messages.

Ongoing work includes the utilization of analytical models and discrete event simulation for comparing *handover* latency among the presented methods, as well as other methods, such as the methods presented in [7] and [8]. Moreover, a study related to the influence of mobility management and authentication protocols in the QoS as well as in the quality of experience related to multimedia applications has been conducted.

REFERENCES

[9] Jin Cao; Maode Ma; Hui Li, "An Uniform *Handover* Authentication between E-UTRAN and Non-3GPP Access Networks," Wireless Communications, IEEE Transactions on , vol.11, no.10, pp.3644,3650, October 2012.

[10] Idrissi, Y.E.H.E.; Zahid, N.; Jedra, M., "Security analysis of 3GPP (LTE) — WLAN interworking and a new local authentication method based on EAP-AKA," Future Generation Communication Technology

(FGCT), 2012 International Conference on , vol., no., pp.137,142, 12-14 Dec. 2012.

[11] El Hajjaji El Idrissi, Younes; Zahid, Noureddine; Jedra, Mohamed, "A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA," Telecommunications (ICT), 2013 20th International Conference on , vol., no., pp.1,5, 6-8 May 2013 [4] – A universal lightweight authentication scheme based on delegation mechanism in heterogeneous network.

[12] Chou-Chen Yang; Shin-Hao Lo; Lu, E.J., "A Universal Lightweight Authentication Scheme Based on Delegation Mechanism in Heterogeneous Networks," Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on , vol., no., pp.963,966, 4-7 Sept. 2012.

[13] Bouabidi, I.E.; Daly, I.; Zarai, F., "Secure handoff protocol in 3GPP LTE networks," Communications and Networking (ComNet), 2012 Third International Conference on , vol., no., pp.1,6, March 29 2012-April 1 2012.

[14] Hassanein, Ahmed H., et al. "New Authentication and Key Agreement Protocol for LTE-WLAN Interworking." International Journal of Computer Applications 61.19 (2013): 20-24.

[15] Sithirasenan, E.; Kumar, S.; Ramezani, K.; Muthukkumarasamy, V., "An EAP Framework for Unified Authentication in Wireless Networks," Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on , vol., no., pp.389,397, 16-18 Nov. 2011.

[16] Sithirasenan, E.; Ramezani, K.; Muthukkumarasamy, V., "Enhanced CRA protocol for seamless connectivity in wireless networks," Communications and Information Technologies (ISCIT), 2012 International Symposium on , vol., no., pp.1075,1079, 2-5 Oct. 2012.

[17] S. K. Das, E. Lee, K. Basu, S.K. Sen, “Performance optimization of VoIP calls over wireless links using H.323 protocol”, IEEE Transactions on Computers 52 (6) (2003) pp. 742–752, Junho 2003.

[18] Ribeiro Jr, Sebastião Boanerges. Proposal of authentication model for interconnection of heterogeneous wireless networks.2011. 227 p. Dissertation (Master’s degree in Electrical Engineering)– Universidade de Brasília,Brasília,2011. [Advisor:PauloR.L. Gondim].

[19] Gondim, P. R., & Trineto, J. (2012, December). DSMIP and PMIP for mobility management of heterogeneous access networks: Evaluation of authentication delay. In Globecom Workshops (GC Wkshps), 2012 IEEE (pp. 308-313). IEEE.

[20] 3GPP TS 33.402 V12.4.0 (2014-10): "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[21] 3GPP TS 23.402 V12.6.0 (2014-09): “Architecture enhancements for non-3GPP accesses”.