UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE COMPUTAÇÃO
MESTRADO EM CIÊNCIA DA COMPUTAÇÃO

WILLIAM DE ARAUJO SALES

UMA ENTIDADE FUNCIONAL PARA AUTENTICAÇÃO DE DISPOSITIVOS MÓVEIS ENTRE ÁREAS DE MICROMOBILIDADE

FORTALEZA
2004

WILLIAM DE ARAUJO SALES

UMA ENTIDADE FUNCIONAL PARA AUTENTICAÇÃO DE DISPOSITIVOS MÓVEIS ENTRE ÁREAS DE MICROMOBILIDADE

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Orientadora: Profa. Dra. Rossana Maria de Castro Andrade

FORTALEZA
2004

WILLIAM DE ARAUJO SALES

UMA ENTIDADE FUNCIONAL PARA AUTENTICAÇÃO DE DISPOSITIVOS MÓVEIS ENTRE ÁREAS DE MICROMOBILIDADE

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Aprovada em ___/___/_____

BANCA EXAMINADORA

_____

Profa. Dra. Rossana Maria de Castro Andrade (Orientadora)
Universidade Federal do Ceará - UFC

_____

Prof. Dr. José Neuman de Souza
Universidade Federal do Ceará - UFC

_____

Profa. Dra. Judith Kelner
Universidade Federal de Pernambuco-UFPE

_____

Prof. Dr. Francisco Rodrigo Cavalcante
Universidade Federal do Ceará-UFC

Aos meus pais, Ciro e Eliza.

AGRADECIMENTOS

É difícil listar todos que colaboraram direta ou indiretamente com esse trabalho. No entanto, agradeço em particular, o esforço, dedicação e atenção das seguintes pessoas e instituições:

- À Deus, por permitir que eu suba mais um degrau rumo a satisfação profissional e pessoal.
- Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ) e ao Instituto Atlântico, pelo incentivo financeiro.
- À minha orientadora, professora Rossana Andrade, pela sua grande ajuda e compreensão.
- Aos professores e funcionários do Mestrado em Ciência da Computação da Universidade Federal do Ceará, em especial ao professor José Neuman de Souza.
- À minha querida namorada, companheira e cúmplice, Roberta, pelo apoio imprescindível.
- Aos meus queridos pais, Ciro Sales e Eliza Maria, pelo carinho e atenção.
- Aos meus amigos, Paulo Henrique e Bringel Filho pela ajuda na revisão dos textos.
- A todos os amigos da turma de Mestrado que propiciaram momentos alegres para compensar os momentos difíceis dessa empreitada acadêmica.
- A todos os integrantes do Grupo de Redes, Engenharia de Software e Telecomunicações (GREaT) do Departamento de Computação da UFC, em especial à secretária do GREaT, Suzana Rodrigues.

RESUMO

A Internet Móvel tem possibilitado a transferência de informações de forma ininterrupta através de dispositivos móveis (MN – *Mobile Node*), permitindo a um usuário manter uma comunicação ativa enquanto muda de rede de acesso. *Mobile IP* (MIP) é um protocolo desenvolvido pela *Internet Engineering Task Force* para permitir mobilidade global entre redes IP. No entanto, MIP não oferece suporte transparente à mobilidade, o que implica em longos períodos de espera no processo de registro de atualização. Com a intenção de possibilitar *handoffs* mais rápidos e suaves, foram idealizados protocolos de mobilidade adequados para áreas geográficas restritas (domínio administrativo), denominados protocolos de micromobilidade. Entretanto, o protocolo utilizado pelos dispositivos móveis ao mudarem de domínio administrativo continua sendo o MIP. A adição de uma entidade funcional (denominada de EGM – Entidade Gerenciadora de Mobilidade) ao MIP para regionalizar as atualizações de registro entre domínios de micromobilidade foi então proposta para solucionar esse problema. Porém, essa proposta não inclui um processo para autenticar os dispositivos móveis de forma eficiente, o que acarreta em altos atrasos para verificar a autenticidade de um MN. Para minimizar esse atraso, esta dissertação propõe a adição de uma nova entidade funcional à estrutura do *Mobile IP*, denominada de Agente de Segurança (AS), cuja função é permitir ao MN realizar a autenticação em um domínio administrativo sem a necessidade de acessar seu agente de mobilidade domiciliar. A proposta utiliza diagramas de seqüência para descrever os cenários de autenticação existentes e a lógica BAN para especificar e validar formalmente a proposta. O *Network Simulator* é utilizado para verificar a eficiência da proposta e obter parâmetros de comparação com a proposta original do *Mobile IP*.

Palavras-chave: Registro de Localização, Autenticação, *Mobile IP*, Especificação Formal de Protocolos, Lógica BAN.

ABSTRACT

Mobile Internet allows information transfer using mobile nodes (MN) without interruption, enabling a user to maintain an active communication while roaming to another access network. Mobile IP (MIP) is a protocol developed by *Internet Engineering Task Force* to permit global mobility between IP networks. However, MIP does not offer transparent mobility support and , for this reason, long delay periods happen in the location registration process. In order to allow soft and fast handoffs, mobility protocols for limited geographic areas (i.e., administrative domains) were proposed in the literature and called micromobility protocols. Since MIP was still used by the mobile nodes when changing to another administrative domain, the addition of a functional entity (called EGM – Entitity for mobility management) was proposed to reduce the location registration updates between micromobility domains. Nevertheless, this proposal does not include a process to authenticate a mobile node efficiently, then, high delays occur when verifying the authenticity of the MN. Thus, this work proposes the addition of a new functional entity, called Security Agent, to the structure of Mobile IP for minimizing this delay. This entity allows the mobile device to execute the authentication in a new administrative domain without the need of having access to its home agent. Sequence diagrams are used to show the authentication scenarios and logic BAN to formally specify the proposal. Network Simulator is used to verify the proposal efficiency and to obtain measurements in relation to the Mobile IP first proposal.

Palavras-chave: Location Registration, Authentication, Mobile IP, Protocol Formal Specification, BAN Logic.

LISTA DE FIGURAS

Figura 2.1 - Duas Redes de Acesso Conectadas Através da Internet 19
Figura 2.2 - Ambiente de Domínios Administrativos..... 20
Figura 2.3 - Componentes do *Mobile IP* Versão 4 22
Figura 2.4 - Roteamento e tunelamento no *Mobile IPv4* 25
Figura 2.5 - Tunelamento Reverso 26
Figura 2.6 - Arquitetura da proposta EGM..... 29
Figura 2.7 - Usuário registra os terminais de casa e do escritório 30
Figura 2.8 - Usuário B solicita comunicação com Usuário A via servidor Proxy..... 32
Figura 2.9 - Arquitetura de uma rede *Cellular IP*..... 34
Figura 2.10 - Roteamento no CIP 36
Figura 2.11 - Arquitetura do HAWAII 38
Figura 2.12 - Arquitetura da rede HMIP..... 40
Figura 3.1 Modo IP original 50
Figura 3.2 - Modo Transporte do IPSec 51
Figura 3.3 - Modo IP original 51
Figura 3.4 - Modo Túnel do IPSec 51
Figura 3.5 - Diferenças entre o teste de integridade do AH e do ESP..... 52
Figura 3.6 - Modelo geral do AAA..... 54
Figura 3.7 - Modelo geral do AAA aplicado ao *Mobile IP* 55
Figura 4.1 - Modelo de desenvolvimento formal em cascata (adaptado de [SOMMERVILLE 2000])..... 59
Figura 4.2 - Protocolo *Wide-mouthed-frog* (adaptada de [BAN 1990]) 64
Figura 5.1 - Arquitetura da rede MIP com Agente de Segurança..... 79
Figura 5.2 - Solicitação de autenticação de um MN ao mudar de domínio de segurança..... 80
Figura 5.3 - MN envia solicitação de autenticação/atualização de registro..... 93
Figura 5.4 - AS recebe solicitação de autenticação/atualização de registro e envia para o HA ... 94
Figura 5.5 - HA envia resposta à solicitação de autenticação/atualização de registro 95
Figura 5.6 - MN recebe resposta da solicitação de autenticação 95
Figura 5.7 - Solicitação de autenticação de um MN em um mesmo domínio de segurança 96
Figura 5.8 - MN envia solicitação de autenticação/atualização de registro interno 103
Figura 5.9 - AS recebe pacote de solicitação de autenticação/atualização de registro..... 104
Figura 5.10 - MN recebe resposta da solicitação de autenticação 104
Figura 5.11 - Topologia da rede *Mobile IP* utilizada na análise comparativa 105
Figura 5.12 - Topologia da proposta utilizada na análise comparativa 106
Figura 5.13 - Comparação entre o número de solicitações de autenticação entre 108

LISTA DE TABELAS

Tabela 4.1 - Notação da troca de mensagens 61
Tabela 4.2 - Notação da lógica BAN 61
Tabela 4.3 - Protocolo *Wide-Mouthed-Frog* 64
Tabela 4.4 - Mensagens do protocolo idealizado 65
Tabela 4.5 - Suposições iniciais do protocolo *Wide-mouthed-frog* 65
Tabela 4.6 - Primeira mensagem do protocolo idealizado 66
Tabela 4.7 - Segunda mensagem do protocolo idealizado 66
Tabela 5.1 - Suposições iniciais para o cenário em que o MN muda de domínio de segurança . 86
Tabela 5.2 - Suposições iniciais para o cenário em que o MN continua em um domínio de segurança 100
Tabela 5.3 - Tabela comparativa entre o número de *Handoffs* do MIP e AS 108
Tabela 5.4 - Tabela comparativa da perda de pacotes 109

LISTA DE ABREVIATURAS E SIGLAS

AA	Autoridade Administrativa
AAA	*Authentication, Authorization, and Accounting*
AAAH	AAA *Home*
AAAL	AAA *Local*
AH	*Authentication Header*
AS	Agente de Segurança
BU	*Binding Updates*
CCoA	*co-located care-of-address*
CIP	*Cellular IP*
CN	*Correspondent Node*
CoA	*care-of-address*
DA	Domínio Administrativo
DHCP	*Dynamic Host Configuration Protocol*
ESP	*Encapsulating Security Payload*
FA	*Foreign Agent*
FN	*Foreign Network*
GSM	*Global System Mobile*
GW	*Gateway*
HA	*Home Agent*
Hat	*Home attendent*
HAWAII	*Handoff Aware Wireless Access Internet Infrastructure*
HLR	*Home Location Register*
HMIP	*Hierarchical Mobile IP*
HN	*Home Network*
IETF	*Internet Engineering Task Force*
IPSec	*IP Security*
MIP	*Mobile IP*
MIPv4	*Mobile IP* versão *4*
MIPv6	*Mobile IP* versão 6

MN	*Mobile Node*
NS	*Network Simulator*
NAM	*Network Animator*
RI	Roteador Interno
SA	*Security Agent*
SIM	*Subscriber Identity Module*
SIP	*Session Initiation Protocol*
SPI	*Security Parameters Index*
SSL	*Security Socket Layer*
TIMIP	*Terminal Independent Mobility for IP*

SUMÁRIO

AGRADECIMENTOS v
RESUMO vi
ABSTRACT vii
LISTA DE FIGURAS viii
LISTA DE TABELAS ix
LISTA DE ABREVIATURAS E SIGLAS x
SUMÁRIO xii
CAPÍTULO 1 Introdução 14
1.1 Motivação 14
1.2 Objetivos e contribuições do trabalho 15
1.3 Estrutura da Dissertação 16
CAPÍTULO 2 Internet Móvel 18
2.1 Introdução 18
2.2 Gerenciamento de Mobilidade 20
2.3 Protocolos de Macromobilidade 21
2.3.1 *Mobile IP* versão 4 22
2.3.2 *Mobile IP* versão 6 27
2.3.3 EGM – elemento de rede para registro de localização 27
2.3.4 Session Initiation Protocol 29
2.4 Protocolos de Micromobilidade 32
2.4.1 Cellular IP 33
2.4.2 Handoff-Aware Wireless Access internet infrastrucuture 37
2.4.3 Hierarchical Mobile IP 40
2.5 Conclusão 41
CAPÍTULO 3 Segurança em Redes 42
3.1 Introdução 42
3.2 Segurança da Informação 43
3.2.1 Ataques 43
3.2.2 Serviços 43
3.2.3 Linguagens de Padrões - Tropyc e Morar 44
3.2.4 Norma técnica de segurança - IEEE 802.1x 45
3.3 Segurança no *Mobile IP* 46
3.3.1 Mobile-Foreign Authentication Extension 47
3.3.2 Mobile IP Challenge/Response Extensions 48
3.3.3 IP Security 49
3.3.4 Authentication, Authorization, and Accounting 53

3.3.5 Discussão 56
3.4 Conclusão 57
CAPÍTULO 4 Metodologia de Desenvolvimento 58
4.1 Introdução 58
4.2 Projeto com Especificação Formal 59
4.2.1 Lógica BAN 60
4.2.2 Validação do Protocolo *Wide-mouthed-frog* utilizando Lógica BAN 64
4.3 Simulação 67
4.3.1 Simuladores disponíveis 68
4.3.2 Network Simulator 69
4.4 Conclusão 74
CAPÍTULO 5 AS – Um Agente de Segurança para autenticação de dispositivos móveis.. 75
5.1 Introdução 75
5.2 Mecanismos de segurança utilizados 76
5.3 Definição de Requisitos 77
5.4 Projeto com Especificação Formal e Simulação 78
5.4.1 Arquitetura 78
5.4.2 Comportamento Funcional 79
5.5 Protocolo Proposto *versus* MIP 105
5.5.1 Ambiente de Simulação 105
5.5.2 Métricas 107
5.5.3 Resultados Obtidos 107
5.6 Conclusão 110
CAPÍTULO 6 Conclusão 111
6.1 Resultados Alcançados 111
6.2 Problemas Encontrados 112
6.3 Trabalhos Futuros 112
REFERÊNCIA BIBLIOGRÁFICA 114

CAPÍTULO 1 INTRODUÇÃO

1.1 MOTIVAÇÃO

A Internet Móvel tem possibilitado a transferência de informações de forma ininterrupta através de dispositivos móveis, permitindo a um usuário manter uma comunicação ativa enquanto muda de rede de acesso. *Mobile IP* (MIP) [PERKINS 2002] é um protocolo desenvolvido pela *Internet Engineering Task Force* [IETF 2003] para permitir mobilidade global entre redes IP. Ele foi idealizado para ambientes com usuários de baixa mobilidade, ou seja, baixo número de *handoffs* (mudança de ponto de acesso). Para ambientes de alta mobilidade, ele se apresenta ineficiente, devido à freqüente necessidade do dispositivo móvel realizar registro em seu *Home Agent* (HA) toda vez que mudar de *Foreign Network* (FN). Isso implica em longos atrasos no processo de registro e grande carga de sinalização na Internet, principalmente quando um *Mobile Node* (MN) estiver distante do seu HA.

Com a intenção de possibilitar *handoffs* rápidos e suaves, algo não possível através do *Mobile IP*, foram idealizados os protocolos de micromobilidade, que são soluções adequadas para áreas geográficas restritas, denominadas de Domínio Administrativo. Através desses protocolos, o processo de atualização de registro é realizado por uma entidade responsável pelo domínio administrativo, denominado de *gateway*, e não mais através do HA.

Apesar das vantagens dos protocolos de micromobilidade, o gerenciamento de mobilidade entre áreas de micromobilidade é realizado através do protocolo *Mobile IP*, que recai nos problemas já citados anteriormente. Para contornar esse problema, ALBANO [ALBANO 2004] [AACA 2003] propõe um protocolo que diminui a freqüência das trocas de mensagens para atualização da localização de um dispositivo móvel entre domínios administrativos através da adição de uma entidade denominada SGM.

No entanto, propostas que regionalizam o processo de atualização de registro também necessitam de mecanismos que minimizem o acesso ao HA para realizar a autenticação de um MN visitante. Vários métodos de segurança estão disponíveis para *Mobile IP*, tais como *Mobile-Foreign Authentication extension* [PERKINS 2002], *Mobile IP Challenge/Response Extensions*

[PERKINS 2000], *Authentication, Authorization, and Accounting* [BDHSK 2003] [CFV 2002] e *IP Security* [ATKINSON 1995/1] [ATKINSON 1995/2]. Entretanto, nenhuma dessas propostas apresenta características voltadas a diminuir o número de acessos ao HA para realizar autenticação de MNs, ou seja, para cada solicitação de autenticação, o MN acessa o HA.

1.2 OBJETIVOS E CONTRIBUIÇÕES DO TRABALHO

O objetivo desta dissertação é otimizar o processo de autenticação de um dispositivo móvel que se desloca entre domínios administrativos, através da diminuição do número de acessos ao *Home Agent* para realizar a autenticação do MN. Esse objetivo é alcançado através da adição de uma entidade funcional ao protocolo *Mobile IP*, denominada Agente de Segurança (AS). Para atingir o objetivo desta dissertação, adaptamos a metodologia em cascata da engenharia de software [SOMMERVILLE 2000] e utilizamos uma técnica de especificação formal e uma ferramenta de simulação [BAN 1990] [NS 2003].

A inovação da nossa proposta está, justamente, em minimizar o número de solicitações ao HA para realizar a autenticação de um MN visitante. Conseqüentemente, a junção da proposta de [ALBANO 2004] [AACA 2003] com a proposta desta dissertação, fornece um ambiente eficiente e seguro de gerência de localização de dispositivos móveis entre áreas de micromobilidade. A concepção inicial desta integração foi introduzida em [ASACS 2004], entretanto, não foi realizada nenhuma simulação ou especificação formal. No desenvolvimento da nossa proposta utilizamos algumas características dessa integração, tais como gerenciamento de mobilidade regional, no entanto, a integração total, abrangendo *paging* e conectividade passiva é considerada ainda como um trabalho futuro desta dissertação.

Como principal contribuição desta dissertação, um protocolo de autenticação é proposto para reduzir o número de acessos ao *Home Agent* para realizar a autenticação do MN, o que acarreta em *handoffs* mais rápidos e suaves entre domínios de micromobilidade.

Uma outra contribuição deste trabalho é a adaptação de uma metodologia de desenvolvimento de software para a especificação de protocolos criptográficos. A técnica de especificação formal escolhida é a lógica BAN, voltada para a especificação e validação de protocolos criptográficos e a ferramenta de simulação escolhida é o *Network Simulator* (NS), por ser bastante utilizado no meio acadêmico e possuir módulos MIP implementados.

A especificação formal com lógica BAN e o desenvolvimento de módulos do protocolo proposto para execução no NS geram ainda uma contribuição secundária desta dissertação que é uma base de referência de estudos para futuros desenvolvedores de protocolos de segurança e de módulos para o NS.

1.3 ESTRUTURA DA DISSERTAÇÃO

Além deste capítulo de Introdução, a dissertação está organizada em cinco capítulos, descritos a seguir.

No Capítulo 2, fazemos uma revisão da área de Internet Móvel, apresentando os conceitos de mobilidade de terminal e pessoal, e mostrando uma classificação para os protocolos de mobilidade existentes: protocolos de rede acesso, de micromobilidade e de macromobilidade. Em seguida, são apresentados, neste mesmo capítulo, os protocolos *Mobile IP* (MIP), EGM – Elemento de rede para registro de localização e *Session Initiation Protocol* (SIP), para o gerenciamento de mobilidade em áreas de macromobilidade, e *Cellular IP* (CIP), *Handoff-Aware Wireless Access internet infrastrucuture* (HAWAII), e *Hierarchical Mobile IP* (HMIP), para o gerenciamento de mobilidade em áreas de micromobilidade.

No Capítulo 3, apresentamos os principais aspectos de segurança da informação em redes de computadores, discutindo ataques e serviços existentes nessa área. Também apresentamos duas linguagens de padrões de grande importância para este trabalho: Tropyc e Morar. Além disso, apresentamos segurança em redes locais IEEE.802 e os trabalhos relacionados com esta dissertação, tais como *Mobile-Foreign Authentication extension, Mobile IP Challenge/Response Extensions, Authentication, Authorization, and Accounting* e *IP Security*. Por fim, discutimos alguns aspectos das aplicações dessas propostas de segurança ao MIP.

No Capítulo 4, apresentamos a metodologia utilizada para desenvolver essa proposta, bem como, detalhamos a lógica BAN, útil para especificar formalmente os protocolos de segurança. Para compreendermos melhor o uso dessa lógica, será realizado um estudo de caso utilizando o protocolo *Wide-mouthed-frog.* Também descrevemos os principais simuladores de redes disponíveis e detalhamos o funcionamento do *Network Simulator*.

No Capítulo 5, apresentamos a proposta deste trabalho, que consiste na adição de uma entidade funcional para realizar o processo de autenticação de um MN visitante sem a

interferência do HA, utilizando a metodologia proposta no Capítulo 4 para formalizar nossa proposta.

Por fim, no Capítulo 6, concluímos a dissertação com um resumo dos principais resultados obtidos e algumas sugestões para trabalhos futuros.

CAPÍTULO 2 INTERNET MÓVEL

O objetivo deste capítulo é fornecer uma visão geral das tecnologias disponíveis para a Internet Móvel. Após uma breve introdução acerca de conceitos utilizados na Internet Móvel, serão detalhados e comparados os conceitos de áreas de macromobilidade e micromobilidade. Em seguida serão apresentados os protocolos *Mobile IP* (MIP), EGM – Elemento de rede para registro de localização e *Session Initiation Protocol* (SIP), para o gerenciamento de mobilidade em áreas de macromobilidade e *Cellular IP* (CIP), *Handoff-Aware Wireless Access internet infrastrucuture* (HAWAII), e *Hierarchical Mobile IP* (HMIP), para o gerenciamento de mobilidade em áreas de micromobilidade.

2.1 INTRODUÇÃO

Inicialmente, faremos a distinção entre dois tipos de mobilidade existentes na Internet Móvel, a mobilidade pessoal e a mobilidade de terminal, conforme apresentado em [WEB 2002].

A mobilidade pessoal é caracterizada por permitir ao usuário a troca do dispositivo que ele está usando para acessar a rede e ainda assim continuar a ter acesso aos recursos e serviços oferecidos por tal rede. Um exemplo desse tipo de mobilidade acontece com os sistemas celulares GSM (*Global System Mobile*) através dos módulos SIMs (*Subscriber Identity Modules*) [WEB 2002].

Por sua vez, a mobilidade de terminal permite a um usuário mudar de ponto de acesso e permanecer conectado à rede, sem perda de comunicação. O equipamento utilizado pelo usuário nesse tipo de mobilidade é denominado dispositivo móvel (*Mobile Node* - MN). A mobilidade de terminal está presente nos sistemas GSM, bem como em redes *Mobile IP*, como veremos na seção 2.3.1. Como nossa proposta é baseada em redes *Mobile IP* (ver Capítulo 5), estaremos sempre nos referindo à mobilidade de terminal no decorrer desse trabalho.

A Figura 2.1 ilustra um exemplo de mobilidade de terminal com duas redes interligadas pela Internet. Através dessas redes, denominadas de redes de acesso [WEB 2002], os dispositivos móveis acessam os serviços que essas redes disponibilizam. A estrutura de uma rede de acesso é

formada por pontos de acesso, *gateways* e roteadores internos, como mostrado nessa Figura. O ponto de acesso é uma entidade que permite ao dispositivo móvel se comunicar com a rede de acesso, podendo ser um roteador ou uma estação-base (*base station*). O *gateway* é o dispositivo que conecta a rede de acesso à Internet e é também conhecido como roteador de borda. O *gateway* possui um endereço IP real que possibilita a comunicação com outros equipamentos localizados na Internet.

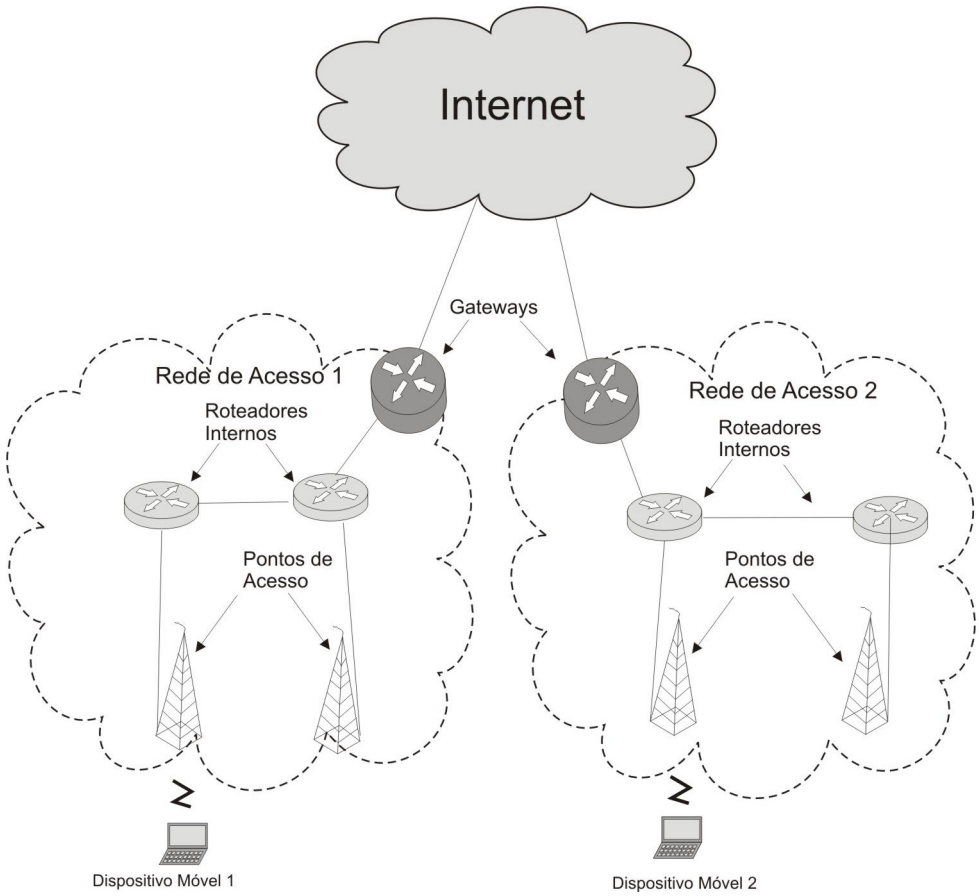


Figura 2.1 - Duas Redes de Acesso Conectadas Através da Internet

Nas redes de acesso, a movimentação de um dispositivo móvel entre pontos de acesso é denominada *handoff*, termo também utilizado pelos sistemas celulares para caracterizar a movimentação de usuários entre suas estações de base (*base stations*). Vale ressaltar ainda que os conceitos de área de localização, atualização de registro e autenticação são também reutilizados dos sistemas celulares pela Internet Móvel.

Vale mencionar que um conjunto de redes de acesso administrado por uma única Autoridade Administrativa (AA) é denominado de Domínio Administrativo (DA) na Internet Móvel [WEB 2002]. A Figura 2.2 representa a estrutura de dois domínios administrativos, contendo duas redes de acesso cada um.

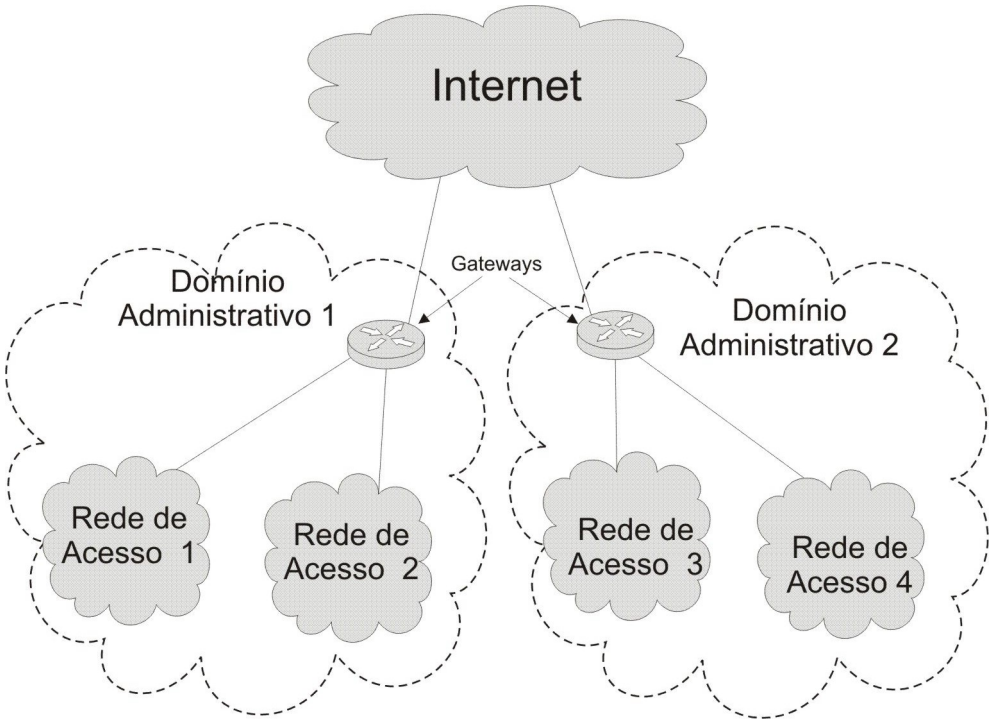


Figura 2.2 - Ambiente de Domínios Administrativos

2.2 GERENCIAMENTO DE MOBILIDADE

Para gerenciar a mobilidade dos usuários entre as redes de acesso foram desenvolvidos protocolos de gerenciamento de mobilidade [PERKINS 2002] [GEN 2001] [CGV 1999]. Esses protocolos podem ser classificados em protocolos de micromobilidade e macromobilidade. Os protocolos de micromobilidade são elaborados para gerenciar a mobilidade dentro de um domínio administrativo (intra-DA), enquanto os protocolos de macromobilidade são desenvolvidos para gerenciar a mobilidade entre domínios administrativos (inter-DA). Neste trabalho serão abordados os protocolos *Mobile IP* (MIP), EGM (Elemento de rede para registro de localização) e *Session Initiation Protocol* (SIP), para o gerenciamento de macromobilidade; e *Cellular IP* (CIP), HAWAII, e *Hierarchical Mobile* IP (HMIP), para o gerenciamento de micromobilidade.

Por terem ambientes de atuação diferentes, os protocolos de gerenciamento de mobilidade possuem características de mobilidade específicas. Se considerarmos um usuário móvel realizando um deslocamento inter-DA, podemos destacar algumas particularidades inerentes a esse tipo de mobilidade que são diferentes da mobilidade intra-DA. A seguir, apresentamos peculiaridades consideradas em [WEB 2002] que são relevantes no contexto do nosso trabalho.

A primeira característica refere-se à autenticação do usuário. No deslocamento inter-DA, por exemplo, o usuário deve ser autenticado novamente devido à fraca ou nenhuma relação de confiança entre os domínios administrativos. Por sua vez, no deslocamento intra-DA, o usuário não é obrigado a realizar uma nova autenticação, uma vez que todas as redes internas a um domínio administrativo são administradas por uma mesma entidade.

Outra característica é a possibilidade de não haver garantia de suporte à mobilidade quando o dispositivo realizar um deslocamento inter-DA, visto que o novo domínio administrativo pode não possuir tal suporte. Quando o deslocamento de um MN for intra-DA e o domínio administrativo possuir suporte à mobilidade, o usuário tem garantia de continuar a ter acesso aos recursos da rede.

Além disso, a política de cobrança e prioridades é diferente para cada domínio administrativo, de tal forma que ao se deslocar para um novo domínio administrativo, o usuário deve se adequar à nova política imposta pela rede sendo visitada. A forma como o usuário se adapta à política de segurança é dependente do domínio visitado.

A última característica é a atribuição de um novo endereço IP ao dispositivo móvel quando o mesmo entra em um domínio administrativo, pois cada domínio administrativo possui uma faixa diferente de endereços IPs. Por sua vez, em um protocolo de micromobilidade o dispositivo pode continuar ou não com o mesmo endereço IP, dependendo do protocolo de microbilidade utilizado.

2.3 PROTOCOLOS DE MACROMOBILIDADE

Nas subseções a seguir detalharemos o funcionamento dos protocolos de macromobilidade *Mobile IP* (versão 4 e versão 6) e *Session Initiation Protocol* (SIP). Embora o funcionamento desses dois protocolos seja bastante parecido, é importante salientar, de antemão, que a diferença fundamental entre eles é que o primeiro atua na camada de rede, enquanto o

segundo na camada de aplicação. Será apresentada também uma proposta que cria um elemento de rede para registro de localização denominado EGM.

2.3.1 *MOBILE IP* VERSÃO 4

Mobile IP versão 4 (MIPv4) [PERKINS 2002] é um protocolo definido pelo IETF [IETF 2003] que permite a usuários móveis migrarem de sua rede de origem (*home network*) para redes estrangeiras (*foreign networks*), ambas dentro do mesmo domínio administrativo ou em domínios administrativos diferentes, sem mudar de endereço IP e sem perder a conectividade.

O protocolo MIPv4 introduz três novas entidades em sua arquitetura: o *mobile node* (dispositivo móvel), o *home agent* (agente domiciliar) e o *foreign agent* (agente estrangeiro). A Figura 2.3 apresenta as entidades do MIPv4.

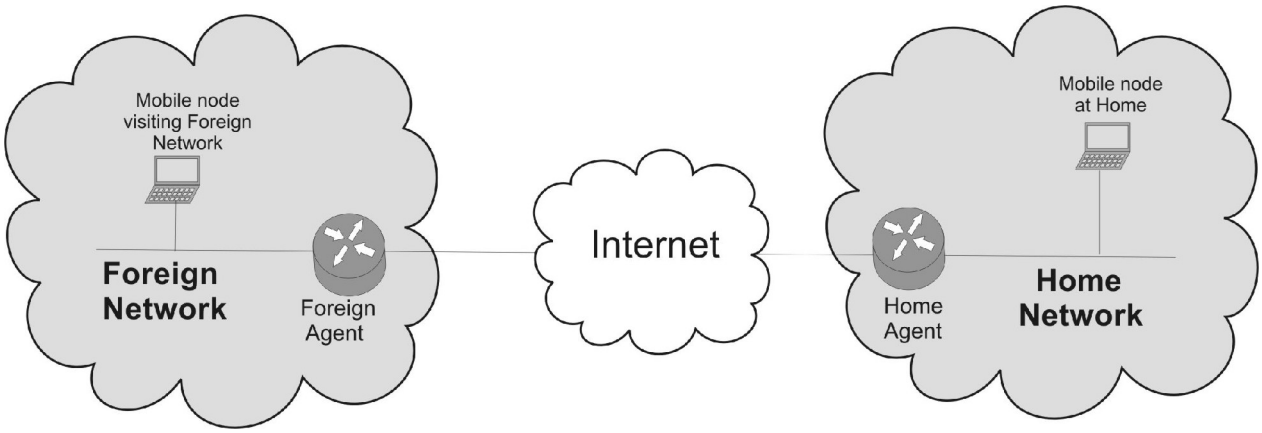


Figura 2.3 - Componentes do *Mobile IP* Versão 4

Mobile Node (MN) é um dispositivo (e.g., celular, *Personal Digital Assistant* ou *laptop*) que é sempre identificado por um endereço IP fixo, denominado *Home Address* (Hadd), independente do seu ponto de acesso à Internet. Ao entrar em uma *Foreign Network*, ou seja, qualquer rede diferente da *Home Network*, o MN recebe um endereço temporário (*care-of-address*) que está associado à posição atual do móvel.

Home Agent (HA) é um agente localizado na *Home Network* responsável por armazenar a posição atual do MN. Esse armazenamento é realizado através de um mapeamento dinâmico entre o *Home Address* e o *care-of-address* (CoA) do MN. O mapeamento é atualizado a cada

mudança de rede realizada pelo MN, através de mensagens emitidas pelos MNs que informam sua posição atual. Outra função do HA é capturar os pacotes enviados por um dispositivo que esteja realizando comunicação com o MN, denominado *Correspondent Node* (CN), e encaminhá-los ao local onde se encontra o MN que está fora de sua *Home Network*.

Foreign Agent (FA) é um agente localizado na *Foreign Network* que pode atuar como um ponto de acesso para os MNs visitantes, entregando os pacotes enviados pelo HA ao MN visitante.

Nas próximas sub-seções detalharemos o comportamento funcional do *Mobile IP* versão 4.

2.3.1.1 COMPORTAMENTO

Nessa seção apresentamos o funcionamento geral do MIPv4 que consiste das seguintes fases: descoberta de agente, registro e tunelamento [PERKINS 2002]. O detalhamento dessas fases é feito nas próximas subseções.

2.3.1.1.1 Descoberta de Agente

A descoberta de agente consiste em fazer com que os MNs conheçam os agentes de mobilidade responsáveis pela rede na qual o MN faz parte ou está visitando.

Os agentes de mobilidade de uma rede (e.g., FA ou HA) anunciam seu endereço IP e os serviços de mobilidade disponíveis (como tunelamento reverso, a ser visto na Seção 2.3.1.2) para os MNs através dos anúncios de agente (*Agent Advertisement*). Os agentes também indicam o tempo de validade do registro e uma lista de *care-of-address* que podem ser utilizados pelo MN no processo de registro.

O envio de anúncios é feito periodicamente pelos agentes da rede e destinado a todos os MNs que se encontram na área em que tais agentes gerenciam. O MN pode solicitar diretamente ao agente o envio imediato de um anúncio, caso não deseje esperar pelo anúncio enviado periodicamente.

Através das mensagens de *Agent Advertisement* o MN pode determinar se ele está em sua *Home Network* ou em uma *Foreign Network*. Caso esteja em sua *Home Network*, não é necessário utilizar os serviços de registro do MIP.

Quando um MN se move para uma *Foreign Network*, ele obtém um *care-of-address* a partir dos *Agent Advertisement* enviados pelo FA, sendo denominado FA Côa neste caso, ou por algum mecanismo externo tal como *Dynamic Host Configuration Protocol* (DHCP) [DROMS 1993], denominado *co-located* CoA.

O FA Coa é o endereço IP do FA responsável pela rede sendo visitada pelo MN. Um MN que adquire esse tipo de *care-of-address* compartilha esse endereço com outros MNs visitantes. Um *co-located* CoA é um endereço IP atribuído temporariamente ao MN, que representa a posição atual do MN na *foreign network* e só pode ser usado por um único MN visitante.

2.3.1.1.2 Registro

Registro é o processo de atualizar a localização de um MN junto ao seu *Home Agent*. Essa atualização deve ser feita a cada mudança de domínio administrativo ou após o tempo de validade do registro anterior expirar.

Se o MN detectar que se encontra em uma nova rede estrangeira ou que o tempo de validade do registro anterior expirou, o MN envia um pedido de atualização de registro (*registration request*) ao seu *Home Agent*. Esse pedido pode ser encaminhado ao FA para que seja direcionado ao HA, ou pode ser enviado diretamente ao HA, caso esteja usando um *co-located care-of-address*. Se o pedido for enviado através do FA, este checa a validade da solicitação. Se a solicitação não for válida, o FA envia uma resposta de registro (*registration reply*) informando que o pedido de registro falhou.

Ao receber a solicitação, o HA verifica a validade da solicitação que inclui, dentre outras verificações, a autenticação do MN (ver Seção 2.3.1.2). Se a solicitação for válida, o HA cria uma associação (*binding update*) entre o endereço do MN e o novo *care-of-address*, um túnel para o *care-of-address* e envia uma resposta (*registration reply*) ao pedido de registro para o MN através do FA ou diretamente ao MN. Se a solicitação não for válida, uma *registration reply* é enviada indicando que houve falha no pedido de registro.

2.3.1.1.3 Tunelamento

Tunelamento é o processo no qual o *Home Agent* intercepta os pacotes destinados a um MN e os envia ao local em que tal MN se encontra através do encapsulamento IP-sobre-IP

[PERKINS 1996]. Sendo assim, o tunelamento faz parte do processo de roteamento do protocolo *Mobile IP*.

O encapsulamento IP-sobre-IP consiste em criar um novo pacote com destino ao *care-of-address* do MN e inserir o pacote original no espaço de dados desse novo pacote. Ao receber o pacote, o MN extrai o pacote original removendo o cabeçalho IP mais externo, caso seja um endereço *co-located care-of-address*. Por sua vez, os pacotes enviados pelo MN são entregues ao seu destino (e.g., *Correspondent Node*) usando os mecanismos de roteamento IP tradicionais, não necessitando passar pelo HA. A Figura 2.4 ilustra o roteamento no Mobile *IPv4*, com foco no processo de tunelamento.

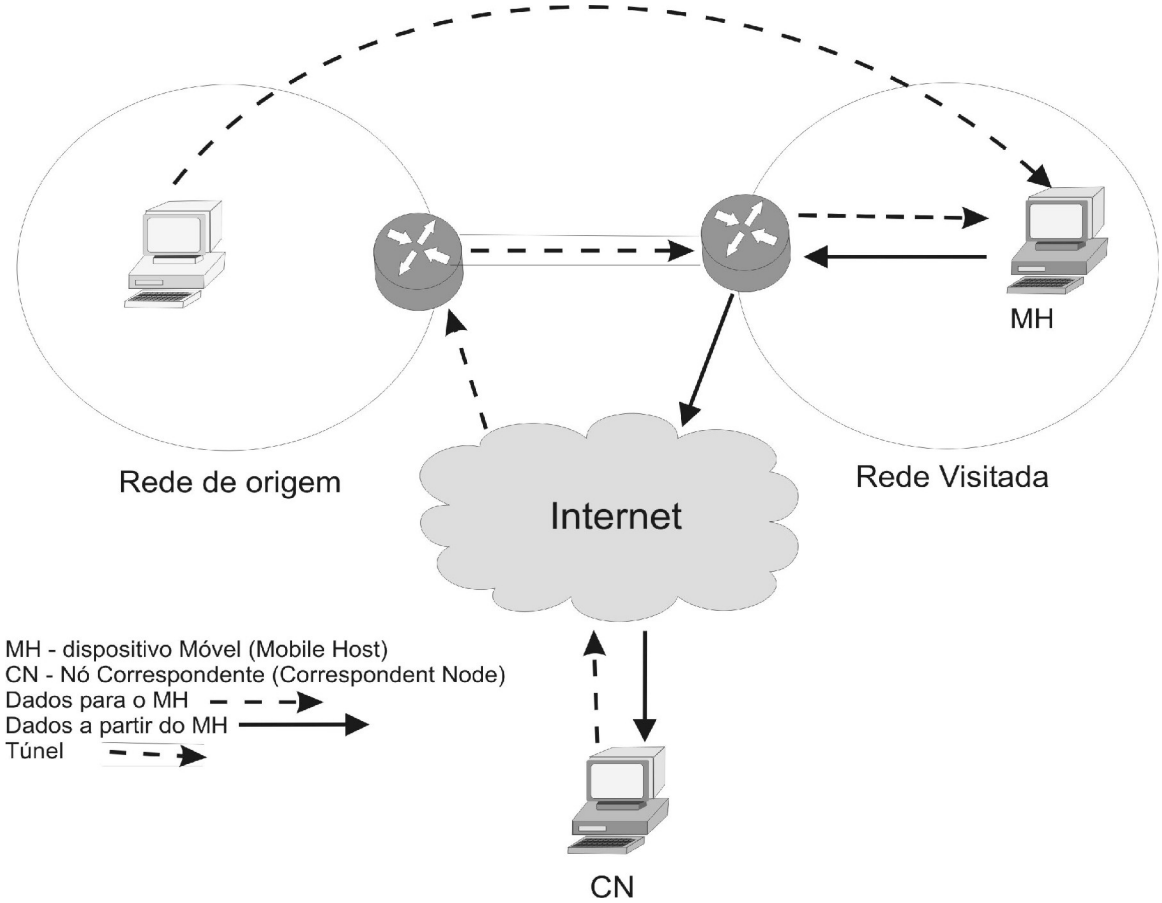


Figura 2.4 - Roteamento e tunelamento no *Mobile IPv4*

2.3.1.2 PROBLEMAS E SOLUÇÕES NO GERENCIAMENTO DE MOBILIDADE

O MIPv4 apresenta algumas falhas no protocolo, tais como o roteamento triangular e a perda de pacotes no filtro de entrada de uma rede [PERKINS 1997]. Nessa seção discutiremos

esses problemas e as respectivas propostas para solucioná-los. Outras falhas e soluções são encontradas na literatura [PERKINS 1997], mas não estão diretamente relacionadas com esta dissertação.

O primeiro problema refere-se aos filtros de entrada (e.g., Firewalls) encontrados nos roteadores de borda das redes visitadas. Esses filtros possuem regras de filtragem que descartam pacotes destinados a *hosts* externos e cujo endereço de origem do pacote não tenha um prefixo igual ao prefixo da rede em que se encontra o filtro. Pelo fato do MN utilizar seu endereço *Home Address* como o endereço de origem dos pacotes enviados para um CN, os pacotes do MN serão descartados pelo Filtro. Para resolver esse problema, uma solução, denominada de Tunelamento Reverso [MONTENEGRO 1998] foi proposta, cujo objetivo é criar um túnel do MN para o HA, denominado de túnel reverso. Ao chegar no HA os pacotes são desencapsulados e entregues ao CN com o *Home Address* como seu endereço de origem. A Figura 2.5 ilustra o tunelamento reverso.

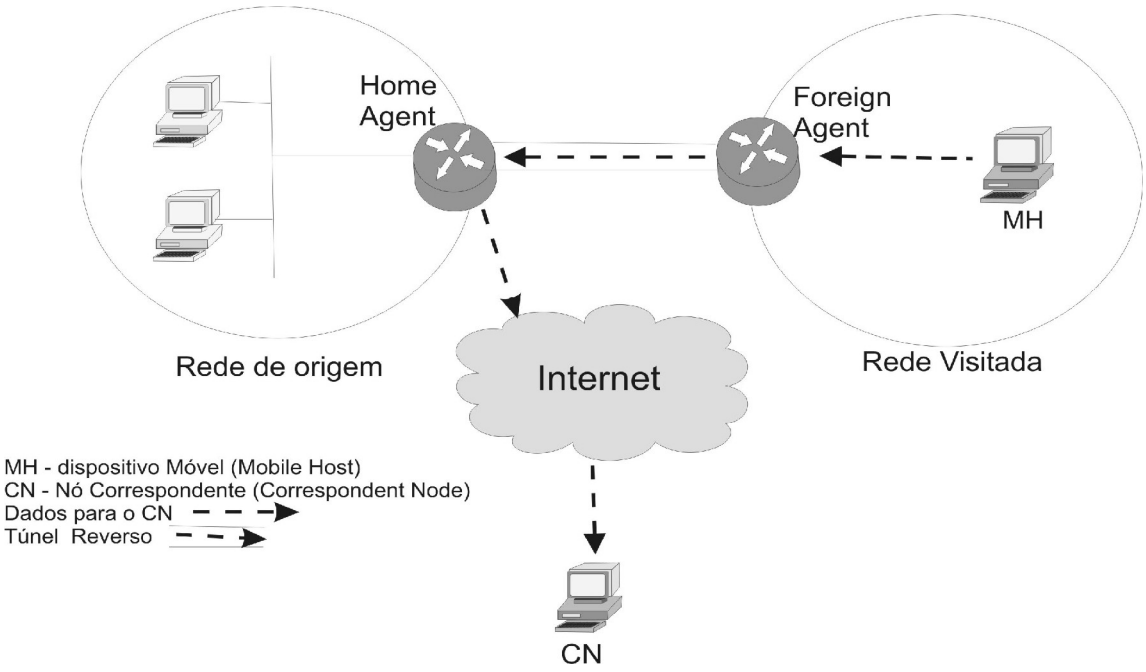


Figura 2.5 - Tunelamento Reverso

O segundo problema ocorre devido ao fato de que no MIPv4 todos os pacotes vindos dos CNs são entregues ao móvel via *Home Agent*, como apresentado anteriormente na Figura 2.4. O MN por sua vez envia diretamente os pacotes destinados ao CN, formando assim um roteamento triangular que é ineficiente principalmente quando houver uma comunicação entre um terminal

visitando uma rede distante e algum CN pertencente a tal rede. Uma solução para esse problema foi proposta em [JP 2000] e denominada Otimização de rota. Através dela é possível transmitir pacotes oriundos dos CNs diretamente ao MN, sem passar pelo HA. Isso é possível através de mensagens de *Binding Updates* (BUs) enviadas pelo *Home Agent* aos CNs informando a nova posição (*care-of-address*) do MN.

2.3.2 *MOBILE IP* VERSÃO 6

O protocolo *Mobile IP* versão 6 (MIPv6) foi projetado para fornecer suporte à mobilidade em redes IPv6 [JP 2004]. Apesar das semelhanças com o MIPv4, o MIPv6 possui características adicionais voltadas para redes IPv6 e que serão apresentadas no restante dessa seção. MIPv6 também incorpora as soluções para os problemas apresentados na Seção 2.3.1.2.

A principal mudança é conseqüência do maior número de endereços IP fornecido pelo IPv6. Com esse número maior de IPs, todos os MNs podem usar um *co-located care-of-address* (CCoA). Uma outra característica é a ausência de *Foreign Agents* nas redes visitadas. Isso é possível graças às novas características de descoberta de vizinhança, auto-configuração de endereço e a capacidade dos roteadores enviarem mensagens de anúncio de roteador do IPv6 [DH 1995/1] [DH 1995/1]. Além disso, a otimização de rota é agora parte integrante do protocolo MIPv6. As mensagens de *binding updates* são enviadas diretamente pelos MNs aos CNs, retirando essa funcionalidade do HA.

Também não é mais necessário realizar o tunelamento reverso, visto que o *home address* e o *care-of-address* do MN são indicados nos pacotes enviados para um CN, diferente do MIPv4 que usava apenas o *home address*. Isso permite que um MN use seu CoA como o endereço de origem no cabeçalho IP do pacote e possa conseqüentemente atravessar os filtros de entrada da rede sendo visitada.

2.3.3 EGM – ELEMENTO DE REDE PARA REGISTRO DE LOCALIZAÇÃO

[ALBANO 2004] [AACA 2003] apresenta uma proposta de aplicação dos princípios de mobilidade utilizados nos sistemas celulares com o objetivo de minimizar o número de registros necessários para localizar um dispositivo móvel no deslocamento entre domínios de micromobilidade. Deste modo, o registro de localização de um MN somente será realizado

quando dados precisarem ser enviados a ele. Da mesma forma, o móvel está sempre pronto a utilizar a rede quando precisar efetuar uma transmissão, sem a necessidade de estabelecer vários registros prévios com sua rede de origem.

Para que os dispositivos móveis possuam a capacidade de estar conectados passivamente à rede IP enquanto migram entre regiões de micromobilidade, é necessária uma entidade funcional de rede que atue em mais de uma área de micromobilidade, sendo capaz de localizar os dispositivos móveis através de um sistema de *paging* e oferecer a eles os recursos necessários para se conectarem a rede IP.

A proposta consiste na adição de um elemento de rede responsável pelo gerenciamento de macromobilidade em vários pontos de uma rede de longa distância, de forma a manter atualizada a localização de um determinado número de dispositivos móveis. Estando ligado à rede fixa e podendo ser consultado pelos *gateways* das redes de origem e por outros nós da rede semelhantes, este elemento é utilizado no armazenamento do registro de localização dos terminais e na busca dos mesmos quando estiverem em trânsito. Esse novo componente é chamado Elemento Gerenciador de Macromobilidade (EGM).

A rede formada por um conjunto de EGMs constitui uma área de macromobilidade que engloba várias redes *Cellular IP* (Figura 2.6), estabelecendo uma camada superior a outras redes que operam com micromobilidade para, além de proporcionar mecanismos de localização, tornar menor o esforço requerido para localizar o MN em uma mudança entre redes.

A função principal do EGM é mapear a localização do móvel quando este estiver transitando entre áreas de micromobilidade, conforme ilustra a Figura 2.6. As características de conectividade passiva e *paging* utilizadas pelo *Cellular IP* e que não estão presentes no *Mobile IP* são agora utilizadas em macromobilidade. A proposta considera que as regiões de micromobilidade operam com *Cellular IP*, possuindo assim um *gateway* para a comunicação com a Internet, e que a rede de telefonia móvel está conectada à rede IP, através de elementos que propiciem essa interface.

A Figura 2.6 ilustra a arquitetura da proposta. As várias redes *Cellular IP* se comunicam à Internet através de seu *gateway*. O EGM está conectado aos *gateways* através de uma rede TCP/IP. Além disso, o EGM está conectado aos elementos da rede de telefonia celular, como estações-base e outros EGMs. Como pode ser observado na Figura 2.6, o dispositivo móvel

participa originalmente de uma rede *Cellular IP* e é atendido pelo EGM enquanto migra para outra região de micromobilidade.

Na proposta, é considerado que o EGM faz parte da rede de telefonia celular, utilizando-se de sua infra-estrutura para realizar as funções de localização e o próprio EGM funciona como interface entre a rede de telefonia e a rede IP. Nesse contexto, as funções do EGM podem ser adicionadas a entidades já presentes nos sistemas de telefonia, como nós GGSN e SGSN do sistema GPRS [ALBANO 2004] [AACA 2003].

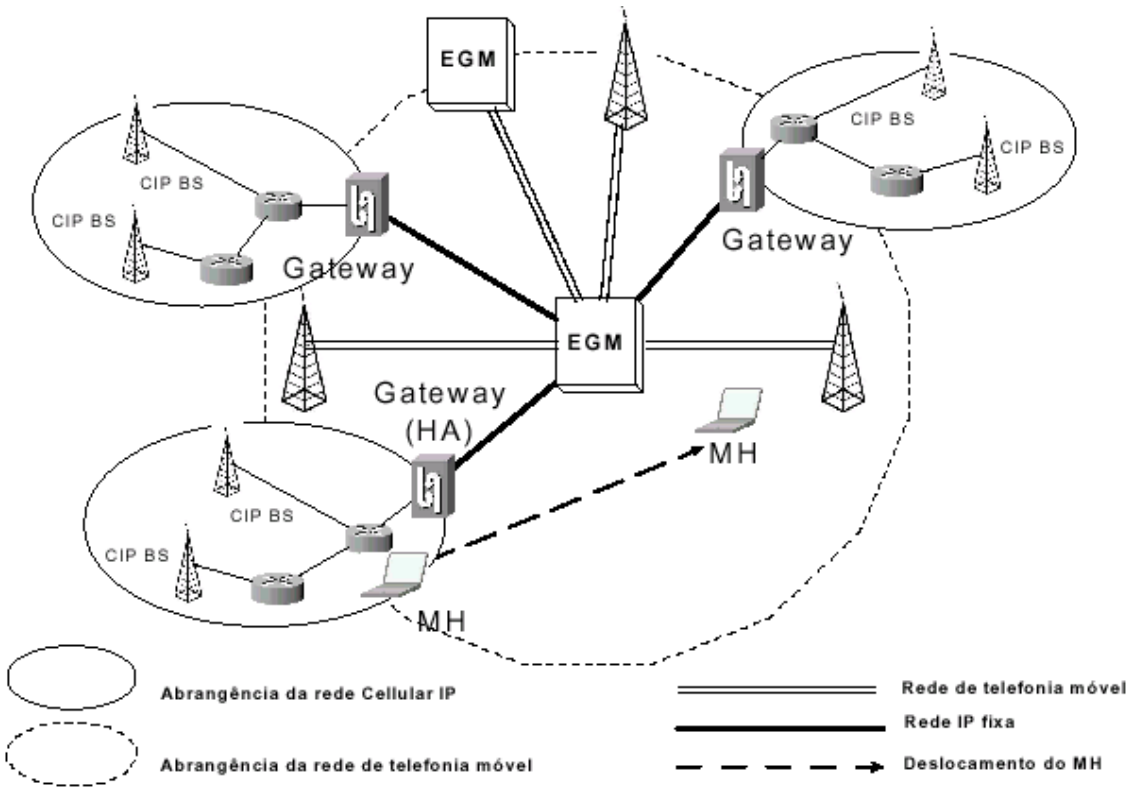


Figura 2.6 - Arquitetura da proposta EGM

Fonte: [ALBANO 2004]

2.3.4 SESSION INITIATION PROTOCOL

O *Session Initiation Protocol* (SIP) é um protocolo de gerenciamento de mobilidade, desenvolvido pelo IETF, capaz de fornecer mobilidade pessoal e mobilidade de terminal [CKK 2002]. Como mostrada na Seção 2.1, a mobilidade pessoal permite a transferência de uma comunicação em andamento de um dispositivo para outro. Um exemplo desse tipo de mobilidade

no SIP é a transferência de uma comunicação que está sendo realizada em um celular para um projetor, que fornecerá a imagem obtida da outra parte comunicante. Por sua vez, a mobilidade de terminal permite a mudança de domínio administrativo sem perder a comunicação com a rede, graças ao gerenciamento de mobilidade realizado pelo SIP. Um exemplo de mobilidade de terminal ocorre quando um usuário muda de um domínio administrativo para outro.

Para o funcionamento do SIP é necessária a presença de agentes de usuários (AU) nos dispositivos do usuário. Os usuários do SIP devem ser identificados através de SIP URLs, que lembram o formato de endereço de e-mail, e que têm o formato sip:usuário@DOMINIO, onde DOMINIO é o domínio original do usuário.

A Figura 2.7 apresenta o processo de registro no SIP para o usuário A.

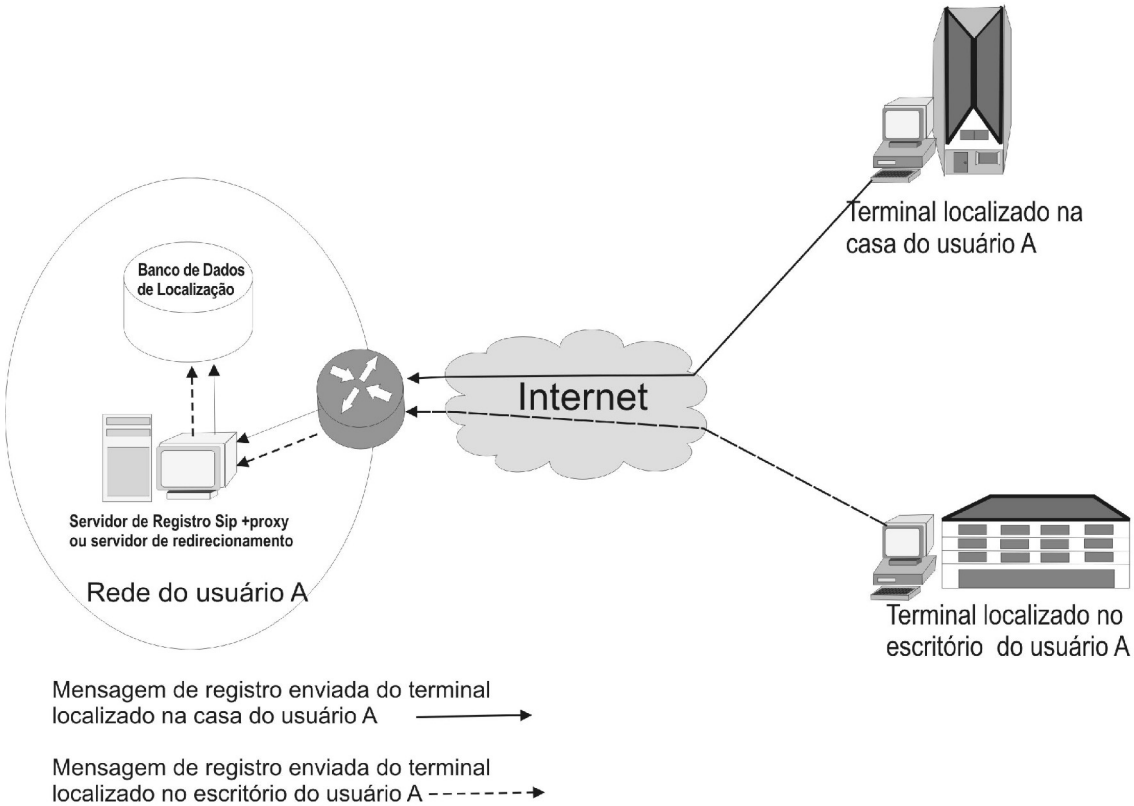


Figura 2.7 - Usuário registra os terminais de casa e do escritório

Em cada domínio há um servidor de registro SIP, que possui um endereço IP estático e é facilmente acessível por servidores DNS. Esse servidor SIP intercepta as mensagens de registro e atualiza a informação de localização do dispositivo. A mensagem de registro possui o SIP URL, o endereço IP atual que se encontra o usuário, o número da porta e o protocolo de transporte que está sendo utilizado no dispositivo (e.g., TCP), visto que SIP funciona independente do protocolo

de transporte. Outros campos adicionais da mensagem de registro são possíveis, como o tempo de validade do pedido de registro, que tradicionalmente é uma hora. O servidor de registro autentica o usuário e cria o mapeamento entre o URL SIP e o endereço de rede no banco de dados de localização.

Através do SIP URL, o usuário pode ser contactado independente da sua localização atual e o endereço IP utilizado. Entretanto, apenas conhecendo o SIP URL não é suficiente para rotear uma mensagem para um usuário. Também é necessário um servidor *proxy* ou um servidor de redirecionamento.

O servidor *proxy* é o responsável pelo mapeamento da URL para o endereço IP atual utilizando o servidor de registro. Após o mapeamento, o *proxy* encaminha a mensagem recebida para o endereço IP obtido. O servidor de redirecionamento é menos freqüente na arquitetura SIP e tem função similar ao servidor de DNS. Através dele, um usuário A pode solicitar a localização de um usuário B e receber uma lista de endereços. Após isso, o usuário A realiza toda comunicação diretamente com o usuário B.

Uma possibilidade do uso do SIP é o mapeamento de uma URL SIP para vários endereços IPs. Para visualizar essa facilidade do SIP, a Figura 2.7 ilustra um cenário, onde um usuário A está atualmente trabalhando em dois terminais, cada um com um AU, e que teve o endereço IP registrado junto ao servidor de localização.

Na Figura 2.8, se um usuário B desejar contactar o usuário A, ele envia uma mensagem de solicitação de comunicação ao *proxy*, especificando o URL SIP do usuário A. O *proxy* descobre que o usuário A está registrado para dois endereços de terminal e envia uma cópia da mensagem para cada um desses endereços. O usuário A envia uma resposta de solicitação de um dos terminais para o proxy, e este por sua vez retorna a resposta do AU do usuário A para o usuário B.

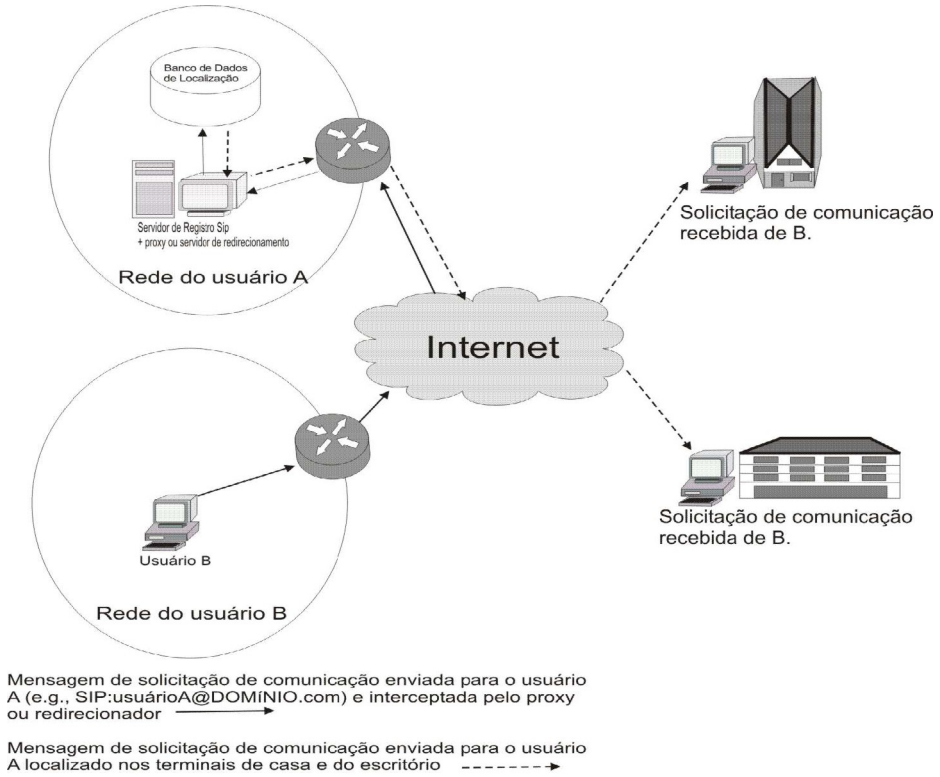


Figura 2.8 - Usuário B solicita comunicação com Usuário A via servidor Proxy

2.4 PROTOCOLOS DE MICROMOBILIDADE

Como mencionado na seção anterior, os pacotes endereçados para um nó móvel são entregues, através do MIP, utilizando o roteamento IP tradicional para um endereço temporário atribuído a esse nó em seu ponto de acesso atual. Isso oferece um esquema simples e escalável para a mobilidade global. No entanto, MIP não oferece suporte transparente à mobilidade, devido à necessidade do nó móvel atualizar o registro de localização em seu HA toda vez que mudar de ponto de ligação a Internet. Isso implica em longos períodos de espera no processo de registro e grande carga de sinalização na Internet, além de alta taxa de perda de datagramas, principalmente quando o MN estiver distante do seu HA.

Com a intenção de possibilitar *handoffs* rápidos e suaves, algo que não é possível no MIP, foram idealizados protocolos de mobilidade adequados para áreas geográficas restritas, denominados protocolos de micromobilidade, em contraste com os protocolos de macromobilidade (MIP e SIP), que gerenciam a mobilidade global e foram apresentados anteriormente.

Os protocolos de micromobilidade gerenciam a movimentação localmente, conseqüentemente, os problemas com altos atrasos, perda de pacotes e sobrecarga da Internet são minimizados. Dessa forma, aplicações que seriam inviáveis em um ambiente com os problemas de altos atrasos e perda de pacotes podem ser utilizadas, como por exemplo, voz sobre IP e videoconferência.

De uma forma geral, as propostas existentes para micromobilidade podem ser classificadas em esquemas baseados em roteamento e esquemas baseados em tunelamento.

Esquemas baseados em roteamento exploram a robustez da forma de transferência do IP tradicional. Por exemplo, um banco de dados distribuído de terminais móveis é criado e mantido dentro de um domínio de rede. Esse banco de dados consiste de tabelas com informações de endereços IP dos usuários e é mantido pelos agentes de mobilidade dentro do domínio administrativo (ver Seção 2.1). Esses esquemas são exemplificados pelos protocolos de micromobilidade *Cellular IP* e *Hawaii*, que diferem entre si na funcionalidade dos nós e no método de construção das tabelas de endereços.

Por sua vez, os esquemas baseados em tunelamento aplicam os conceitos de registro e encapsulamento de uma maneira local ou hierárquica, criando então uma concatenação flexível de túneis locais. No caso do MIP, a proposta do *Hierarchical Mobile IP* enquadra-se nessa categoria.

Os protocolos de micromobilidade, *Cellular IP* [CGV 1999] [CGKVCT 2000], HAWAII [RLTVS 1999] e *Hierarchical Mobile IP* [GJP 2002] serão descritos nas subseções seguintes.

2.4.1 CELLULAR IP

Cellular IP (CIP) é um protocolo de micromobilidade proposto pela Columbia *University* e pela Ericsson baseado no paradigma IP, herdando os seguintes princípios dos sistemas celulares para gerenciamento de mobilidade: conectividade passiva, *paging* e controle rápido de *handoff*. Nas subseções a seguir detalharemos os processos de roteamento, *handoff* e *paging* do *Cellular IP*, bem como a conectividade passiva que será considerada parte integrante do processo de *paging*.

A arquitetura da rede *cellular IP* é composta por *Mobile Node* (MN), *base station* (BS), roteadores internos (RI) e *gateway* (GW), como mostra a Figura 2.9. A seguir apresentaremos a arquitetura da rede CIP, bem como a forma como ela se comunica com outras redes.

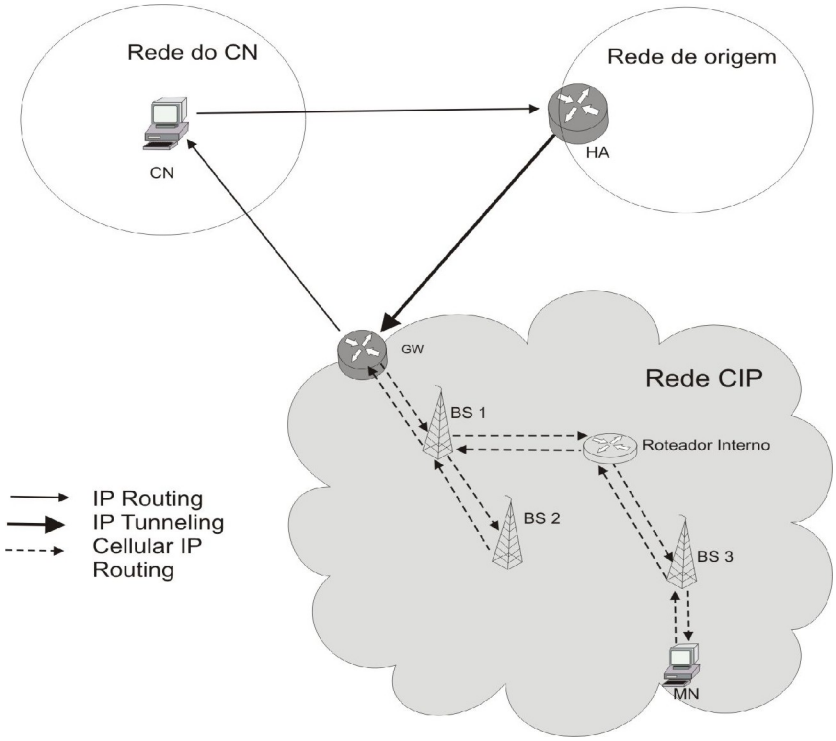


Figura 2.9 - Arquitetura de uma rede *Cellular IP*

Os MNs são os dispositivos móveis que utilizam os serviços e recursos da rede CIP; já as *base stations*, além de atuarem como pontos de acesso sem fio para os MNs, também realizam funções relacionadas ao roteamento de pacotes IP; os roteadores internos são responsáveis unicamente pelo roteamento CIP; por fim, os *gateways* (também conhecidos como roteadores de borda) conectam as redes CIP à Internet. Eles têm um papel fundamental na rede CIP, pois recebem, desencapsulam e enviam os pacotes para a BS onde se encontra o MN visitante. Dentro de uma rede CIP, o MN é identificado através de seu *Home Address* e os pacotes são roteados sem tunelamento ou conversão de endereço. Os pacotes enviados para um *host* externo à rede CIP são primeiramente roteados para o *gateway* e em seguida enviados para o *host* de destino.

A comunicação da rede CIP com outras redes (e.g., rede de origem ou rede do CN na Figura 2.9) é feita através do protocolo MIP. Para isso, eles utilizam o endereço IP do *gateway* como seu endereço *care-of-address*. Dessa forma, assumindo que a rede CIP utiliza a versão 4 do MIP para a comunicação externa e que não existe nenhuma otimização de rota no protocolo MIP (veja Seção 2.3.1.2), um pacote direcionado para o MN que se encontra dentro da rede CIP será

primeiramente encaminhado para seu *Home Agent*, onde é tunelado para o *gateway*. O *Home Agent* armazena o *care-of-address* do *gateway*, como sendo o *care-of-address* do MN.

Na rede *cellular IP*, por questões de otimização, o gerenciamento de localização e o suporte ao *handoff* são integrados ao roteamento; entretanto, por questões didáticas, essas funções serão explicadas separadamente nas subseções a seguir. Para minimizar as mensagens de controle, pacotes de dados transmitidos pelos MNs são usados para informar a localização dos mesmos.

2.4.1.1 ROTEAMENTO

No CIP, todos os pacotes gerados pelos MNs e destinados a qualquer *host* (interno ou externo à rede CIP) devem passar pelo *gateway* e só então serem entregues ao seu destino. Assim, toda *base station* e todo roteador interno devem possuir a informação de qual interface de saída deve enviar os pacotes recebidos pelos MNs a fim de alcançar o *gateway*. Essa informação é obtida através de mensagens de *beacon* enviadas periodicamente pelos *gateways* para toda a rede de acesso do CIP.

No momento em que os pacotes passam pelos nós da rede (e.g., *base station* e roteador interno) em direção ao *gateway*, é armazenado um registro que mapeia o endereço IP do MN emissor e a interface de entrada na qual foi recebido o pacote. A coleção desses registros é denominada de *routing cache*. Dessa forma, ao receber um pacote endereçado a um MN, o nó consulta na sua tabela o mapeamento referente ao endereço IP do destino do pacote e retorna a respectiva interface de saída. Esse processo é realizado até que o MN seja alcançado pela BS num processo *hop-a-hop*. Esse mapeamento continua válido por um período de tempo, denominado *route-timeout*, e sua validade é renovada a cada pacote recebido na mesma interface de entrada emitida pelo MN em questão.

Quando não possuir dados a serem enviados, o MN pode enviar pacotes de *route-update* para o *gateway* a fim de manter atualizado o mapeamento existente em todos os nós da rota. Esses pacotes são enviados em um intervalo regular de tempo, denominado *route-update- time*, e não deixam a rede de acesso *Cellular IP*.

A Figura 2.10 ilustra o caminho seguido por um pacote de dados enviado por um MN com destino a um CN na Internet. Uma rede CIP possui um conjunto de células (representadas por hexágonos na figura) e cada célula possui uma ou mais *base stations*. O MN em questão se

encontra na célula 5, e está acessando a rede através da *base station* 6 (BS6). A seqüência percorrida pelo pacote ate chegar ao *gateway* é a seguinte: BS 6, roteador interno, BS 2 e BS1.

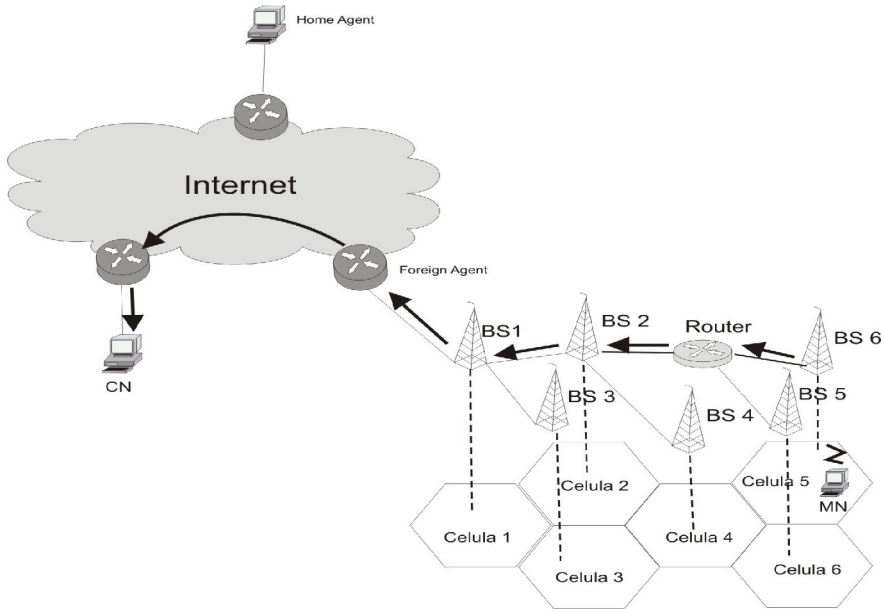


Figura 2.10 - Roteamento no CIP

2.4.1.2 HANDOFF

Como vimos na Seção 2.1, *handoff* é a movimentação de um dispositivo móvel (e.g., MN) entre pontos de acesso de uma rede (*base stations*). No CIP, a solicitação de *handoff* é feita pelo MN e é direcionada a BS que possui a maior potência de sinal das mensagens de *beacon* emitidas. No CIP existem dois tipos de *handoff*: o *hard handoff* e o *semisoft handoff*.

No *hard handoff*, ao receber uma mensagem de *beacon* enviada por uma BS com um sinal mais forte do que a atual, o MN envia um pacote de *route-update* para a nova BS e passa a utilizá-la. Isso cria um mapeamento *routing cache* nos nós pertencentes à rota entre o MN e o *gateway*. O mapeamento associado à BS anterior não é desfeito automaticamente, ele é mantido até que expire o *route-update time*. Durante o tempo de latência de *handoff*, que é o tempo gasto entre o *handoff* e a chegada do primeiro pacote através da nova rota, pacotes direcionados para o MN podem, entretanto, ser enviados para a rota anterior e conseqüentemente serem perdidos. Essa característica do *hard handoff* implica em uma solução de gerenciamento de mobilidade simples, que suporta um *handoff* rápido, a um preço de perda em potencial de alguns pacotes.

No *semi-soft handoff*, ao receber um *beacon* de uma BS com sinal mais forte que a atual, o MN envia para a nova BS um pacote de *route-update*, mas continua a receber pacotes pela BS antiga. Dessa forma, o MN possuirá dois pontos de acessos à rede, o que minimiza a perda de pacotes durante o *handoff*. No entanto, durante o período em que o MN possui comunicação com as duas BS (denominado *semisoft delay),* será consumido o dobro de recursos da rede. Após o *semisoft delay* o MN passa a utilizar somente a nova BS.

2.4.1.3 PAGING

Paging é a capacidade de uma rede encontrar um MN em uma área geograficamente restrita quando necessitar enviar dados a ele. Assim, o MN pode ficar em um modo ocioso (*idle*), ou seja, sem consumir recursos da rede e do próprio equipamento quando não possuir dados para enviar. Quando o MN está ocioso, mas pode se conectar a uma rede ou ser alcançado por ela, dizemos que ele possui a característica de conectividade passiva. O processo de conectividade passiva e *paging* são explicados a seguir.

Quando um MN não recebe pacotes por um determinado tempo, denominado *active-state timeout*, ele muda seu estado para o estado ocioso e permite que os mapeamentos *routing cache* sejam desfeitos. Para que possa ser localizado, o MN envia, em intervalos definidos por *paging-update-timeout*, pacotes de *paging-update*, que são pacotes vazios e roteados em um modelo *hop-a-hop* (similar ao *routing-update*) para o *gateway*.

O *paging-cache* é similar ao *routing-cache*, exceto por duas diferenças básicas. A primeira é que o *paging-cache* possui um tempo de vida, denominado *paging-timeout*, que é maior do que o período do *routing-cache*. A segunda é que os mapeamentos *paging-caches* são atualizados por qualquer pacote enviado por um MN, incluindo *paging-updates*. O mapeamento *paging-cache* é utilizado quando o *gateway* ou as BSs não acham um mapeamento para um MN no *routing cache*. Caso a BS não possua uma entrada no *paging-cache* para um determinado MN, ela envia o pacote recebido para todas as suas interfaces, exceto a interface que recebeu o pacote.

2.4.2 HANDOFF-AWARE WIRELESS ACCESS INTERNET INFRASTRUCUTURE

Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [RLTVS 1999] é uma proposta de micromobilidade baseada em domínios (ver Seção 2.1). Assim como o CIP,

HAWAII foi proposta para minimizar a perda de comunicação e a latência nos *handoffs* realizados pelos dispositivos móveis. HAWAII utiliza o protocolo *Mobile IP* para gerenciar a mobilidade inter-domínios e é transparente para os MNs.

A arquitetura do HAWAII é composta por *Mobile Node* (MN), *Base Station* (BS), Roteador Interno (RI) e Roteador Raiz (RR). A Figura 2.11 ilustra os componentes da arquitetura HAWAII.

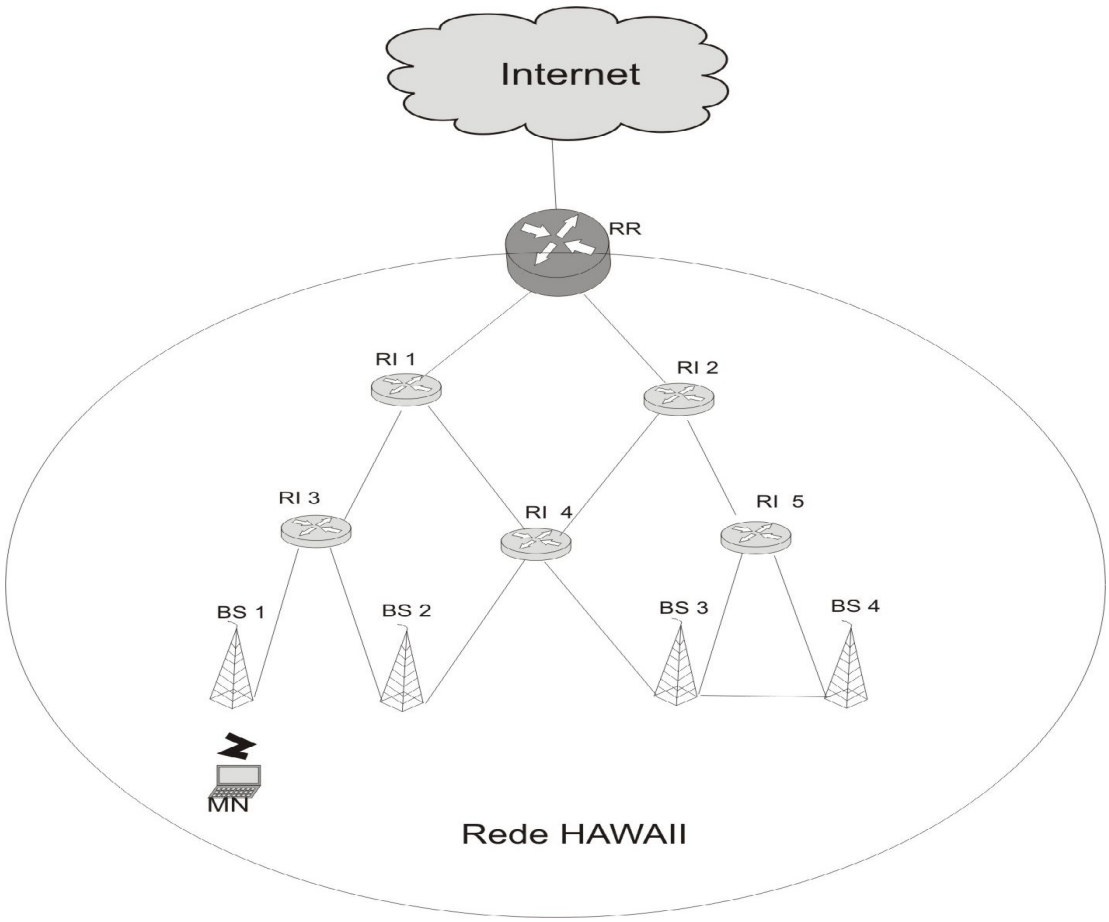


Figura 2.11 - Arquitetura do HAWAII

Os roteadores internos são as únicas entidades que executam o protocolo HAWAII dentro da rede. As BSs, além de sua função original de ponto de acesso para os MNs, funcionam como um tradutor do protocolo que o MN utiliza (e.g., MIP) e o HAWAII. O roteador raiz do domínio realiza o papel de *gateway* da rede com a Internet. Por fim, os MNs são dispositivos que utilizam os recursos da rede HAWAII.

O gerenciamento de mobilidade do HAWAII é realizado através dos esquemas de configuração de rota (*path setup scheme*), que consistem em um método para atualizar os roteadores (BS, RI e RR) em um domínio, a fim de manter a conectividade do MN enquanto um *handoff* estiver sendo realizado.

HAWAII utiliza mensagens de configuração de rotas para estabelecer e atualizar entradas de roteamento nos roteadores do domínio, de maneira que um pacote, ao chegar no roteador raiz, possa ser entregue ao MN de destino. Uma mensagem de atualização de rota (*path setup update*) é enviada por uma BS após receber uma solicitação de registro MIP vinda de um MN. O MN envia essa solicitação após realizar um *handoff* ou ser ligado.

Periodicamente, o MN envia mensagens de renovação de registro para a BS, que por sua vez envia uma mensagem para atualizar os roteadores que se encontram na rota de uma maneira *hop-a-hop*, até alcançar o roteador raiz.

Ao ser ligado, o MN envia uma solicitação MIP de atualização de registro para a estação-base mais próxima. A estação-base, então, envia uma mensagem de atualização de configuração de rota usando uma rota padrão. Cada roteador no caminho entre o MN e o roteador raiz adiciona uma entrada de roteamento para o MN. Por fim, o roteador raiz envia uma mensagem de confirmação para a estação-base que cria e envia uma mensagem MIP de resposta à solicitação.

Quando os pacotes endereçados para um MN chegam ao roteador raiz, eles são encaminhados para o MN usando as entradas de roteamento estabelecidas no processo de configuração de rota.

Existem dois tipos de esquemas de atualização de rota. O primeiro, denominado esquema de *forwarding*, é voltado para redes sem fio em que os MNs são capazes de receber/transmitir por apenas uma estação-base. O segundo, denominado *Non-Forwarding*, é otimizado para redes onde o MN pode receber/transmitir por duas ou mais estações-base simultaneamente e por um período curto de tempo.

O MN é reconhecido dentro de seu domínio de origem através do *Home Address*. Os pacotes endereçados para um MN que se encontra em seu domínio de origem são, primeiramente, entregues ao roteador raiz do domínio e só então redirecionados para o MN através de rotas estabelecidas através dos esquemas de configuração de rota.

Quando o MN se encontra em um domínio estrangeiro, o protocolo MIP é utilizado. Caso o domínio estrangeiro suporte o protocolo HAWAII, o MN recebe um *co-located care-of-addres*

(CCoA) atribuído pelo domínio estrangeiro. Os pacotes são tunelados para o *care-of-address* pelo seu *Home Agent*. Esse endereço permanece fixo enquanto o MN se encontra dentro do mesmo domínio estrangeiro.

2.4.3 HIERARCHICAL MOBILE IP

Hierarchical Mobile IP (HMIP) é uma proposta baseada no *Mobile IP* e cujo objetivo é diminuir o tempo gasto para um MN realizar *handoff* entre redes de acesso. Para alcançar esse objetivo, HMIP propõe uma nova entidade, denominada de *Gateway Foreign Agent* (GFA). O GFA deverá estar hierarquicamente superior ao FA das redes que ele abrange. A arquitetura de uma rede HMIP é apresentada na Figura 2.12. Ela apresenta duas redes MIP, possuindo um *Foreign Agent* cada uma; também são mostradas.

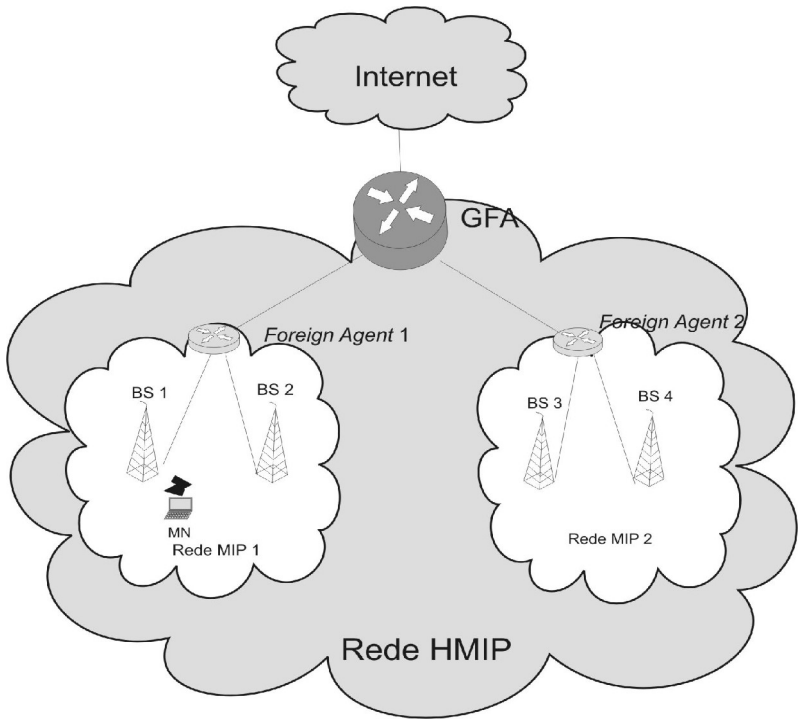


Figura 2.12 - Arquitetura da rede HMIP

Através da rede HMIP, um MN visitante só realizará o registro com seu *Home Agent* apenas uma vez. Quando o MN mudar de uma rede para outra dentro da área de abrangência do GFA, será necessário apenas realizar o registro com o GFA, não mais com o HA, diminuindo com isso o tempo gasto no processo de registro.

Enquanto o MN estiver visitando uma rede HMIP, o *Home Agent* conhecerá apenas o *care-of-address* do GFA como sendo o endereço temporário do MN.

2.5 CONCLUSÃO

Neste capítulo, investigamos as propostas existentes para gerenciamento de mobilidade para Internet Móvel. Além disso, comparamos os conceitos de macromobilidade e micromobilidade, detalhando o funcionamento dos protocolos de macromobilidade MIP, EGM e SIP, bem como dos protocolos de micromobilidade CIP, HAWAII e HMIP. No próximo capítulo serão apresentadas algumas propostas de segurança para redes MIP, foco desta dissertação.

CAPÍTULO 3 SEGURANÇA EM REDES

Neste capítulo faremos uma introdução geral sobre o estado atual da área de segurança da informação, mostrando os ataques à informação existentes e os serviços disponíveis para impedir ou amenizar tais ataques. Além disso, apresentaremos as linguagens de padrões MORaR e Tropyc, que possuem padrões de autenticação em seu escopo, e a solução de segurança do IEEE 802. Em seguida, serão discutidos os problemas decorrentes da falta de autenticação em uma rede gerenciada pelo *Mobile IP* e as soluções de segurança disponíveis para o protocolo *Mobile IP*.

3.1 INTRODUÇÃO

Ataques contra redes locais de computadores são bastante discutidos na literatura [BALPARDA 2001] [STALLINGS 2000]. Vários desses ataques também atingem as redes sem fio, por exemplo, os ataques por negação de serviço (*Denial of Service* - DoS), que podem comprometer o funcionamento normal de uma rede, negando a algum usuário válido o acesso a um recurso ou a um serviço fornecido pelo sistema. Outros ataques muito comuns são os acessos não autorizados ao sistema, que permitem um intruso utilizar recursos do sistema sem ter privilégios para tal.

Para tentar contornar alguns dos problemas de segurança mais comuns em sistemas móveis sem fio, tais como os sistemas celulares e a Internet Móvel, foram propostas novas soluções e também foram adaptadas algumas soluções existentes para redes fixas [PERKINS 2002] [PERKINS 2000] [ATKINSON 1995/1] [ATKINSON 1995/2] [BDHSK 2003] [CFV 2002]. Também foram formuladas linguagens de padrões para auxiliar o desenvolvimento de soluções seguras para esses sistemas [BRD 2000] [ANDRADE 2001].

Maiores detalhes sobre segurança da informação e as soluções existentes para os problemas de segurança, com foco para a Internet Móvel, serão apresentadas nas próximas seções.

3.2 SEGURANÇA DA INFORMAÇÃO

A preocupação com segurança da informação surgiu da necessidade de evitar que uma comunicação realizada entre dois usuários (i.e., emissor e receptor) seja lida ou modificada por uma entidade não autorizada (i.e., intruso). As ações executadas por intrusos sobre os dados de uma comunicação são denominadas ataques, e os meios para se evitar que esses ataques sejam realizados são conhecidos por serviços de segurança [STALLINGS 2000]. Nas subseções seguintes discutiremos alguns ataques e serviços de segurança existentes bem como soluções de segurança que podem ser aplicadas em redes tradicionais e sem fio.

3.2.1 ATAQUES

Ataques são ações executadas por intrusos a partir das vulnerabilidades de um sistema computacional ou de uma rede, e são classificados em passivos e ativos [STALLINGS 2000].

Os ataques passivos consistem na interceptação de informações confidenciais de uma comunicação por uma entidade não autorizada. O intruso não modifica a mensagem, mas pode copiá-la. É o ataque mais comum e o mais difícil de ser detectado, pois não há como saber se uma mensagem recebida já foi lida por outro usuário.

Os ataques ativos, ao contrário dos passivos, modificam as informações trocadas em uma comunicação. Dentre os mais conhecidos, destacamos a interrupção, a modificação e a fabricação. Interrupção é o ataque que interrompe o fluxo de mensagens trocadas entre as partes comunicantes por longos períodos de tempo ou por sucessões de pequenos intervalos. Um exemplo desse tipo de ameaça é o corte da linha de comunicação. Modificação é o ataque no qual um intruso, além de interceptar as mensagens, altera e reenvia para o destinatário. Por fim, na fabricação, uma entidade não autorizada insere mensagens em uma comunicação.

3.2.2 SERVIÇOS

Serviços são medidas necessárias para evitar ou minimizar os ataques à segurança. Existem seis serviços de segurança bastante conhecidos: privacidade, autenticação do emissor, controle de acesso, disponibilidade, integridade e não-repudiação [STALLINGS 2000]. Esses serviços são detalhados a seguir:

Privacidade é um serviço que fornece resistência aos ataques por interceptação. Seu objetivo é impedir que o conteúdo de uma comunicação seja revelado a usuários não autorizados. Muitas vezes, nem mesmo a existência de uma comunicação deve ser revelada. A cifragem da mensagem e da identidade das duas partes da comunicação é, freqüentemente, o método para fornecer privacidade.

Autenticação do emissor garante que o emissor é quem realmente ele diz ser. Um possível ataque decorrente da falta de autenticação do emissor acarreta no acesso não autorizado a recursos e informações por um usuário que não possui permissão para isso.

Controle de acesso é um serviço para permitir que somente entidades autorizadas tenham acesso aos recursos do sistema. Um ataque possível em um ambiente que não possua esse serviço é a entrada no sistema de um intruso que simule uma entidade autorizada.

Disponibilidade garante que os recursos da rede estejam disponíveis independentes dos ataques de entidades maliciosas. Um ataque relacionado a esse serviço é o de negação de serviço (*Denial of Service*-DoS), no qual um intruso pode interferir em uma transmissão, interromper o protocolo de roteamento da rede, ou parar algum serviço de rede.

Integridade garante que a mensagem enviada não foi corrompida, seja por falhas da rede, ou devido a ataques maliciosos.

Não-repudiação garante que o emissor não negue o envio da mensagem. É importante para detectar e isolar dispositivos comprometidos.

3.2.3 LINGUAGENS DE PADRÕES - TROPYC E MORAR

Linguagens de padrões são utilizadas na área de Engenharia de Software com o intuito de agrupar um conjunto de padrões (i.e. *patterns*) que contenham soluções provadas para problemas de um domínio específico. No caso do domínio de segurança da informação, conseguimos identificar duas linguagens de padrões aplicáveis aos sistemas móveis sem fio [BRD 2000] [ANDRADE 2001].

Tropyc é uma linguagem de padrões para segurança voltada para software de criptografia baseada na arquitetura genérica de criptografia orientada a objeto [BRD 2000]. A linguagem é composta dos seguintes padrões: Privacidade da informação, Autenticação do emissor, Integridade da mensagem, Assinatura, Assinatura com apêndice, Privacidade com integridade,

Privacidade com autenticação do emissor, Privacidade com assinatura e privacidade com assinatura com apêndice.

A linguagem de padrões MoRaR captura padrões de requisitos e análise em sistemas celulares da 2ª geração a 3ª geração [ANDRADE 2001]. Dessa forma, novos sistemas celulares podem ser desenvolvidos utilizando os padrões encontrados nessa linguagem. Nela são tratadas questões de gerenciamento de mobilidade, onde está incluída a parte de segurança, e gerenciamento de recursos de rádio.

A linguagem de padrões Tropyc documenta soluções de segurança genéricas o suficiente para serem aplicadas em diferentes sistemas fixos. Para os sistemas sem fio pode ser utilizada de forma complementar tanto a linguagem de padrões Tropyc quanto a Morar. No nosso trabalho, utilizamos as soluções de segurança descritas na linguagem MoRaR (e.g., padrões autenticação e banco de dados de segurança) aliada aos padrões da linguagem Tropyc (e.g., autenticação do emissor, integridade da mensagem e assinatura).

Vale ressaltar que outras soluções da Linguagem MoRaR não relacionadas com segurança de informação podem ser utilizadas em sistemas celulares, uma vez que esses sistemas possuem soluções fáceis de serem aplicadas à Internet Móvel. Por exemplo, Albano [ALBANO 2004] utilizou as soluções de *handoff*, conectividade passiva, MSC âncora e *paging* em sua proposta de gerenciamento de localização.

3.2.4 NORMA TÉCNICA DE SEGURANÇA - IEEE 802.1X

IEEE 802.1x [CRAIGER 2002] é uma norma técnica (i.e. *standard*) relacionada a segurança em redes tradicionais (i.e. com fio) e sem fio, especificamente segurança em redes IEEE 802, que aplica o protocolo *Extensible Authentication Protocol* (EAP) [BV 1998]. Por sua vez, EAP é um protocolo de autenticação que fornece um *framework* que permite a utilização de diferentes métodos de autenticação. A proposta do EAP consiste em utilizar os certificados da infra-estrutura de chave pública e *tokens* de desafio-resposta de forma transparente, ao contrário dos protocolos que utilizam apenas nomes de usuários e senhas para autenticar um usuário que deseja utilizar os recursos de uma rede.

A arquitetura do 802.1x consiste em três elementos: o suplicante, que é um usuário ou cliente que deseja ser autenticado; o servidor de autenticação, que é o servidor atual que está

realizando a autenticação; e o autenticador, que é um dispositivo que permite a conexão do suplicante à rede de acesso.

Uma característica importante do 802.1x é que o autenticador por ser um dispositivo simples torna-se ideal para redes sem fio, que possuem pontos de acesso de pouca capacidade de memória e baixo poder de processamento.

O funcionamento geral do 802.1x consiste em:

- O suplicante envia uma solicitação ao autenticador, que é então passado para o servidor de autenticação.
- O servidor de autenticação retorna um desafio para o autenticador que o encaminha para o suplicante. É importante salientar que diferentes métodos de autenticação utilizados nesse passo incorrem em diferentes tipos e números de mensagens. EAP suporta autenticação apenas do lado cliente e autenticação mútua.
- O suplicante envia ao autenticador uma resposta ao desafio e este, por sua vez, encaminha ao servidor de autenticação.
- Se o suplicante fornecer a identidade corretamente, o servidor de autenticação envia uma mensagem de sucesso na autenticação, que passa então pelo autenticador. Após esse processo, o autenticador permite acesso ao suplicante a rede.

3.3 SEGURANÇA NO *MOBILE IP*

Nesta seção, iremos analisar algumas propostas de segurança que utilizam os serviços mencionados na Seção 3.2.2 para evitar os prováveis ataques de segurança a uma rede *Mobile IP*, foco desta dissertação.

De forma geral, um *Mobile Node* utilizando o protocolo MIPv4 pode realizar o processo de autenticação/registro com seu *Home Agent* de duas maneiras: a primeira acontece quando o MN envia uma solicitação de autenticação/registro ao *Foreign Agent* da rede sendo visitada, que, por sua vez, retransmite essa solicitação ao *Home Agent* do MN. Nesse caso, o MN utiliza o endereço IP do FA como seu endereço *care-of-adrdress*. A segunda maneira é quando o MN envia uma solicitação de atualização/registro diretamente ao *Home Agent* utilizando como *care-*

of-adddress o endereço IP fornecido ao MN através de mensagens de anúncio emitidas pelos *Foreign Agent*.

Nas duas situações, existe a possibilidade de um usuário mal intencionado realizar uma atualização de registro fazendo-se passar por um MN válido. Isso é feito enviando uma solicitação de registro que contenha o endereço IP do MN que está sendo atacado e um endereço *care-of-address* no qual o intruso possa ter acesso. Como conseqüência, o *Home Agent* do MN legítimo realizará o mapeamento do falso *care-of-address* com o endereço IP do MN, ocasionando um ataque por interrupção na comunicação com o verdadeiro MN. Outra conseqüência desse ataque é a obtenção ilícita dos dados que seriam enviados ao MN. Dessa forma, se não houver um esquema de autenticação, qualquer usuário mal intencionado pode captar informações confidencias ou interromper uma comunicação entre um MN e seu HA.

Para proteger os usuários de dispositivos móveis dos ataques existentes nas redes MIP, apresentamos, nas seções seguintes, quatro soluções bastante difundidas para segurança em redes *Mobile IP*: *Mobile-Foreign Authentication extension*, *Mobile IP Challenge/Response Extensions*, *Authentication Authorization and Accounting* (AAA) e IP *Security* (IPSec).

3.3.1 MOBILE-FOREIGN AUTHENTICATION EXTENSION

Mobile-Foreign Authentication extension é uma proposta para fornecer o serviço de autenticação para redes *Mobile IP* versão 4 proposta por PERKINS [PERKINS 2002]. Ela consiste na adição de extensões às mensagens definidas pelo protocolo MIP para autenticar o emissor das mensagens de controle. A extensão possui um campo denominado *authentication*, que é o resultado da aplicação de um algoritmo sobre um conjunto de informações utilizando uma chave simétrica conhecida pelo MN e o seu HA.

Para que o receptor possa decifrar o *authentication* e, conseqüentemente, autenticar o emissor da mensagem, é necessário que o emissor e o receptor troquem um conjunto de informações de segurança, tais como algoritmo e chave simétrica utilizada antes do estabelecimento de uma comunicação autenticada. Entre um par de emissor e receptor pode haver vários conjuntos de informações de segurança.

O parâmetro *Security Parameters Index* (SPI), um valor indicativo de qual conjunto algoritmo/chave foi utilizado é adicionado na extensão para que o emissor tenha conhecimento dos algoritmos e chaves que foram utilizadas para cifrar o *authentication*. Através do SPI, o

receptor pode localizar, em sua base de dados, as informações necessárias para realizar a decifragem do *authentication*.

A fim de evitar que um intruso reutilize mensagens de controle, como a de atualização de registro, o campo *authentication* possui uma informação que garante que a mensagem não foi enviada anteriormente, e possui as características de ser sempre diferente para cada solicitação de registro, e impossível de ser forjado por um intruso. Ela pode ser gerada randomicamente e denominada de *nonce*, ou pode ser a marca do tempo no momento do envio de uma mensagem, denominado neste caso de *timestamp*. Neste caso, o HA e o MN devem realizar sincronização constantemente para evitar que haja uma variação muito grande entre seus relógios. Se o emissor de uma comunicação enviar uma mensagem com o *timestamp* muito anterior ao tempo marcado no receptor, o receptor descartará a mensagem, considerando ser uma já enviada anteriormente.

Três extensões são disponíveis para garantir a autenticação das partes envolvidas na comunicação: MN-HA, MN-FA e HA-FA. A primeira é utilizada no pedido e na resposta de solicitação de registros; a segunda garante uma comunicação segura entre o MN e o FA; e a terceira garante a comunicação segura entre o HA e o FA.

O algoritmo de autenticação padrão usa o MD5 no modo *prefix+sufix* para processar um resumo da mensagem de registro. Neste trabalho, chamamos de *resumo* o resultado da aplicação de uma função *hash* a um texto. Um problema dessa solução é a escalabilidade, pois cada par de entidades comunicantes devem possuir uma associação de segurança pré-estabelecida.

3.3.2 MOBILE IP CHALLENGE/RESPONSE EXTENSIONS

Na Seção 3.3.1, PERKINS [PERKINS 2000] define uma extensão de autenticação ao MIPv4 pela qual um MN pode se autenticar ao *Foreign Agent* da rede sendo visitada (e.g., extensão MN-FA). No entanto, essa extensão não impede que um usuário mal intencionado envie uma solicitação de registro, captada a partir de um processo válido de registro realizado anteriormente por um outro MN, e utilize os recursos da rede indevidamente. Para minimizar esse problema, a proposta feita por PERKINS [PERKINS 2000] define extensões ao MIPv4 sobre os anúncios de agente (*Agent Advertisements*), e às solicitações de registro (*Registration Request*) através de um mecanismo denominado *challenge/response*.

Nas mensagens de anúncios de agente emitidas pelo FA é adicionada uma extensão, denominada extensão de desafio (*Challenge extension*), cuja função é lançar um desafio ao MN

com a finalidade de verificar a identidade desse MN através da resposta a esse desafio. Esse desafio consiste em um número aleatório criado pelo FA.

Ao receber o anúncio do FA com a extensão de desafio, o MN verifica se possui uma associação de segurança (AS) com o FA e, em caso afirmativo, adiciona uma extensão de autenticação MN-FA (i.e., *Mobile-Foreign Agent Authentication extension*) à solicitação de registro. Essa extensão deve possuir uma resposta ao desafio emitido pelo FA. Caso não possua uma associação de segurança, o MN adiciona uma extensão de autenticação MN-AAA entre um MN e um servidor AAA (o protocolo AAA será visto na Seção 3.3.4).

3.3.3 IP SECURITY

IP Security (IPSec) [ATKINSON 1995/1] [ATKINSON 1995/2] garante segurança na camada IP sem afetar as aplicações das camadas superiores. Entre os *gateways* e/ou dispositivos que implementam IPSec, uma rede virtual privada (VPN) pode ser construída com confidencialidade de dados satisfatória, até sob redes inseguras, como a Internet.

IPSec introduz o conceito de associação de segurança, um conjunto de parâmetros que permite negociar algoritmos de cifra que será utilizado. Através da associação de segurança o emissor e o receptor conhecem os mecanismos de segurança utilizados para estabelecer uma comunicação segura. Se for necessária uma relação de confiança nos dois sentidos de uma comunicação, é necessário, então, duas associações de segurança.

Uma associação de segurança é unicamente identificada por um endereço IP e um índice de parâmetro de segurança (*Security Parameter Index* - SPI). Desta forma, em qualquer pacote IP, a associação de segurança é unicamente identificada pelo endereço de destino e pelo SPI. Uma associação de segurança é definida pelos seguintes parâmetros:

- Algoritmo de autenticação e modo do algoritmo usado com cabeçalho de autenticação IP (necessário para implementações AH);
- Chave usada no algoritmo de autenticação utilizada com o cabeçalho de autenticação (necessário para implementações AH);
- Algoritmo de criptografia, modo do algoritmo, e transformação usada no cabeçalho de encapsulamento de dados de segurança (necessário às implementações ESP);

- Chave usada no algoritmo de criptografia utilizado no cabeçalho de encapsulamento de dados de segurança (necessário às implementações ESP);
- Presença / ausência e tamanho do campo do vetor de inicialização ou sincronização criptográfica para o algoritmo de criptografia (necessário às implementações ESP);
- Algoritmo de autenticação e modo usados com a transformada ESP, se alguma estiver em uso (recomendada para implementações ESP);
- Chaves de autenticação usadas com o algoritmo de autenticação, as quais são partes da transformada ESP, caso haja alguma (recomendada para implementações ESP);
- Tempo de vida da chave ou tempo para o qual deverá ocorrer mudança da mesma;
- Tempo de vida da associação de segurança;
- Endereço origem da associação de segurança, o qual poderia ser um endereço "*wildcard*" se mais de uma origem divide a mesma associação de segurança com o destino;
- Nível de sensibilidade (por exemplo, "secreto" ou "não classificado") dos dados a serem protegidos (requerido para todos os sistemas que necessitam prover segurança em níveis múltiplos, recomendado para todos os outros sistemas).

3.3.3.1 MODOS TRANSPORTE E TÚNEL

IPSec possui dois tipos de *Security Association*: o modo Transporte e o modo Túnel. No modo Transporte, o IPSec protege os dados (*payload*) do pacote IP, mas não o cabeçalho original. Nesse modo é inserido um cabeçalho IPSec entre o cabeçalho IP original e o *payload* do pacote. A Figura 3.1 ilustra o formato do pacote IP original e a Figura 3.2 mostra o modo Transporte do IPSec.

Cabeçalho IP original	TCP	Dados

|---------- *Payload* ----------|

Figura 3.1 Modo IP original

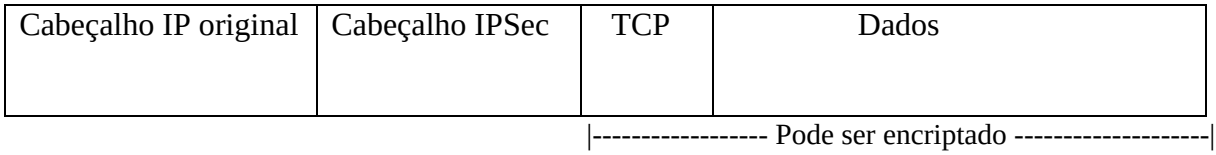


Figura 3.2 - Modo Transporte do IPSec

O modo transporte garante confidencialidade dos dados trocados entre dois terminais que utilizam o IPSec, mas não impede que seja feita uma análise do fluxo entre esses dois terminais por um intruso. Através dos cabeçalhos IPs, esse intruso pode determinar quais são as partes que estão se comunicando e com qual freqüência.

No modo Túnel, todo o pacote, inclusive o cabeçalho, é encapsulado dentro de um novo pacote, ou seja, o pacote a ser enviado se transforma em dados (*payload*) do novo pacote. O cabeçalho IPSec é inserido entre o cabeçalho original e o cabeçalho IP do novo pacote, como mostrado na Figura 3.4 e a Figura 3.3 ilustra o pacote IP original.

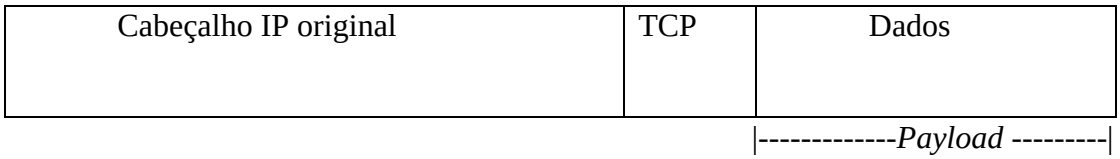


Figura 3.3 - Modo IP original

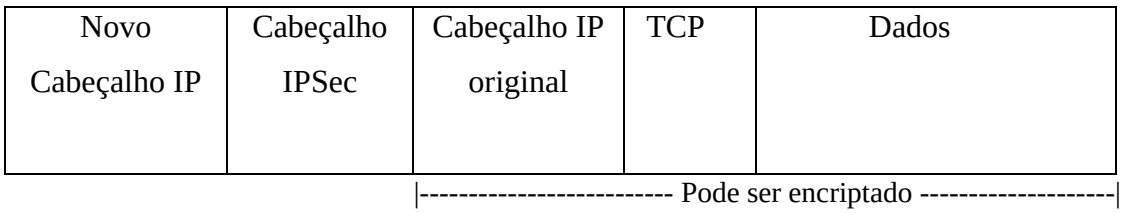


Figura 3.4 - Modo Túnel do IPSec

No modo Túnel os endereços de origem e destino contidos no novo cabeçalho são correspondentes aos pontos extremos do túnel, pois os endereços IP do pacote original são transportados dentro da parte segura do pacote. Conseqüentemente, é improvável uma análise de fluxo por um intruso.

3.3.3.2 PROTOCOLOS DE SEGURANÇA

IPSec define dois protocolos de segurança: o primeiro é o *Authentication Header* (AH) [ATKINSON 1995/2], que suporta integridade e autenticação utilizando algoritmos simétricos, como MD5 e SHA1; o outro é o *Encapsulating Security Payload* (ESP) [ATKINSON 1995/1], que suporta confidencialidade através de algoritmos de criptografia simétricos (DES e 3-DES) e, opcionalmente, integridade e autenticação. Cada protocolo possui seu próprio formato de cabeçalho IPSec e pode suportar o modo Túnel ou o modo Transporte.

Apesar de possuir as funções de autenticação e integridade incorporadas ao ESP, o AH não perde sua utilidade, pois possui características particulares importantes. Uma diferença fundamental entre os protocolos refere-se ao teste de integridade realizado. No ESP, o teste de integridade é realizado apenas no *payload* do pacote IP, excluindo o cabeçalho. Em contraste, o AH testa o pacote completo, incluindo o cabeçalho. A Figura 3.5 ilustra essa diferença.

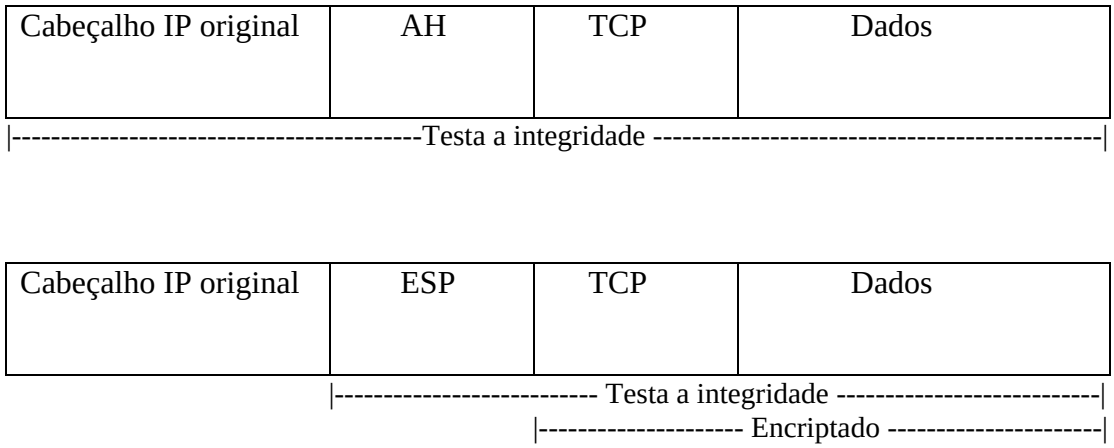


Figura 3.5 - Diferenças entre o teste de integridade do AH e do ESP

O IPSec pode ser aplicado de várias maneiras entre os componentes do MIP. Uma possibilidade é o suporte de segurança fim-a-fim, em que os pacotes transmitidos entre o MN e o CN são cifrados. Este cenário tem duas limitações: primeiro, o MN necessita manter um AS com cada CN com qual ele se comunica, o que afeta a escalabilidade; segundo, todos os CNs que se comunicam com um MN necessitam ter IPSec disponível, caso contrário não haverá nenhum mecanismo de segurança no enlace sem fio. Outro cenário possível é a criação de um túnel IPSec entre o *Home Agent* e o MN. Nesse ambiente o *Home Agent* só necessita armazenar um AS para

cada MN, similarmente aos sistemas celulares atuais, onde o *Home Location Register* (HLR) armazena uma configuração para cada usuário móvel.

3.3.4 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

Authentication, Authorization and Accouting (AAA) [BDHSK 2003] [CFV 2002] é uma proposta desenvolvida pelo IETF para fornecer as funções de autenticação, autorização e contabilização integradas em um único protocolo. Nesta seção apresentamos o modelo geral e o funcionamento do protocolo AAA. Na subseção 3.3.4.1 apresentaremos a adaptação do modelo geral do AAA ao protocolo MIP.

O modelo geral é composto por clientes, atendentes, servidores AAA e *Brokers*, como mostrado na Figura 3.6. O cliente é a entidade que utiliza os recursos de autenticação, autorização e contabilização do protocolo AAA para acessar os recursos da rede. O atendente, por sua vez, localiza-se no *Home Domain* (domínio de origem) e no *Foreign Domain* (domínio estrangeiro), e é a entidade responsável por receber todas as solicitações de acesso aos recursos da rede enviados pelos clientes. Os atendentes localizados no *Home Domain* e no *Foreign Domain* são denominados, respectivamente, *Home Attendent* (Hat) e *Foreign Attendent* (Fat). Para liberar o acesso aos recursos, o atendente deve solicitar ao cliente uma credencial, para que possa validar a identidade do cliente. Não há garantia que o atendente possa ter disponíveis as informações necessárias para a validação do cliente. Sendo assim, o atendente deve recorrer a uma autoridade local no mesmo *Foreign Domain* que possua tais informações, denominada servidor AAA *Local* (AAAL).

O servidor AAAL autentica o cliente caso ele disponha de informações de segurança; caso contrário, ele espera que o cliente seja configurado para verificar a credencial do mesmo no servidor AAA localizado no *Home Domain* do cliente, denominado AAA *Home* (AAAH). O AAAL e o AAAH são configurados com informações de segurança e com controles de acesso suficientes para autorizarem o usuário a utilizar os recursos solicitados.

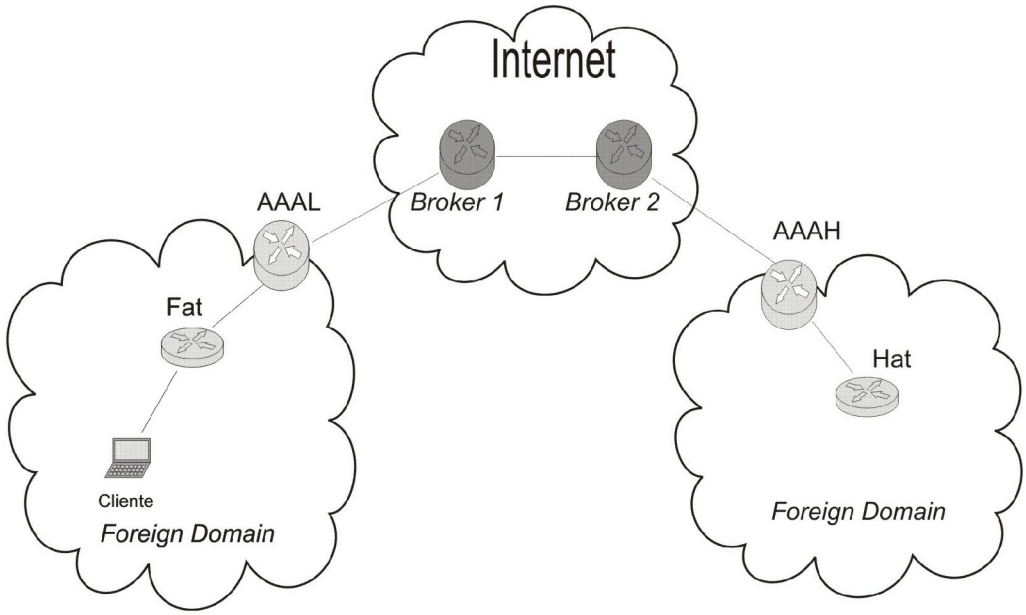
Além da função de autenticação do cliente, os servidores realizam funções de gerenciamento de requisições de autorização e coleta dados de contabilização dos recursos de rede consumidos.

Após a autorização ter sido obtida pelo AAAL através do AAAH, o AAAL notifica o atendente sobre a liberação do recurso solicitado pelo MN. O atendente, por sua vez, libera tais

recursos. É possível ter vários atendentes para cada AAAL e vários clientes para cada atendente. Cada domínio disponibiliza um AAAH para verificar as credenciais dos clientes que são administrados por ele.

O modelo geral do AAA também contém *Brokers*, entidades que realizam o papel de mediadoras de confiança entre dois servidores AAA que não possuem relação de confiança entre si. Portanto, os servidores AAA devem possuir uma relação de confiança com o *Broker* para haver uma comunicação segura entre eles.

De forma a permitir que as informações trocadas entre dois servidores AAA, entre um servidor AAA e um *Broker* e/ou entre um servidor AAA e um cliente sejam protegidas contra ataques de intrusos, é necessário criar e distribuir associações de segurança entre estas entidades.



AAAL - AAA *Server Local*
AAAH - AAA *Server Home*
Fat -*Foreign Attendent*
Hat -*Home Attendent*

Figura 3.6 - Modelo geral do AAA

3.3.4.1 APLICAÇÃO DO AAA NO PROTOCOLO *MOBILE IP*

Essa seção descreve as mudanças e adaptações necessárias ao protocolo AAA para que ele seja aplicado em uma rede *Mobile IP*. Primeiro é preciso mapear entidades pertencentes ao AAA em entidades do *Mobile IP*. Por exemplo, o cliente do protocolo AAA será representado pelo MN do MIP. O FA e o HA desempenharão o papel do atendente no AAA. No contexto do AAA, o HA desempenhará um papel secundário no processo de autenticação, ficando subordinado ao AAAH.

Após o processo de registro inicial, o MN pode continuar usando o *Mobile IP* dentro de um domínio estrangeiro sem a necessidade de utilizar os servidores AAA. O modelo geral do AAA atualizado para suportar o *Mobile IP* é mostrado na Figura 3.7.

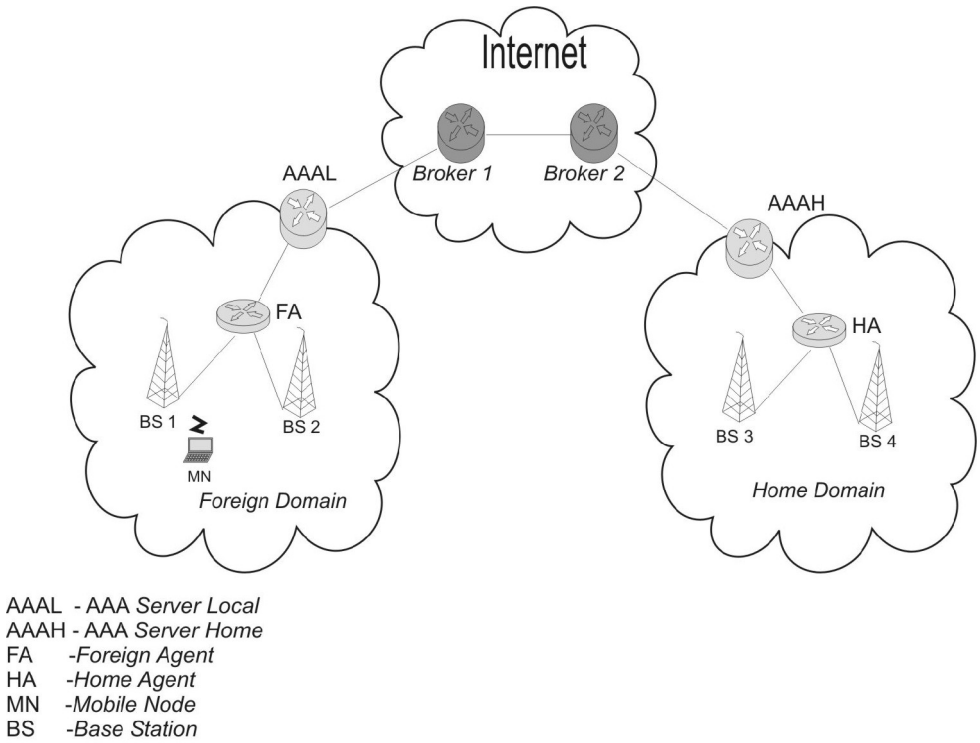


Figura 3.7 - Modelo geral do AAA aplicado ao *Mobile IP*

A comunicação entre os servidores AAA pode resultar em um tempo de espera muito alto, visto que os servidores terão que utilizar a Internet e poderão estar geograficamente distantes.

Para minimizar esse impacto no tempo, foi proposta a integração entre as funções do AAA e o registro inicial do *Mobile IP*. Dessa forma, todas as funções necessárias para o AAA e o registro do MIP devem ser executadas durante uma única passagem na Internet, reduzindo o tempo gasto no processo global.

O modelo original do AAA não necessita do HA para realizar a autenticação, no entanto, *Mobile IP* requer que cada pedido de registro seja realizado pelo HA. Diante disso, é necessário que, durante o processo inicial de registro, seja feita uma configuração que permita ao FA e ao HA realizarem subseqüentes registros. Portanto, após o registro inicial, o AAAL e o AAAH não são mais necessários.

Para que os registros subseqüentes sejam possíveis, é necessário que os servidores AAA sejam capazes de executar alguma forma de distribuição de chave durante o procedimento inicial de registro do MIP. Essa distribuição de chave executa um conjunto de funções de segurança, como por exemplo: identificação ou criação de uma associação de segurança (AS) entre o móvel e o HA necessária para executar o protocolo MIP; identificação ou criação de uma associação de segurança entre o MN e o FA, que será útil para garantir a identidade do móvel nos futuros pedidos de registro em um mesmo domínio administrativo; identificação ou criação da associação de segurança entre o FA e o HA, que será usada nos futuros registros realizados no mesmo domínio administrativo, de forma que o FA possa continuar a ter a segurança que o HA permanece autorizando os serviços *Mobile IP* para o móvel; participação na distribuição de associações de segurança entre as entidades do *Mobile IP* citadas acima; por fim, o servidor AAA deve ser capaz de validar os certificados fornecidos pelos móveis e prover uma resposta confiável para o AE.

O tempo de validade das associações de segurança distribuída pelos servidores AAA deve ser o suficiente para evitar constantes distribuições de chaves, pois esse processo pode causar grandes atrasos entre pedidos de registro.

3.3.5 DISCUSSÃO

Como apresentado na Seção 2.3.3, [ALBANO 2004] propõe a adição de uma entidade, denominada EGM, para minimizar o número de atualizações de registro de um MN que se desloca entre áreas de micromobilidade. No entanto, os autores não fornecem uma proposta de autenticação que vise minimizar o número de solicitações de autenticação ao HA. As propostas

de autenticação descritas anteriormente na seção 3.3 podem ser utilizadas, no entanto, nenhuma delas apresenta as características necessárias para diminuir o número de acessos ao HA.

Portanto, a inovação da nossa proposta está, justamente, em minimizar o número de solicitações ao HA para realizar a autenticação de um MN visitante, como será apresentado no Capítulo 5. Conseqüentemente, a junção da proposta de [ALBANO 2004] [AACA 2003] com a proposta desta dissertação, fornece um ambiente eficiente e seguro de gerência de localização de dispositivos móveis entre áreas de micromobilidade. A concepção inicial desta integração foi introduzida em [ASACS 2004], entretanto, não foi realizada nenhuma simulação ou especificação formal. No desenvolvimento da nossa proposta utilizamos algumas características dessa integração, tais como gerenciamento de mobilidade regional, no entanto, a integração total, abrangendo *paging* e conectividade passiva é considerada ainda como um trabalho futuro desta dissertação.

3.4 CONCLUSÃO

Neste capítulo apresentamos uma visão geral sobre segurança da informação, detalhando os ataques à informação existentes, bem como os serviços disponíveis para impedir ou amenizar tais ataques. Também apresentamos duas linguagens de padrões utilizadas nesse trabalho: Morar e Tropyc. Ambas possuem padrões de autenticação em seu escopo. Por fim, mostramos as soluções de segurança para redes *Mobile IP* disponíveis: *Mobile-Foreign Authentication extension*, *Mobile IP Challenge/Response Extensions*, *Authentication Authorization and Accounting* (AAA) e IP *Security* (IPSec).

No próximo capítulo apresentamos a metodologia utilizada para desenvolver nossa proposta, incluindo diagramas de seqüências, lógica BAN e o simulador *Network Simulator*.

CAPÍTULO 4 METODOLOGIA DE DESENVOLVIMENTO

Neste capítulo apresentaremos a metodologia de desenvolvimento utilizada para nossa proposta. A lógica BAN, técnica de especificação formal utilizada na metodologia, também será discutida. Além disso, será apresentada uma visão geral de diagramas de seqüência e dos simuladores de redes de computadores disponíveis, em particular, o *Network Simulator*.

4.1 INTRODUÇÃO

A utilização de métodos da engenharia de software no desenvolvimento de protocolos é útil para disciplinar o processo de construção de protocolos de alta qualidade, apresentando uma boa relação custo-benefício no desenvolvimento como um todo. Nessa dissertação utilizaremos o modelo de desenvolvimento formal de sistemas, que consiste em uma abordagem com características similares ao modelo em cascata, sendo que o desenvolvimento tem como base a transformação formal de uma especificação formal em um programa [SOMMERVILLE 2000].

A Figura 4.1 apresenta o modelo a ser utilizado nessa proposta que é uma adaptação do modelo de processo formal apresentado em [SOMMERVILLE 2000].

Para a definição de requisitos utilizaremos uma descrição informal com textos detalhando a funcionalidade do protocolo.

No projeto, em primeiro lugar, uma descrição formal com diagramas de seqüência, que mostram o fluxo de mensagens trocadas entre as entidades de um sistema, é realizada. Em seguida, utilizamos a lógica BAN, um método para especificação formal de protocolos de segurança que vem sendo bastante utilizado na literatura [BAN 1990]. A correta especificação em um estágio preliminar de desenvolvimento de um protocolo evita que erros sejam detectados tardiamente e permite validar que o protocolo atende aos requisitos anunciados.

Vale ressaltar que uma especificação formal de protocolos engloba uma ou mais técnicas de descrição formal que utilizam conceitos bem definidos e modelos matemáticos para representar propriedades significativas de um protocolo. O uso de técnicas formais durante a

especificação de um protocolo permite a eliminação de ambigüidades e inconsistências, por exemplo, as quais apenas seriam detectadas mais tarde durante fases de implementação e testes do ciclo de desenvolvimento de um sistema [AALSY 1999].

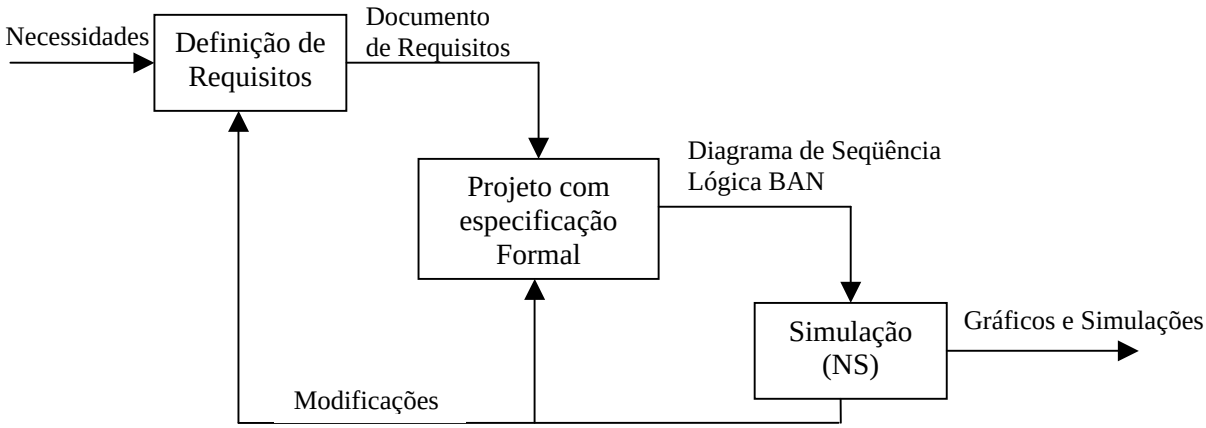


Figura 4.1 - Modelo de desenvolvimento formal em cascata (adaptado de [SOMMERVILLE 2000])

Para a simulação de sistemas, utilizamos o *Network Simulator*, pois permite verificar se o protocolo proposto se comporta como o especificado, sem a necessidade de uma implementação real.

Nosso trabalho não fornece um software que implementa a metodologia proposta, de tal forma que o criador de novos protocolos de segurança deve realizar os processos sugeridos na metodologia de forma passo a passo.

Na Seção 4.2 apresentaremos o projeto com especificação formal, destacando o diagrama de seqüência e a lógica BAN, e na Seção 4.3 discutimos sobre os simuladores existentes, particularmente, o *Network Simulator*.

4.2 PROJETO COM ESPECIFICAÇÃO FORMAL

Depois de definidos os requisitos com texto, o projeto do protocolo proposto na metodologia utilizada consiste na especificação formal utilizando diagramas de seqüência e a lógica BAN.

Métodos formais são bastante utilizados para especificar formalmente protocolos, visando evitar ambigüidades e falhas na especificação, construção, e verificação de tais protocolos.

A utilização de diagramas de seqüências nos permite mostrar visualmente a troca de mensagens entre as entidades envolvidas em um cenário de um protocolo. Ela facilita em uma maior legibilidade do protocolo. Maiores detalhes a respeito de diagramas de seqüência podem ser encontrados em [ANDRADE 2001].

A aplicação de métodos formais na área de criptografia é relativamente recente [MEADOWS 1995] [MEADOWS 2000] e seu objetivo é oferecer uma análise completa do protocolo criptográfico, determinando se os objetivos propostos pelo protocolo são realmente alcançados.

Para a análise de protocolos criptográficos, modelos baseados em lógica modal, que por sua vez utilizam os conceitos de crença e de conhecimento dos participantes do protocolo criptográfico, são utilizados na literatura. Os principais modelos conhecidos são a lógica BAN e a lógica GNY, sendo que a lógica GNY é uma extensão da lógica BAN, porém muito mais complexa, pois possui bem mais regras e é considerada impraticável por alguns autores [GSG 1999].

Por ser mais simples, intuitiva e eficaz, a lógica BAN será utilizada neste trabalho para especificar formalmente nossa proposta. Uma descrição mais detalhada da lógica BAN é mostrada na próxima seção.

4.2.1 LÓGICA BAN

A lógica BAN foi desenvolvida por Burrows, Abadi e Needham para analisar formalmente os protocolos criptográficos, principalmente os protocolos de autenticação e distribuição de chaves [BAN 1990]. Através dela é possível detectar falhas em protocolos bastante conhecidos, como os de *Needham-Schroeder*, *Yahalom* e *Kerberos*. É também possível validar novos protocolos propostos, como feito em [AD 1994].

Como toda lógica, BAN possui um conjunto de notações e postulados. Por questões de entendimento foram feitas adaptações às notações das expressões apresentadas em [BAN 1990], e convencionado o seguinte: os participantes de uma comunicação serão identificados pelas letras maiúsculas P, Q e R, enquanto as fórmulas serão representadas pela letra X e Y; a troca de mensagens entre dois participantes é indicada pela notação na Tabela 4.1:

Tabela 4.1 - Notação da troca de mensagens

M*i* A→B	Mensagem, onde *i* é a *i*-ésima mensagem do protocolo

O objetivo da lógica BAN é obter o resultado proposto pelo protocolo através das crenças iniciais dos participantes e o uso dos postulados. Para isso é necessário transformar o protocolo proposto em um idealizado, a partir do qual será possível aplicar postulados.

A lista na Tabela 4.2 mostra como são representados os elementos na notação BAN.

Tabela 4.2 - Notação da lógica BAN

P acredita X	O participante P acredita na fórmula X ou está autorizado a acreditar em X
P recebeu X	O participante P recebeu a mensagem que contem a fórmula X
P disse X	Em algum momento no passado P enviou uma mensagem contendo X
P controla X	P tem jurisdição sobre X. P é uma autoridade sobre X
novo(X)	A fórmula X é nova, isto é, a fórmula X não foi enviada em nenhuma mensagem anterior à execução atual do protocolo
$P \leftrightarrow^{k} Q$:	K é uma chave satisfatória para P e Q. A chave K é apenas conhecida pelas partes comunicantes P e Q ou por alguém em que eles confiam, jamais por outro participante não autorizado
$\Rightarrow^{K} P$	P tem K como sua chave pública. A chave privada de P é representada por K^{-1} e é somente conhecida por P ou por qualquer outra entidade em que P confie
$\{X\}_K$	A fórmula X é cifrada com a chave K

A lógica BAN possui quatro postulados básicos: regra do significado da mensagem (R1), regra da verificação do identificador (R2), regra da jurisdição (R3) e a regra da crença da declaração (R4). Cada uma delas será descrita a seguir com algumas adaptações feitas com o intuito de melhorar a compreensão dos postulados.

(R1) Regra do significado da mensagem

$$\frac{P \text{ acredita } P \overset{k}{\leftrightarrow} Q,\ P \text{ recebeu } \{X\}_k}{P \text{ acredita } Q \text{ disse } X}$$

Essa regra define que se P recebeu uma fórmula X cifrada com a chave K e se P acredita que K é uma chave satisfatória para se comunicar com Q, então P acredita que Q uma vez enviou uma mensagem contendo X.

De forma similar apresentamos a seguinte regra aplicada à chave pública da criptografia de chave assimétrica:

(R1') Regra do significado da mensagem para chave assimétrica

$$\frac{P \text{ acredita } \overset{K}{\Rightarrow} Q,\ P \text{ recebeu } \{X\}_k^{-1}}{P \text{ acredita } Q \text{ disse } X}$$

(R2) Regra da verificação do identificador

$$\frac{P \text{ acredita novo}(X),\ P \text{ acredita } Q \text{ disse } X}{P \text{ acredita } Q \text{ acredita } X}$$

Neste postulado se P acredita que a fórmula X é nova, e P acredita que Q uma vez disse X, então P também acredita que Q acredita em X.

(R3) Regra da jurisdição

$$\frac{P \text{ acredita } Q \text{ controla } X,\ P \text{ acredita } Q \text{ acredita } X}{P \text{ acredita } X}$$

A regra da jurisdição indica que se P acredita que Q tem jurisdição sobre X e P acredita que Q acredita na fórmula X, então P acredita em X.

(R4) Regra da crença da declaração

As regras a seguir são propriedades de fácil compreensão, por isso as descrevemos sucintamente.

(R4a)

$$\frac{\text{P acredita X, P acredita Y}}{\text{P acredita (X,Y)}}$$

Essa regra determina que se P acredita em X, e P também acredita em Y, então P acredita na mensagem que contenha X e Y.

(R4b)

$$\frac{\text{P acredita (X,Y)}}{\text{P acredita X}}$$

Essa regra determina que se P acredita na mensagem que contenha as formulas X e Y, então P acredita em X e também acredita em Y.

(R4c)

$$\frac{\text{P acredita Q acredita (X,Y)}}{\text{P acredita Q acredita X}}$$

Da mesma forma que a regra anterior, se P acredita que Q acredita em X e em Y, então P acredita que Q acredita em X. P também acredita que Q acredita em Y.

(R4d)

$$\frac{\text{P acredita novo(X)}}{\text{P acredita novo(X,Y)}}$$

Essa regra garante que se P acredita que uma fórmula X é nova, então P acredita que a mensagem inteira que contém X é nova.

As crenças de todos os participantes do protocolo podem ser declaradas utilizando essas regras e a notação apresentada anteriormente. Na próxima seção analisaremos um protocolo bastante simples desenvolvido por [BAN 1990], o protocolo *Wide-mouthed-frog*, cujo objetivo é demonstrar o uso da lógica BAN.

4.2.2 VALIDAÇÃO DO PROTOCOLO *WIDE-MOUTHED-FROG* UTILIZANDO LÓGICA BAN

As mensagens do protocolo *Wide-mouthed-frog*, descrito em [BAN 1990], são apresentadas na Figura 4.2 e na Tabela 4.3 com o objetivo de exemplificar o uso da lógica BAN na formalização de protocolos de segurança.

Tabela 4.3 - Protocolo *Wide-Mouthed-Frog*

Mensagem	Conteúdo
1	$A \rightarrow S$: A, $\{T_a, B, K_{ab}\}_{Kas}$
2	$S \rightarrow B$: $\{T_a, B, K_{ab}\}_{Kbs}$

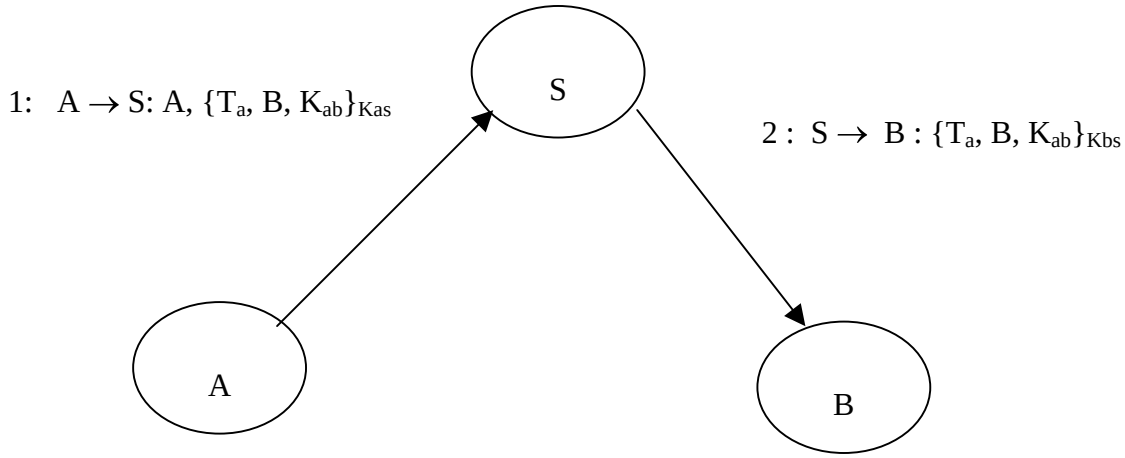


Figura 4.2 - Protocolo *Wide-mouthed-frog* (adaptada de [BAN 1990])

Segundo o protocolo *Wide-mouthed-frog*, o participante A envia uma chave de sessão e um *timestamp* T_a para S, uma entidade confiada por A e por B, ou seja, é uma terceira parte confiável. S então verifica se a mensagem é recente através do T_a e, caso seja, envia a mensagem

para B adicionado do seu próprio *timestamp* T_s. B, por sua vez, verifica se o T_s é o mais recente que ele possui vindo de S. Como todos os *timestamps* são verificados ou gerados por S, então cada participante só necessita estar sincronizado com S.

A partir do protocolo original é necessário obter o protocolo idealizado, como apresentado na Tabela 4.4.

Tabela 4.4 - Mensagens do protocolo idealizado

Mensagem	Conteúdo
1	S recebeu $\{T_a, (A \leftrightarrow^k B)\}_{Kas}$
2	B recebeu $\{T_a$, A acredita $(A \leftrightarrow^k B)\}_{Kbs}$

O objetivo do protocolo é fazer com que A e B acreditem na chave $(A \leftrightarrow^k B)$. Para isso, inicialmente, são capturadas as suposições iniciais (de forma implícita ou explicitamente) e aplicado os postulados da lógica BAN. Esse procedimento é repetido até que se alcance o objetivo proposto.

Existem nove suposições para esse protocolo, como apresentado na Tabela 4.5.

Tabela 4.5 - Suposições iniciais do protocolo *Wide-mouthed-frog*

Suposição	Descrição da Suposição
S1	A acredita $A \leftrightarrow^k S$
S2	S acredita $A \leftrightarrow^k S$
S3	B acredita $B \leftrightarrow^k S$
S4	S acredita $B \leftrightarrow^k S$
S5	A acredita $A \leftrightarrow^k B$
S6	S acredita novo(T_a)
S7	B acredita novo(T_s)
S8	B acredita (A controla $A \leftrightarrow^k B$)
S9	B acredita (S controla (A acredita $A \leftrightarrow^k B$))

As quatro primeiras suposições (S1 a S4) são garantias que tanto A como B possuem uma chave simétrica com S e que confiam nessa chave. Pela descrição do protocolo *Wide-mouthed-*

frog, quem gera a chave entre A e B é A, então A acredita nessa chave. Por isso, tem-se a suposição S5. No protocolo, todos os participantes devem ter seus relógios sincronizados com S. Dessa forma, S acredita que T_a é novo e B acredita que T_s é novo também, como mostra as suposições S6 e S7. Como A cria a chave $A \leftrightarrow^{k} B$ e B confia que A possa criar essa chave, então B acredita que A tem jurisdição sobre essa chave, como mostra a suposição S8. A última suposição mostra que B acredita que S tem jurisdição sobre a crença que A acredita em $A \leftrightarrow^{k} B$.

Como comentamos anteriormente, o objetivo desse protocolo é fazer com que A e B acreditem em $A \leftrightarrow^{k} B$. Por S5 é alcançada a primeira parte do objetivo. Falta provar, então, que B acredita em $A \leftrightarrow^{k} B$. Para isso, será analisada a primeira mensagem do protocolo idealizado presente na Tabela 4.4 e repetido na Tabela 4.6.

Tabela 4.6 - Primeira mensagem do protocolo idealizado

Mensagem	Conteúdo
1	S recebeu $\{T_a, (A \leftrightarrow^{k} B)\}_{Kas}$

Aplicando na mensagem 1 do protocolo idealizado a suposição S1 e a regra do significado da mensagem (R1), temos que S acredita que A disse $(T_a, (A \leftrightarrow^{k} B))$, ou seja:

S acredita A disse $(T_a, (A \leftrightarrow^{k} B))$ (1)

Usando regra da verificação do identificador e a suposição S6 em (1), temos que S acredita que A acredita em $(A \leftrightarrow^{k} B)$, ou seja:

S acredita A acredita $(A \leftrightarrow^{k} B)$ (2)

S então envia a segunda mensagem para B como apresenta a Tabela 4.7.

Tabela 4.7 - Segunda mensagem do protocolo idealizado

Mensagem	Conteúdo
2	B recebeu $\{T_a$, A acredita $(A \leftrightarrow^{k} B)\}_{Kbs}$

Aplicando a suposição S3 na mensagem 2 e a regra do significado da mensagem, temos que B acredita que S disse $(T_a$, A acredita $(A \leftrightarrow^{k} B))$, ou seja:

B acredita S disse $(T_a$, A acredita $(A \leftrightarrow^{k} B))$ (3)

Usando regra da verificação do identificador e a suposição S7 em (3), temos que B acredita que A acredita em ($A \leftrightarrow^{k} B$), ou seja:

B acredita A acredita ($A \leftrightarrow^{k} B$) (4)

Usando a regra da jurisdição e a suposição S8 em (4) temos que:

B acredita ($A \leftrightarrow kB$).

Dessa forma temos que:

A acredita ($A \leftrightarrow^{k} B$) e

B acredita ($A \leftrightarrow^{k} B$), que é justamente a proposta do protocolo. Assim, é provado que o protocolo é válido para o que ele se propõe.

Como mencionado anteriormente e podemos observar com este exemplo, a lógica BAN é bastante simples e fornece meios para especificar e validar um protocolo. Sendo assim, este trabalho usará a lógica BAN para validar a proposta detalhada no Capítulo 5.

4.3 SIMULAÇÃO

A simulação de sistemas é geralmente utilizada quando não é possível realizar experimentos no sistema real devido a alguns obstáculos, como o tempo necessário para a realização do experimento, o alto custo ou a dificuldade de realizar fisicamente o experimento.

As soluções propostas para resolver determinados problemas em redes de computadores podem ser simuladas com o intuito de verificar sua funcionalidade. Através da simulação é possível reproduzir a realidade da rede, possibilitando inserir, excluir ou modificar componentes da rede simulada.

Particularmente, as propostas de segurança para sistemas móveis sem fio são, na maioria, verificadas através de simuladores com suporte para ambientes de rede sem fio. O uso desses simuladores de rede possibilita simular estações base, dispositivos móveis e o canal de rádio que realiza a comunicação com uma rede celular, além de permitir especificar parâmetros para simulação, como por exemplo, o número de usuários na célula, a quantidade de canais disponíveis e outras características fundamentais para o funcionamento da rede em questão. Após a execução de uma simulação, a análise dos resultados gera conclusões a respeito do ambiente sendo simulado. Essa tarefa é facilitada através do uso de ferramentas gráficas (e.g., *Network Animator* [NAM 2003]*).*

4.3.1 SIMULADORES DISPONÍVEIS

Vários simuladores estão disponíveis para verificar redes de computadores tradicionais (i.e., fixas e com fio), bem como redes móveis e sem fio. A seguir descreveremos alguns deles, como OMNET++, OPNET, GloMoSim e *Network Simulator*. Uma lista mais exaustiva de simuladores disponíveis podem ser encontrada em [SIMUL 2003].

OMNeT++ [OMNET 2003] é uma ferramenta de domínio público implementado em C, para a simulação de eventos discretos orientados a objeto. Ela é baseada em componentes e oferece interface gráfica e animação. Pode ser instalado em sistemas Unix, Linux e Windows e já é bastante utilizada pela comunidade científica. OMNeT++ é utilizada, por exemplo, para a modelagem de protocolos de comunicação, bem como para a modelagem de tráfego em redes de computadores.

OPNET [OPNET 2003] é um pacote de produtos que permite projetar, desenvolver, gerenciar e simular a infra-estrutura, os equipamentos e as aplicações de uma rede de computadores. Ele também oferece editor gráfico e animação da simulação. OPNET é um simulador comercial.

GloMoSim [GLOMOSIM 2003] é um ambiente de simulação escalável para redes com fio e que também suporta protocolos para redes puramente sem fio. Atualmente está em desenvolvimento, mas existe uma versão comercial denominada QualNet.

Network Simulator (NS) [NS 2003] é um simulador de eventos discretos, voltado para o desenvolvimento de pesquisas em redes de computadores. Foi projetado inicialmente em 1989 e é escrito em C++ e Otcl (i.e., versão orientada a objeto da linguagem tcl). A idéia de se utilizar essas duas linguagens de programação advém da necessidade de se ter um ambiente que permita, eficientemente, desenvolver protocolos e manipular estruturas de dados (utilizando a linguagem C), bem como possibilite a configuração rápida dos parâmetros da simulação (utilizando Otcl).

Neste trabalho utilizaremos o *Network Simulator* para simular nossa proposta devido aos seguintes fatores: possuir código de domínio público, ou seja, aberto para estudo e modificação; ter um alto poder e versatilidade para criação de novos módulos, mesmo apresentando complexidade no desenvolvimento de tais módulos; ser bastante difundido no meio acadêmico e alvo de diversas pesquisas, como as realizadas pelo Grupo de Redes e Sistemas Distribuídos do Departamento de Computação da UFC (http://www.lia.ufc.br/~great); por fim, disponibiliza

módulos para simular os protocolos MIP e CIP, utilizados nesse trabalho. Na próxima seção apresentamos maiores detalhes sobre o *Network Simulator*.

4.3.2 NETWORK SIMULATOR

Como mencionado na Seção 4.2.1, os módulos do NS são escritos em C++ e Otcl. C++, por ser uma linguagem de grande desempenho, torna-se ideal para a implementação de protocolos detalhados que utilizem grandes conjuntos de dados. No entanto, C++ não é adequado para implementar as mudanças rápidas dos parâmetros das simulações, pois seu processo de compilação, retirada de erros, e execução é lento. Por isso, necessita-se de uma linguagem baseada em scripts, como Otcl, para flexibilizar e facilitar as mudanças dos parâmetros de simulação. No entanto, por ser uma linguagem interpretada, Otcl é bem mais lenta que C++.

O acoplamento entre C++ e Otcl é realizado através da linguagem tclcl, que é um conjunto de módulos específicos que acompanha o NS. Através de tclcl, uma classe escrita em C++ pode ser instanciada usando-se código Otcl, e qualquer parâmetro modificado nesse código Otcl será refletido no objeto C++ instanciado. O código fonte básico do NS foi desenvolvido em C++, mas grande parte dos módulos utilizados para tecnologias específicas de rede foi desenvolvida em Otcl. A Figura 4.1 mostra a arquitetura geral do NS.

Através do NS podem-se simular quase todos os tipos de redes locais. Além disso, existem módulos que simulam qualidade de serviço, comunicação *multicasting* e a pilha completa do protocolo TCP/IP. Com o crescimento de pesquisas em redes sem fio, também foram incluídos módulos para protocolos de roteamento *ad-hoc*, *Mobile IP*, *Satellite networking* e difusão direcionada. Além disso, possui a facilidade de *tracing*, que é a coleta e registro de dados de cada evento da simulação para análise posterior. Outras facilidades disponíveis são: visualizador gráfico para animações da simulação (nam – *network animator*); *timers* e escalonadores, modelos de simulação de erros e ferramentas de matemáticas (e.g., gerador de números aleatórios); ferramenta de plotagem, o *xgraph*; Por fim, vários geradores de trafego.

Após a criação do script em Otcl resta executá-lo no NS e analisar os resultados gerados pelos registros de cada evento simulado. Como apresentado no capítulo 5.

4.3.2.1 CRIANDO SIMULAÇÕES

Nessa seção apresentamos o processo de criação de uma simulação no NS baseada em [NS 2003]. De uma forma geral, para criar uma simulação é necessário escrever um script Otcl contendo as seguintes partes:

- Criação do escalonador de eventos;
- Abertura de arquivos para *tracing* e análise posterior;
- Criação da topologia de rede (i.e., criação de nós e conexão entre eles);
- Criação dos agentes da camada de transporte e a sua conexão com os nós;
- Criação dos geradores de tráfego e a sua conexão com os agentes da camada de transporte;
- Encerramento da simulação, animação e geração de estatísticas.

No caso de simulações de protocolos como o MIP utilizado nesse trabalho, apenas os itens citados anteriormente são necessários. No entanto, simulações mais complexas podem ser realizadas como apresentado em [NS 2003]. A seguir detalhamos cada uma dessas atividades.

4.3.2.1.1 Criação do escalonador de eventos

Como NS é um simulador de evento discreto, ele necessita de um escalonador para controlar os eventos. Esse escalonador é definido no início do script Otcl através do comando:

set ns [new simulator]

Os eventos são armazenados na fila de eventos e estão na ordem de seus tempos de execução. Após a criação do escalonador, podem-se acrescentar eventos através do comando:

$ns at <tempo><evento>, onde <tempo> é o momento para ser disparado o evento <evento>.

Para iniciar o escalonador usa-se o comando $ns run.

4.3.2.1.2 Abertura de arquivos para *tracing*

Para que uma simulação seja de alguma utilidade, é necessário que ao final das simulações se tenha resultados para se fazer análises. O NS registra todos os pacotes que passam por todos os *links* através do comando:

$ns trace-all [open saída.tr w], onde saída.tr é o arquivo que armazenara os registros e 'w' significa que o arquivo é aberto para escrita. Também é possível registrar apenas *links* específicos, como por exemplo, para registrar o tráfego entre dois nós (no1 e o no2) utiliza-se o comando:

$ns trace-queue $no1 $no2.

Todos os comandos de registro devem aparecer após a criação do escalonador.

4.3.2.1.3 Criação da topologia de rede

Após as configurações iniciais descritas nas seções anteriores, é necessário criar a topologia da rede, que consiste nos nós e as conexões entre esses nós. Para criar um nó denominado *nodename*, utiliza-se o comando:

set *nodename*[$ns node]

Por sua vez, para criar um *link* entre o no1 e o no2, com uma largura de banda especificada por <*Largura de banda*>, um *delay* especificado por<*delay*> e um tipo de fila a ser usado pelos nós definido por <*Tipo da Fila*>. Utilize o comando:

$ns duplex-link $no1 $no2 <Largura de banda><delay><Tipo da Fila>

Os tipos de fila que podem existir nos nós do NS para armazenar os pacotes até poderem ser transmitidos são: DropTail, RED, CBQ, FQ, SFQ, DRR.

Um exemplo de criação de um *link* entre os nós no1 e no2 com largura de banda de 5 M e *delay* de 2 ms e utilizando o tipo de fila DropTail é:

$ns duplex-link $no1 $no2 5Mb 2ms DropTail.

4.3.2.1.4 Criação dos agentes da camada de transporte

Nessa seção, é ilustrado como criar agentes da camada de transporte. O NS disponibiliza os seguintes agentes emissores unidirecionais: *Tahoe*, *Reno*, *NewReno*, *Sack*, *Vegas* e *Fack*.

Para criar um novo agente que envia pacotes usando o protocolo TCP utiliza-se à linha de comando:

$set tcp[new Agent/TCP]

Da mesma forma, para criar agentes que recebem pacotes TCP tem-se:

$set tcpsink[new Agent/TCPSink]

É necessário realizar uma ligação entre o agente emissor e o nó do modelo através do comando:

$ns attach-agent $no1 $tcp

Igualmente, é necessário realizar uma ligação entre o agente receptor e o nó:

$ns attach-agent $no2 $tcpsink

Por fim, basta conectar o agente emissor com respectivo receptor:

$ns connect $tcp $tcpsink

4.3.2.1.5 Criação dos geradores de tráfego

Após definirmos os agentes que atuarão na camada de transporte, é necessário criar o tráfego que será executado sobre esses agentes. No NS existem vários tráfegos disponíveis (e.g., FTP, Telnet e CBR).

Por exemplo, para criar um tráfego FTP utiliza-se o comando:

$set ftp[new Application/FTP]

E para conectá-lo ao agente:

$ftp attach-agent $tcp

Da mesma forma é a criação de outros tráfego disponíveis no NS.

4.3.2.1.6 Encerramento da simulação

Por fim, é necessário fechar os arquivos abertos para registrar os eventos. Para isso é utilizado o comando:

close saída.tr

O arquivo fechado deve ser o mesmo que foi aberto no início da simulação. Também é possível nesse último momento da simulação executar comandos para mostrar os resultados através de animadores gráficos (nam) e ferramentas de plotagem (*xgraph*).

4.3.2.2 EXEMPLO DE SIMULAÇÃO

Nessa seção mostramos um *script* que possui cinco nós (no0, no1, no2, no3 e no4), e três *links* (n0-n1, n1-n2 e n2-n3). Também será atribuído um tráfego FTP partindo do no0 ao no3 e que inicia no tempo 1.1s. A duração da simulação é de 2 segundos e ao final será feita uma chamada à ferramenta *network animator* sobre o resultado da simulação, armazenado no arquivo saída.nam. As linhas iniciadas com # são comentários.

```
#Cria Escalonador
Set ns[new Simulator]
#Habilita registro
$ns trace-all [open saída.tr w]
#Habilita registro para ser visualizado no nam
$ns namtrace-all [open saída.nam w]
#Cria Nós
set n0 [$ns node]; set n1 [$ns node]; set n2 [$ns node]; set n3 [$ns node]; set n4 [$ns node]
#Cria links
$ns duplex-link $n0 $n1 5Mb 2ms DropTail
$ns duplex-link $n1 $n2 1.5Mb 10ms DropTail
$ns duplex-link $n2 $n3 5Mb 2ms DropTail
#Cria agentes TCP e os conecta
set tcp[new Agent/TCP]
set tcpsink[new Agent/TCPSink]
$ns attach-agent $n0 $tcp
$ns attach-agent $n3 $tcpsink
$ns connect $tcp $sink
#Cria Tráfego e amarra ao agente
set ftp [new Application/FTP]
$ftp attach-agent $tcp
#configura o tempo inicial do tráfego
$ns at 1.1 “$ftp start”
#finaliza simulação
$ns at 2.0 “finish”
Proc finish{}{
        Global ns
        Puts “Executando nam…”
        Exec nam saida.nam &
        Exit 0
}
$ns run
```

4.4 CONCLUSÃO

Neste capítulo, apresentamos a metodologia a ser utilizada no desenvolvimento da nossa proposta, incluindo a lógica BAN, que é um método formal para especificação de protocolos de segurança, e os simuladores de redes disponíveis existentes, com foco para o *Network Simulator*, utilizado nesta dissertação. No capítulo seguinte detalharemos o funcionamento da entidade de autenticação proposta nessa dissertação.

CAPÍTULO 5 AS – UM AGENTE DE SEGURANÇA PARA AUTENTICAÇÃO DE DISPOSITIVOS MÓVEIS

Esse capítulo apresenta uma proposta para otimizar a autenticação de *Mobile Nodes* enquanto estão se movimentando entre áreas de micromobilidade. Para alcançar esse objetivo, adicionamos uma nova entidade funcional, denominada de *A*gente de Segurança (AS), cuja principal responsabilidade é autenticar os MNs de forma rápida e quase independente do *Home Agent*. As seções a seguir realizam o desenvolvimento do protocolo utilizando a metodologia definida no Capítulo 4, que utiliza diagramas de seqüência, lógica BAN e o simulador *Network Simulator*. Por fim, apresentamos os resultados obtidos através das simulações utilizando o *Network Simulator,* comparando o protocolo proposto *versus* o protocolo MIP.

5.1 INTRODUÇÃO

A cada mudança de domínio administrativo realizado por um *Mobile Node,* é necessária uma atualização de registro e uma autenticação com o *Home Agent,* como apresentado no Capítulo 2. Com o intuito de minimizar o número de acessos ao HA para realizar a autenticação de um MN, este trabalho propõe a adição de uma nova entidade funcional denominada de Agente de Segurança (AS), cuja principal função é armazenar informações necessárias para autenticar um MN quando este estiver transitando entre áreas de micromobilidade.

O AS funciona em conjunto com a entidade funcional introduzida em [ALBANO 2004] [AACA 2003], que objetiva minimizar o número de acessos ao HA para registrar um MN. Dessa forma, a junção das duas propostas fornece uma forma rápida de autenticar um MN e de atualizar o registro de localização do mesmo.

Para o desenvolvimento desta proposta utilizaremos a metodologia apresentada no Capítulo 4. Na Seção 5.2 os conceitos e mecanismos de segurança aplicados na nossa proposta são destacados. A Seção 5.3 apresenta a definição de requisitos do protocolo. A Seção 5.4 introduz a especificação e validação formal da nossa proposta com a lógica BAN. Além disso, esta seção detalha a etapa de simulação utilizando o NS, com um cenário em que um MN muda

de domínio de segurança. Em seguida, esta seção mostra a validação e verificação de outro cenário em que um MN continua dentro de um mesmo domínio de segurança. A Seção 5.5 realiza uma análise comparativa entre a nossa proposta integrada à proposta em [ALBANO 2004] e a do *Mobile IP* original.

5.2 MECANISMOS DE SEGURANÇA UTILIZADOS

Para que seja possível realizar a autenticação do usuário, utilizamos o conceito de *Autenticador*, introduzido na especificação do MIP, que é um identificador que possui as informações cifradas com uma chave simétrica conhecida pelas partes comunicantes e que tem como objetivo validar a parte emissora. Dessa forma, cada MN deve conter uma chave compartilhada com o seu *Home Agent*.

Para que não seja possível um ataque por *replay*, um campo contendo o instante atual do sistema (*timestamp*) deve ser adicionado. Assim, ao receber o *Autenticador*, o destinatário deve comparar o *timestamp* com o tempo atual do sistema, aceitando a mensagem caso forem aproximados, e rejeitando caso contrário. Dessa forma, o *Autenticador* pode ser usado apenas uma vez. É necessário, então, que haja constante sincronização entre as partes comunicantes. Outra maneira de combater ataques por *replay* é através de identificadores, que são valores randômicos gerados e enviados pelo emissor, e que devem ser retornados pelo receptor ao emissor.

Os conceitos de tempestividade e criptografia de chave pública ou assimétrica são também utilizados nesta proposta para garantir a autenticação. Tempestividade é a característica de uma mensagem ter sido gerada recentemente e é utilizada para evitar que mensagens antigas sejam reutilizadas. A forma de verificar a tempestividade é através de *timestamps*.

No decorrer desse capítulo adotaremos a estrutura das mensagens da seguinte forma:

$$\text{Mensagem m Origem} \rightarrow \text{Destino: campo}_1,\text{campo}_2,.....,\text{campo}_n$$

onde m designa o número, em ordem crescente, de uma mensagem enviada de Origem para Destino e cujos campos são $\text{campo}_1,\text{campo}_2,.....,\text{campo}_n$. O símbolo “,” é usado para representar a concatenação dos campos da mensagem.

5.3 DEFINIÇÃO DE REQUISITOS

Nessa seção apresentamos os requisitos para a proposta de autenticação dessa dissertação. Inicialmente, introduzimos o conceito de domínio de segurança para denominar uma área constituída por um conjunto de domínios administrativos próximos e que tenham uma relação de confiança com o Agente de Segurança responsável por essa área. O AS é o responsável pela autenticação dos MNs que estejam dentro de um domínio de segurança. Toda requisição de autenticação de MNs visitantes deve, obrigatoriamente, passar pelo AS.

O objetivo desses domínios de segurança é permitir que um MN visitante possa se deslocar entre os domínios administrativos de um mesmo domínio de segurança sem a constante necessidade de realizar autenticação com o seu HA. A autenticação é tratada localmente dentro de cada domínio de segurança. No entanto, o primeiro pedido de autenticação realizado por um MN visitante dentro de um domínio de segurança deve ser encaminhado para o *Home Agent*, que deve realizar a autenticação de acordo com a especificação do MIP. Isso ocorre devido à falta de informações de segurança necessárias para realizar a autenticação localmente neste cenário inicial. Logo após essa autenticação inicial, o AS responsável pelo domínio de segurança tem permissão e informações para assumir a tarefa de autenticação desse móvel até que o tempo de validade dessa permissão tenha expirado.

Após conhecer o domínio em que se encontra, o MN visitante transmite uma solicitação de autenticação ao AS através do *gateway* do domínio administrativo. Essa solicitação deve possuir um identificador do tipo de mobilidade que o MN executou, de tal forma que o AS possa receber e distinguir o tipo de mobilidade realizada pelo MN: mobilidade interna ao domínio de segurança ou mobilidade entre domínios de segurança. Se o domínio administrativo no qual o MN solicitou a autenticação pertencer a um domínio de segurança diferente do domínio onde o terminal estava anteriormente, a solicitação deve ser transmitida e tratada pelo seu *Home Agent*. Entretanto, se o MN entrar em um domínio administrativo que pertença a um domínio de segurança igual ao anterior, o AS já deve possuir informações de autenticação.

Uma conseqüência direta dessa proposta é a diminuição das mensagens enviadas para os *Home Agents,* que podem estar geograficamente distantes. Essa redução de acessos ao HA acarreta na diminuição do tempo de resposta da solicitação de autenticação, pois o pedido é tratado localmente pelo AS.

Para cada domínio de segurança deve existir pelo menos um AS, no entanto, pode-se configurar um número maior de AS para um mesmo domínio de segurança, de tal forma que se um AS deixar de funcionar um outro poderá substituí-lo automaticamente. Ou ainda, o gerente do domínio de segurança pode determinar um balanceamento de carga entre os Agentes de Segurança.

Se, no entanto, houver apenas um AS em um domínio de segurança e este venha a não funcionar por quaisquer motivos, o processo de autenticação será afetado naquele domínio. Nossa proposta será feita considerando apenas um AS para cada domínio de segurança, e consideramos como um trabalho futuro à especificação e implementação do uso de mais de um AS para cada domínio de segurança.

No restante desta dissertação utilizaremos o *Mobile IP* versão 4 para realizar a especificação formal e simulação da nosso proposta. Isso é justificado pela disponibilidade de módulos estáveis implementados no simulador NS para MIPv4.

5.4 PROJETO COM ESPECIFICAÇÃO FORMAL E SIMULAÇÃO

Nessa seção apresentamos o projeto formal do protocolo proposto nesta dissertação. O projeto do protocolo foi dividido em duas partes: arquitetura e comportamento funcional. Na seção 5.4.1, ilustramos a arquitetura da rede *Mobile IP* com a inserção da nova entidade funcional, o Agente de Segurança. Na Seção 5.4.2 apresentamos a especificação formal da proposta com diagramas de seqüência e lógica BAN, bem como a simulação utilizando o NS. Os seguintes cenários são especificados e simulados: autenticando em um novo domínio de segurança e autenticando em um mesmo domínio de segurança.

5.4.1 ARQUITETURA

A Figura 5.1 ilustra a arquitetura da Internet móvel adicionada da entidade funcional Agente de Segurança (AS).

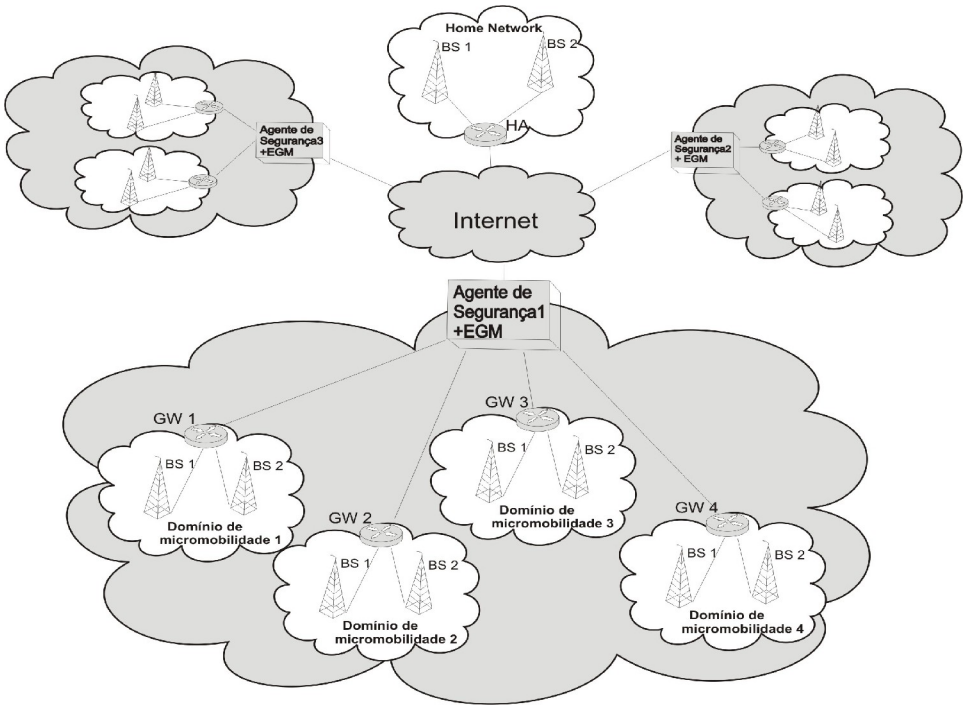


Figura 5.1 - Arquitetura da rede MIP com Agente de Segurança

Esta arquitetura é composta por domínios de segurança, onde cada domínio de segurança é constituído por um conjunto de domínios administrativos e um agente de segurança, responsável pela autenticação dos MNs que estejam dentro de um domínio de segurança. Toda requisição de autenticação de MNs visitantes deve, obrigatoriamente, passar pelo AS. Por trás desta arquitetura, existe o protocolo para realizar o processo de autenticação do MN, que consiste em um conjunto de mensagens que será descrito na Seção 5.4.2.

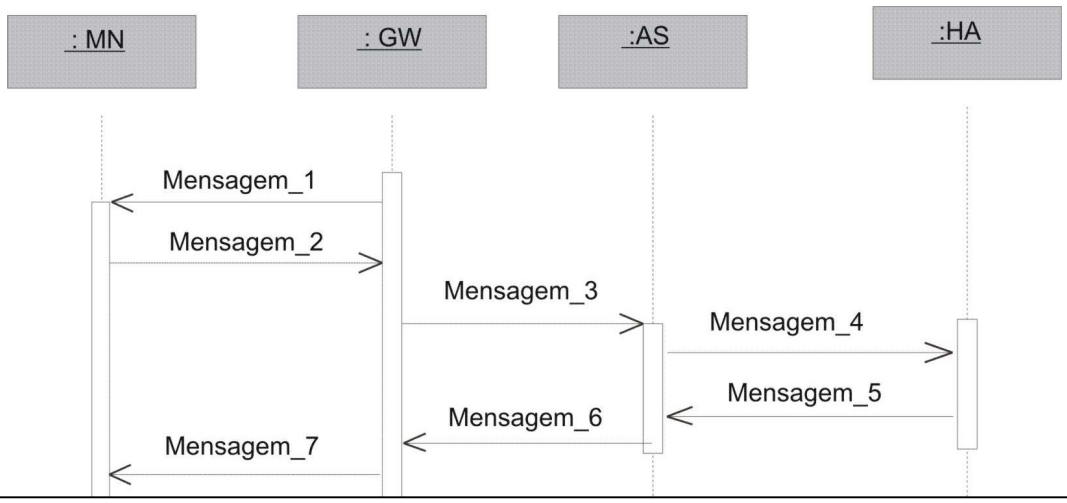
5.4.2 COMPORTAMENTO FUNCIONAL

O protocolo proposto realiza a autenticação de um MN em dois cenários possíveis: o primeiro ocorre quando um MN está mudando de domínio de segurança, como descrito na Seção 5.4.2.1; o segundo acontece quando o móvel se desloca dentro do mesmo domínio de segurança, como apresentado na Seção 5.4.2.2. Em cada cenário será apresentada a seqüência das mensagens trocadas entre as entidades participantes, através dos Diagramas de Seqüência, e a especificação formal através da lógica BAN.

5.4.2.1 AUTENTICANDO UM NOVO DOMÍNIO DE SEGURANÇA

Nessa seção explicaremos em detalhes o funcionamento do processo de autenticação de um MN ao entrar em um domínio administrativo pertencente a um domínio de segurança diferente daquela que servia o domínio administrativo anterior. O processo envolve o *Home Agent*, visto que o Agente de Segurança do domínio visitante inicialmente não possui informações necessárias para validar a identidade do usuário.

Serão apresentadas, nessa seção, as estruturas dos anúncios (Mensagem_1) e das mensagens de solicitação (Mensagem_2, Mensagem_3 e Mensagem_4) e resposta (Mensagem_5, Mensagem_6 e Mensagem_7) do processo de autenticação. A Figura 5.2 apresenta o diagrama de seqüência especificando o protocolo. O significado das mensagens será explicado nas subseções a seguir.



Mensagem_1 GW→MN: A_G, ID_{AS}, T_G

Mensagem_2 MN→GW: Aut_tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, T_{MN}, *Autenticador*,onde *Autenticador*: $K_{MN-HA}[ID_{HA}, ID_{AS}$, Hadd, $T_{MN}]$

Mensagem_3 GW→AS: $KP_{GW}[KU_{AS}$[Aut_Tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, *Autenticador*, $T_{GW}]]$,onde *Autenticador*: $K_{MN-HA}[ID_{HA}, ID_{AS}$, Hadd, $T_{MN}]$

Mensagem_4 AS→HA: $KP_{SA}[KU_{HA}$[Hadd, ID_{AS}, ID_{HA}, T_{AS}, K_{MN-HA}[Hadd,ID_{AS}, ID_{HA}, $T_{AS}]]]$

Mensagem_5 HA→AS: $KP_{HA}[KU_{AS}$[status, T_{HA} ,K_{MN-AS}, $ID_{AS}]$, $K_{MH\_HA}[K_{MN-AS}$, $T_{HA}]]$

Mensagem_6 AS→GW: $KP_{AS}[KU_{GW}$[status, $K_{MH\_HA}[K_{MN-AS}$, $T_{HA}]$, $T_{AS}]]$

Mensagem_7 GW→MN: Hadd, ID_{GW}, status, $K_{MH\_HA}[K_{MN-AS}$, $T_{HA}]$, T_{GW}

Figura 5.2 - Solicitação de autenticação de um MN ao mudar de domínio de segurança

5.4.2.1.1 Anúncios

Nessa seção discutiremos as modificações necessárias nas mensagens de anúncio do *Mobile IP* para suportar as características do protocolo proposto nessa dissertação.

A estrutura da mensagem de anúncio é ilustrada na Figura 5.2 e apresentada a seguir:

Mensagem_1 GW→MN: A_G, ID_{AS}, T_G

Um dispositivo móvel descobre em qual domínio administrativo ele se encontra através das mensagens de anúncio emitidas constantemente pelo *gateway* responsável pelo domínio administrativo (ver Capítulo 2). Para simplificar nossa notação, a mensagem de anúncio original do *gateway*, sem os campos adicionais propostos nesse trabalho, é denominada de A_G.

Nossa proposta adiciona, em tais mensagens de anúncios, um identificador, denominado ID_{AS}, informando o Agente de Segurança responsável pelo domínio de segurança em que o MN se encontra. Dessa forma, o anúncio informará ao MN tanto o domínio administrativo quanto o Agente de Segurança responsável pelo domínio de segurança em que ele se encontra.

O identificador ID_{AS} deve ser armazenado no MN ao finalizar um processo de autenticação realizado com sucesso. Essa informação será útil para que o MN seja capaz de saber se houve mudança ou não de domínio de segurança ao receber as mensagens de anúncio, apenas comparando o identificador recebido e o identificador armazenado do processo de autenticação realizado anteriormente.

Também é adicionado um *timestamp* (T_G) para garantir que o anúncio foi enviado recentemente pelo *gateway*.

Esta dissertação assume que os *gateways* conhecem antecipadamente o domínio de segurança do qual eles fazem parte.

5.4.2.1.2 Solicitação de Autenticação/Registro

Esta seção descreve o processo de solicitação de autenticação e atualização de registro de um dispositivo móvel, bem como o formato das mensagens envolvidas nessa solicitação.

Em nossa proposta, o MN, ao entrar em um domínio administrativo e constatar a mudança do domínio de segurança através do identificador do Agente de Segurança (ID_{AS}) contido na mensagem de anúncio, envia ao *gateway* do domínio administrativo visitado uma

mensagem de solicitação de autenticação/atualização de registro. Caso o MN não tenha mudado de domínio de segurança, o processo de autenticação ocorrerá da forma como será abordado na Seção 5.4.2.2.

A mensagem de autenticação/atualização de registro é apresentada a seguir:

$$\text{Mensagem\_2 MN} \rightarrow \text{GW: Aut\_tipo, Hadd, } ID_{AS}, ID_{GW}, ID_{HA}, T_{MN}, \textit{Autenticador}$$

A solicitação contém um campo denominado Aut_tipo, para indicar se o pedido deve ser tratado localmente pelo Agente de Segurança ou deve ser tratado remotamente pelo *Home Agent*. No primeiro caso, o campo Aut_tipo armazena a informação *local*, e no segundo, armazena a informação *remoto*. Como o cenário avaliado nessa seção representa a primeira solicitação dentro de um domínio de segurança, a solicitação deve ser tratada remotamente, e o campo Aut_tipo deve então ter armazenado a informação *remoto*. A mensagem possui também o *Home Address* do MN (Hadd), o identificador do Agente de Segurança responsável pela autenticação do domínio visitado (ID_{AS}), o identificador do *gateway* responsável pela rede sendo visitada (ID_{GW}), o identificador do *Home Agent* (ID_{HA}), que pode ser representado pelo endereço IP do *Home Agent*, um *timestamp* (T_{MN}), e um *Autenticador* para garantir ao *Home Agent* a identidade do usuário.

A partir da informação sobre o tipo de solicitação sendo realizada (i.e., *remoto* ou *local*) constrói-se o campo *Autenticador*. Para o cenário avaliado nessa seção, o A*utenticador* é constituído pelo identificador do *Home Agent* (ID_{HA}), o *Home Address* do MN (Hadd), o identificador do AS (ID_{AS}) e um *TimeStamp* criado pelo MN, denominado de T_{MN}. Todas as informações contidas no *Autenticador* são cifradas com a chave simétrica compartilhada previamente entre o MN e o seu *Home Agent*, sendo essa chave representada por $K_{MN\text{-}HA.}$ A estrutura do *Autenticador* é apresentada a seguir:

$$\textit{Autenticador}: K_{MN-HA}[ID_{HA}, ID_{AS}, \text{Hadd}, T_{MN}]$$

A mensagem de solicitação enviada pelo MN é direcionada ao *gateway* da rede visitada. O *gateway*, por sua vez, encaminha a solicitação ao AS responsável pela gerência de localização e autenticação do domínio administrativo. Essa solicitação contém o *timestamp* (T_{GW}) e a Mensagem_2 enviada pelo MN. Essas informações são cifradas com a chave pública do AS (KU_{AS}) e assinada pelo *gateway* (KP_{GW}), como apresentado na mensagem_3 a seguir:

Mensagem_3 GW→AS: $KP_{GW}[KU_{AS}[Aut\_Tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, Autenticador, T_{GW}]]$

O Agente de Segurança recebe a solicitação e verifica a assinatura do *gateway* através da chave pública do *gateway;* após isso, decifra a mensagem e obtém as informações enviadas.

A informação ID_{AS} permite ao AS verificar se a solicitação de atualização de registro/autenticação foi realmente destinada a ele. Já a informação ID_{GW} confirma a identificação do *gateway* emissor da mensagem. O AS verifica se a mensagem é recente através da informação T_{GW}. A última verificação a ser feita é quanto ao tipo de autenticação a ser realizada. Para o cenário avaliado nessa seção, a autenticação é remota.

Após todas as verificações, o AS encaminha ao *Home Agent* do MN uma mensagem contendo as informações Hadd, ID_{AS}, ID_{HA} e o autenticador. Também é incluído um *timestamp* (T_{AS}). Esta mensagem deve ser cifrada com a chave pública do *Home Agent* (KU_{HA}) e assinada com a chave privada do AS (KP_{AS}). A estrutura da mensagem 4 é apresentada a seguir:

Mensagem_4 AS→HA: $KP_{SA}[KU_{HA}[Hadd, ID_{AS}, ID_{HA}, T_{AS}, K_{MN-HA}[Hadd, ID_{AS}, ID_{HA}, T_{MN}]]]$

Ao receber a solicitação, o *Home Agent* verifica a assinatura do AS através da chave pública do AS e então decifra a mensagem e obtém as informações enviadas pelo AS. Em seguida, o *Home Agent* verifica a identificação do MN que está solicitando a autenticação (Hadd), para saber se esse MN pertence à sua rede, confirma a identidade do AS que enviou a solicitação, verifica se o campo identificador do AS de destino corresponde à sua identificação, e verifica se a mensagem é recente através da informação $T_{AS.}$ O HA obtém as informações contidas no *Autenticador* utilizando a chave simétrica compartilhada com o MN.

Com essas informações, o HA será capaz de certificar que aquela solicitação é destinada a ele, bem como verificar a identidade do móvel que está fora de sua rede. O HA verifica, também, a tempestividade da solicitação através da comparação do seu *timestamp* com os *timestamps* enviados pelos MN (T_{MN}) e o AS (T_{AS}). Esta verificação é necessária para proteger o domínio administrativo contra ataques do tipo *replay*.

5.4.2.1.3 Resposta da Solicitação

Após se certificar da identidade do MN, o HA envia ao AS uma mensagem de resposta à solicitação de autenticação/registro. A mensagem de resposta contém o resultado da solicitação, denominado de *status*, um *timestamp* (T_{AS}), e uma chave de sessão simétrica gerada aleatoriamente pelo HA, para ser usada pelo MN e o AS (K_{MN-AS}), todas cifradas com a chave pública do AS (KU_{AS}). A mensagem também contém a mesma chave de sessão criada pelo HA, cifrada com a chave compartilhada entre o HA e o MN. Para garantir a identidade do emissor, a mensagem será cifrada com a chave privada do HA (KP_{HA}).

A chave de sessão recebida pelo AS também será recebida pelo MN, como será visto posteriormente nesta seção, servindo para autenticar o MN em futuras solicitações dentro do domínio de segurança. Apresentamos na mensagem 5 a estrutura da mensagem de resposta:

$$Mensagem\_5 \quad HA \rightarrow AS: \quad KP_{HA}[KU_{AS}[status, \quad T_{HA} \quad , K_{MN-AS}, ID_{AS}], \; K_{MH\_HA}[K_{MN-AS}, \; T_{HA}]]$$

O AS, ao receber a resposta da solicitação, verifica a assinatura da mensagem utilizando a chave pública do HA. Após a verificação da assinatura, o AS decifra a mensagem com sua chave privada, recuperando o resultado da solicitação, o *timestamp*, a chave de sessão e o identificador do AS (ID_{AS}). Através do ID_{AS}, o AS verifica se a mensagem foi enviada realmente para ele. Por sua vez, através do resultado da solicitação (*status*), o AS verifica se a autenticação do usuário ocorreu corretamente. Além disso, o AS obtém a chave de sessão que será compartilhada com o MN (K_{MN-AS}).

Após a verificação da identidade do móvel, o AS realiza a atualização de registro do móvel e envia ao *gateway* o resultado da solicitação (*status*), a chave de sessão gerada pelo HA cifrada com a chave compartilhada entre o MN e o HA, e o *timestamp* (T_{AS}). Todos esses campos são cifrados com a chave pública do *gateway (*KU_{GW}*)* e assinada pelo AS (KP_{AS}). A estrutura da mensagem é mostrada a seguir:

$$Mensagem\_6 \; AS \rightarrow GW: \; KP_{AS}[KU_{GW}[status, \; K_{MH\_HA}[K_{MN-AS}, \; T_{AS}], \; T_{AS}]]$$

Ao receber a resposta da solicitação, o *gateway* confere a assinatura do AS e decifra a informação utilizando sua chave privada. Em seguida, verifica se o *timestamp* recebido (T_{AS}) é recente. Para saber se a solicitação foi aceita pelo HA, o AS verifica o campo *status*. Após

realizar as devidas verificações, o *gateway* encaminha a resposta da solicitação para o MN, através da Mensagem_7, última mensagem de autenticação apresentada na Figura 5.2, a seguir:

$$\text{Mensagem\_7 GW}\rightarrow\text{MN: Hadd, ID}_{GW}\text{, status, K}_{MH\_HA}[\text{K}_{MN-AS}\text{, T}_{HA}]\text{, T}_{GW}$$

A mensagem contém o identificador do MN (Hadd), o identificador do *gateway* (ID_{GW}), o resultado da solicitação (*status*) e a chave a ser compartilhada pelo MN e o AS.

O MN, ao receber a resposta da solicitação, verifica o identificador do *gateway* que originou a mensagem (ID_{GW}) e o resultado da solicitação (*status*). Se a resposta da solicitação for positiva, o MN recupera a chave de sessão cifrada com a chave compartilhada entre ele e o HA e inicia o uso dos recursos da rede visitada. Caso contrário, o MN toma conhecimento que não foi possível realizar a autenticação através do HA.

5.4.2.1.4 Especificação Formal Usando Lógica BAN

Nesta seção, vamos especificar formalmente o protocolo para o cenário em que o MN está entrando em um novo domínio de segurança (Veja Figura 5.2). Inicialmente, vamos listar as mensagens do protocolo detalhadas nas Seções 5.4.3.1, 5.4.3.2 e 5.4.3.3, substituindo o campo *Autenticador* pelas informações que ele representa:

Mensagem_1 $\text{GW}\rightarrow\text{MN: A}_{G}\text{, ID}_{AS}\text{, T}_{G}$

Mensagem_2 $\text{MN}\rightarrow\text{GW: Aut\_tipo, Hadd, ID}_{AS}\text{, ID}_{GW}\text{, ID}_{HA}\text{, T}_{MN}\text{, K}_{MN-HA}[\text{Hadd, ID}_{AS}\text{, ID}_{HA}\text{, T}_{MN}]$

Mensagem_3 $\text{GW}\rightarrow\text{AS: KP}_{GW}[\text{KU}_{AS}[\text{Aut\_tipo, Hadd, ID}_{AS}\text{, ID}_{GW}\text{, ID}_{HA}\text{, K}_{MN-HA}[\text{Hadd, ID}_{AS}\text{, ID}_{HA}\text{, T}_{MN}]\text{, T}_{GW}]$

Mensagem_4 $\text{AS}\rightarrow\text{HA: KP}_{SA}[\text{KU}_{HA}[\text{Hadd, ID}_{AS}\text{, ID}_{HA}\text{, T}_{AS}\text{, K}_{MN-HA}[\text{Hadd, ID}_{AS}\text{, ID}_{HA}\text{, T}_{MN}]]]$

Mensagem_5 $\text{HA}\rightarrow\text{AS: KP}_{HA}[\text{KU}_{AS}[\text{status, T}_{HA}\text{, K}_{MN-AS}\text{, ID}_{AS}]\text{, K}_{MH\_HA}[\text{K}_{MN-AS}\text{, T}_{HA}]]$

Mensagem_6 $\text{AS}\rightarrow\text{GW: KP}_{AS}[\text{KU}_{GW}[\text{status, K}_{MH\_HA}[\text{K}_{MN-AS}\text{, T}_{HA}]\text{, T}_{AS}]]$

Mensagem_7 $\text{GW}\rightarrow\text{MN: Hadd, ID}_{GW}\text{, status, K}_{MH\_HA}[\text{K}_{MN-AS}\text{, T}_{HA}]\text{, T}_{GW}$

Conforme apresentado no Capítulo 4, para especificar formalmente um protocolo de segurança utilizando a lógica BAN, é necessário obter o protocolo idealizado e a partir dos

postulados e das suposições iniciais alcançar o objetivo a que o protocolo se propõe. A seguir apresentamos as mensagens do protocolo idealizado, desconsiderando as mensagens 1 e 2, pois não utilizam criptografia, ou seja, estão em texto claro:

- Mensagem_3: AS recebeu $\{\{Hadd, T_{MN}, novo(T_{MN})\}_{KMN-HA}, T_{GW,} novo(T_{GW})\}_{KUAS}\}_{KPGW}$
- Mensagem_4: HA recebeu $\{\{Hadd,T_{MN}, novo(T_{MN})\}_{KMN-HA}, T_{AS}, novo(T_{AS})\}_{KUHA}\}_{KPSA}$
- Mensagem_5: AS recebeu $\{\{status, T_{HA}, K_{MN-AS}\}_{KUAS}, \{K_{MN-AS}\}_{KMH\_HA}\}_{KPHA}$
- Mensagem_6 GW recebeu $\{\{status, \{K_{MN-AS}\}_{KMH\_HA}, T_{AS}\}_{KUAS}\}_{KPGW}$
- Mensagem_7 MN recebeu $\{status, K_{MH\_HA}[K_{MN-AS,} T_{HA}], T_{GW}\}$

O objetivo do protocolo é fazer com que MN e AS acreditem na chave K_{MN-AS}. Para isso, capturamos as suposições iniciais e aplicamos os postulados da lógica BAN, até concluirmos que o protocolo alcança o objetivo proposto.

Existem vinte e uma suposições para esse protocolo, como listadas na Tabela 5.1.

Tabela 5.1 - Suposições iniciais para o cenário em que o MN muda de domínio de segurança

Suposição	Descrição da Suposição
S1	MN acredita $MN \leftrightarrow^{k} HA$
S2	HA acredita $MN \leftrightarrow^{k} HA$
S3	AS acredita $\Rightarrow^{K} HA$
S4	HA acredita $\Rightarrow^{K} AS$
S5	GW acredita $\Rightarrow^{K} AS$
S6	AS acredita $\Rightarrow^{K} GW$
S7	AS acredita $\Rightarrow^{K} AS$
S8	GW acredita $\Rightarrow^{K} GW$
S9	HA acredita $\Rightarrow^{K} HA$
S10	HA acredita $MN \leftrightarrow^{k} AS$
S11	AS acredita (HA controla $MN \leftrightarrow^{k} AS$)

S12	MN acredita (HA controla MN$\leftrightarrow^{k}$AS)
S13	HA acredita novo(T_{MN})
S14	HA acredita novo(T_{SA})
S15	AS acredita novo(T_{MN})
S16	AS acredita novo(T_{GW})
S17	AS acredita novo(T_{HA})
S18	GW acredita novo(T_{AS})
S19	MN acredita novo(T_{HA})
S20	MN acredita (HA controla (AS acredita MN$\leftrightarrow^{k}$AS))
S21	AS acredita (HA controla (MN acredita MN$\leftrightarrow^{k}$AS))

As duas primeiras suposições (S1 e S2) garantem que o MN possui uma chave simétrica com o HA e ambos confiam nessa chave. As duas suposições seguintes (S3 e S4) garantem que o Agente de Segurança (AS) confia na chave pública do *Home Agent* e vice-versa. As suposições S5 e S6 garantem que o *gateway* confia na chave pública do AS e vice-versa. As suposições S7, S8 e S9 garantem que as entidades confiam em suas próprias chaves privadas, ou seja, que sua chave privada não é conhecida por outras entidades não autorizadas.

Pelo protocolo proposto, a entidade que gera a chave entre MN e o AS é o HA, então o próprio HA acredita nessa chave, como apresentado na suposição S10. Como o *Home Agent* cria a chave MN$\leftrightarrow^{k}$AS, e o MN e o AS confiam que o HA possa criar essa chave, então MN e AS acreditam que o HA tem jurisdição sobre essa chave, como mostram as suposições S11 e S12.

No protocolo proposto, todos os participantes devem ter seus relógios sincronizados com o HA. Dessa forma, temos as seguintes crenças: o HA acredita que T_{MN} e T_{GW} são novos (S13 e S14); o AS acredita que T_{MN}, T_{GW} e T_{HA} são novos (S15, S16 e S17); o *gateway* acredita que T_{AS} é novo (S18); e, por fim, o MN acredita que T_{HA} é novo (S19).

A suposição S20 mostra que o MN acredita que o HA tem jurisdição sobre a crença que AS acredita em MN$\leftrightarrow^{k}$AS. Por fim, a suposição S21 mostra que o AS acredita que o HA tem jurisdição sobre a crença que o MN acredita em MN$\leftrightarrow^{k}$AS.

Como comentamos anteriormente, o objetivo desse protocolo é fazer com que o MN e o AS acreditem em A$\leftrightarrow^{k}$B. Para alcançarmos esse objetivo, nos itens seguintes vamos analisar

cada mensagem do protocolo idealizado aplicando as regras e as crenças iniciais, até alcançarmos o final desse protocolo:

- **Mensagem_3: AS recebeu {{Hadd, T_{MN}, novo(T_{MN})}$_{KMN-HA}$, T_{GW}, novo(T_{GW})}$_{KUAS}$}$_{KPGW}$**

Inicialmente, aplicamos a suposição S6 e a regra do significado da mensagem (R1), detalhada no Capítulo 4, na Mensagem_3, tendo como resultado:

AS acredita GW disse {Hadd,T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{GW}, novo(T_{GW})}KU_{AS} **(1)**

Na prática, a aplicação dessa regra sobre a mensagem assinada por GW representa a verificação dessa assinatura pelo AS.

Em seguida, aplicando novamente a regra do significado da mensagem (R1) e a suposição S7 em (1) para obter as informações cifradas com a chave pública do AS, temos que:

AS acredita GW disse {{Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{GW}, novo(T_{GW})} **(2)**

Por fim, aplicando a regra da verificação do identificador (R2) e a suposição S16 em (2), temos que:

AS acredita GW acredita {Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}} **(3)**

Ao final da análise da Mensagem_3, podemos concluir que o AS acredita que o GW acredita em {Hadd, T_{MN}, novo(T_{MN})}$_{KMN-HA}$. Dessa forma, o AS pode utilizar essa informação na Mensagem_4 com a segurança de que ela foi enviada pelo GW, e de que é uma informação recente. É importante salientar que o AS não sabe se essa mensagem realmente partiu de um MN válido, isso só vai ser possível quando o HA retornar uma resposta ao pedido da solicitação.

- **Mensagem_4: HA recebeu {{Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{AS}, novo(T_{AS})} KU_{HA}} KP_{AS}**

Aplicando a suposição S4 e a regra do significado da mensagem (R1), para verificar a assinatura do AS, temos que:

HA acredita SA disse {Hadd,T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{AS}, novo(T_{AS})} KU_{HA} **(4)**

Aplicando a suposição S9 e a regra do significado da mensagem (R1), para decifrar a mensagem recebida, temos que:

HA acredita SA disse {Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{AS}, novo(T_{AS})} **(5)**

Aplicando a regra da verificação do identificador e a suposição S14 em (5), temos que:

HA acredita SA Acredita {Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}} **(6)**

Até esse momento, o HA acredita que a mensagem enviada pelo AS foi realmente enviado por ele, e que ela é recente, ou seja, não está sendo reutilizada. Agora, será analisada a mensagem criada e enviada pelo MN, que é parte da mensagem (6).

Aplicando a regra do significado da mensagem (R1) e a suposição S2 na mensagem {Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}}, temos que:

HA acredita MN Acredita {Hadd,T_{MN}, novo(T_{MN})} **(7)**

Aplicando a regra da verificação do identificador e a suposição S13 em (7), temos que:

HA acredita MN Acredita {Hadd} **(8)**

Dessa forma, temos que o HA acredita que a mensagem foi originada pelo MN e é recente. Após essa verificação, o HA atualiza o registro de localização do MN e envia uma mensagem de resposta para o MN, através do AS, contendo uma chave compartilhada (K_{MN-AS}), como mostrada na Mensagem_5 a seguir.

- **Mensagem_5: AS recebeu {{*status*, T_{HA}, K_{MN-AS}}KU_{AS}, {K_{MN-AS}}K_{MH_HA}} KP_{HA}**

  Aplicando a suposição S3 e a regra do significado da mensagem (R1), temos que:

  AS acredita HA disse {{*status*, T_{HA}, K_{MN-AS}}KU_{AS}, {K_{MN-AS}}K_{MH_HA}} **(9)**

  Aplicando a suposição S7 e a regra do significado da mensagem (R1) na primeira parte da mensagem temos:

  AS acredita HA disse {*status*, T_{HA} ,K_{MN-AS}} **(10)**

  Aplicando a regra da verificação do identificador (R2) e a suposição S17 em (10), temos que:

  AS acredita HA acredita{*status*, K_{MN-AS}} **(11)**

  Após verificar que o MN foi autenticado pelo HA, através da informação contida no campo *status*, o AS passa a acreditar na chave a ser compartilhada com o MN (K_{MN-AS}) e envia a

mensagem Mensagem_6 para o *gateway* do domínio de micromobilidade onde se encontra o MN. Caso a informação contida em *status* indique que o MN não foi autenticado, o AS envia uma resposta de solicitação com o campo *status* indicando que a solicitação falhou e sem a chave K_{MN-AS}.

Portanto, a partir da análise de Mensagem_5, podemos alcançar o primeiro objetivo do protocolo proposto: o AS acredita na chave K_{MN-AS} que será compartilhada com o MN.

Continuamos agora o fluxo das mensagens (Mensagem_6 e Mensagem_7) para alcançar o segundo objetivo do protocolo proposto, que é verificar se o MN acredita na chave K_{MN-AS} que será compartilhada com o AS.

- **Mensagem_6 GW recebeu {{status, {K_{MN-AS}}K_{MH_HA}, T_{AS}} KU_{AS}} KP_{GW}**

Aplicando a suposição S8 e a regra do significado da mensagem (R1) para verificar a assinatura do *gateway*, temos que:

$$\text{GW acredita AS disse } \{\{status,\ \{K_{MN-AS}\}K_{MH\_HA},\ T_{AS}\}\ KU_{AS}\} \textbf{ (12)}$$

Aplicando a suposição S5 e a regra do significado da mensagem (R1) para decifrar a mensagem recebida, temos que:

$$\text{GW acredita AS disse } \{status,\ \{K_{MN-AS}\}_{KMH\_HA},\ T_{AS}\} \textbf{ (13)}$$

Aplicando a regra da verificação do identificador (R2) e a suposição S18 em (13), temos que:

$$\text{GW acredita AS acredita } \{status,\ \{K_{MN-AS}\}K_{MH\_HA}\} \textbf{ (14)}$$

Ao chegar no passo (14), o GW já conhece o resultado da solicitação de autenticação e possui uma informação que contém a chave a ser enviada para o MN, caso o MN seja autenticado corretamente. Essa chave será utilizada pelo MN e AS em futuras solicitações de autenticação dentro do mesmo domínio de segurança. O *gateway* então envia uma mensagem para o MN que contém a chave K_{MN-AS}, como mostrado na Mensagem_7, a seguir.

- **Mensagem_7 MN recebeu {status, K_{MH_HA}[K_{MN-AS}, T_{HA}], T_{GW}}**

Através dessa mensagem, o MN recebe a chave que será utilizada para realizar futuras autenticações dentro do domínio de segurança. Inicialmente, será verificado o *timestamp* enviado pelo *gateway* (T_{GW}) para examinar se a mensagem é recente. Também é verificado o resultado da

solicitação de autenticação através do campo *status* enviado na mensagem. Caso a autenticação tenha sido feita corretamente o MN obtém a chave K_{MN-AS} como provado a seguir:

Aplicando a suposição S1 e a regra do significado da mensagem (R1), temos que:

MN acredita HA disse K_{MN-AS}, T_{HA} **(15)**

Aplicando a regra da verificação do identificador e a suposição S19, temos que:

MN acredita HA acredita K_{MN-AS} **(16)**

O que implica que o MN acredita que a chave K_{MN-AS} foi enviada pelo HA, ou seja:

HA acredita K_{MN-AS}

Desta forma, temos ao final dessa análise da troca de mensagens que:

AS acredita K_{MN-AS} e

HA acredita $K_{MN-AS,}$ que são os objetivos do protocolo proposto.

Portanto, o MN foi autenticado pelo HA, que passou informações de segurança para o AS, para que não seja necessário realizar todo esse processo quando o MN necessitar realizar autenticação dentro do mesmo domínio de segurança; além disso, o MN acredita que foi autenticado pelo o seu verdadeiro HA.

5.4.2.1.5 Simulação

Nessa seção apresentamos a simulação do processo de autenticação de um MN ao mudar de domínio de segurança, ou seja, o MN sai de um domínio administrativo D1 que faz parte de um domínio de segurança S1 e entra em um domínio administrativo D2 componente de um domínio de segurança S2. Como vimos anteriormente, esse cenário envolve o *Home Agent*, visto que o Agente de Segurança do domínio visitante inicialmente não possui informações necessárias para validar a identidade do usuário.

Para essa simulação, foram desenvolvidos módulos de atualização de registro local, proposto por [ALBANO 2004] [AACA 2003], e de autenticação, resultado dessa dissertação.

As Figuras 5.3, 5.4, 5.5., e 5.6 ilustram a simulação desse cenário utilizando o *Network Simulator* e o ambiente de animação gráfico NAM, vistos no Capítulo 4. A notação utilizada para representar os nós da simulação é a seguinte:

- HA - *Home Agent* do MN
- RI - Roteadores Internos pertencentes à Internet

- GW – *gateway* responsável por um domínio administrativo. Nesse trabalho referenciamos o *gateway* como sendo o próprio domínio administrativo, para fins de facilitar a escrita dessa dissertação.
- AS - Agente de Segurança responsável pelos domínios administrativos GW0, GW1, GW2 e GW3.
- MN - *Mobile Node*

A simulação consiste nos seguintes elementos: o dispositivo móvel (MN) que realiza comunicação com a rede sendo visitada; um *Home Agent*, responsável pelo gerenciamento de localização do MN; um Agente de segurança, cuja função é autenticar o MN dentro de um domínio de segurança; cinco roteadores internos cujo único intuito é representar a Internet; e seis *gateways* representando os domínios administrativos.

Na Figura 5.3, os nós com rótulos 9, 10,11 e 12 (destacados por uma elipse) simulam *gateways* de domínios administrativos e formam um domínio de segurança gerenciado pelo AS, representado pelo nó 5. Os nós com rótulo 8 e 13, por sua vez, representam *gateways* de domínios administrativos que não fazem parte de nenhum domínio de segurança. Eles são usados para simular a mudança de um ambiente sem domínio de segurança para um outro que possui. É importante perceber que esta proposta não obriga os domínios administrativos a participarem de um domínio de segurança.

Os nós com rótulos 0, 1, 2, 3 e 4 representam roteadores e possuem a única função de representar a Internet. Por fim, o MN é representado pelo nó 6 possui o papel de percorrer os domínios administrativos e receber informações oriundas do HA. Nessa simulação não é implementada a proposta de otimização de rota, vista na Seção 2.3.1.2, de forma que toda a comunicação destinada ao MN deve ser recebida e repassada pelo HA. No entanto, isso não prejudica os resultados da nossa simulação, visto que a fonte onde se originam os dados enviados para o MN é indiferente para este trabalho.

Para mostrar que a autenticação e a atualização de registro foram realizadas com sucesso, criamos um fluxo de dados contínuo CBR (*Constant Bit Rate*) entre o HA e o MN. Esse fluxo também será útil para analisarmos a taxa de perda de pacotes quando o MN muda de domínio administrativo e permanece dentro de um mesmo domínio de segurança, como veremos na Seção 5.5.

As mensagens descritas anteriormente nesse capítulo são ilustradas na simulação através de pacotes, como mostra a Figura 5.3. Na parte inferior da figura são apresentadas mensagens indicativas do processo de autenticação, com o intuito de facilitar o entendimento de cada passo da simulação. Uma última observação a ser feita é sobre os rótulos inseridos na parte superior dos nós para indicar o tipo de elemento na simulação e seu endereço hierárquico. A seguir ilustramos e detalhamos o fluxo das mensagens.

A primeira mensagem da simulação desse cenário acontece quando um MN é ligado ou está entrando em domínio administrativo. Escolhemos o domínio administrativo que é gerenciado pelo *gateway* GW1, por pertencer ao domínio de segurança, mas poderia ser qualquer domínio administrativo. No primeiro momento, o MN cria uma solicitação de autenticação e envia ao *gateway*, que, por sua vez, após realizar as verificações necessárias, envia a solicitação ao AS, como ilustrado na Figura 5.3. A solicitação está representada pelo pacote menor entre os roteadores com rótulos 0 e 2. Na parte inferior da figura apresentada uma mensagem indicando que o MN enviou uma solicitação de autenticação/atualização de registro para o GW1 (CoA:0.8.0) com um *autenticador*. As outras duas mensagens indicam que o *gateway* GW1 atualizou sua tabela de roteamento.

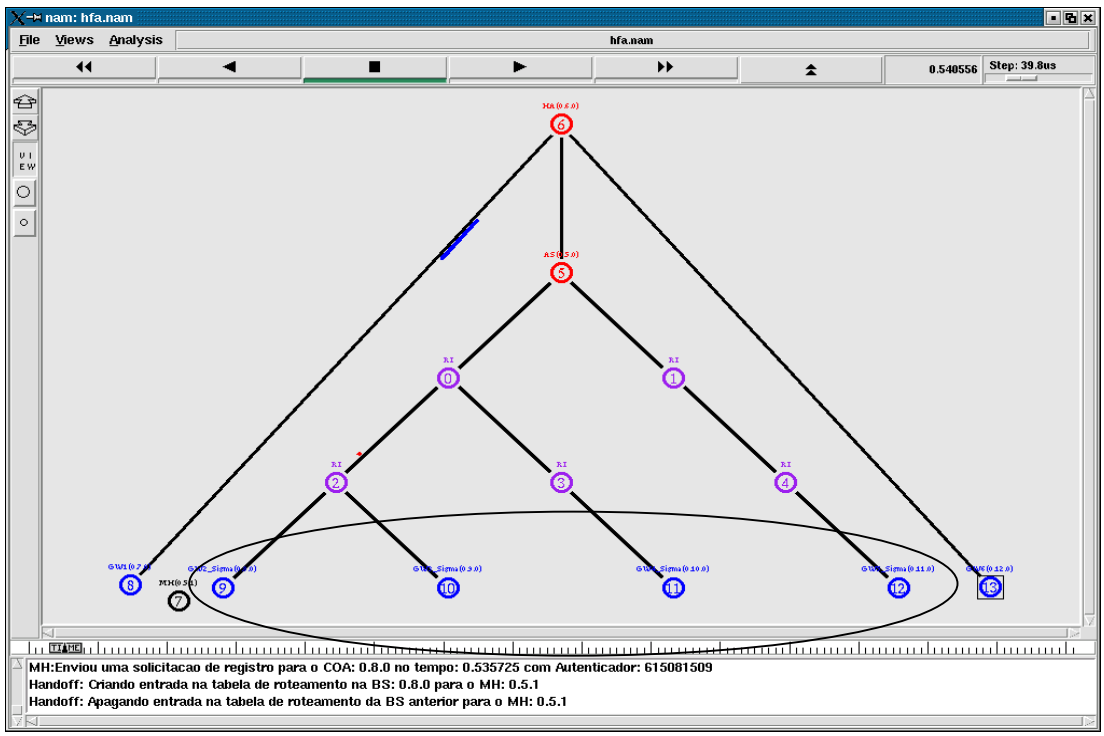


Figura 5.3 - MN envia solicitação de autenticação/atualização de registro

O pacote maior corresponde a uma mensagem de dados enviada para o GW0, responsável pelo domínio administrativo onde se encontrava o MN antes de entrar no GW1. Como o MN não se está mais no GW0 esse pacote será perdido.

A Figura 5.4 ilustra o momento em que o Agente de Segurança responsável pelo domínio de segurança no qual o GW1 faz parte, recebe um pacote contendo a solicitação de autenticação enviada pelo *gateway* GW1. Nesse momento o AS verifica que se trata de uma autenticação/atualização de registro a ser realizada pelo *Home Agent* e envia a solicitação para o HA. Após realizar o processo de autenticação e criação de chave $K_{MN\text{-}HA}$ como descrito na Seção 5.4.2.1.3, o HA envia a resposta da solicitação ao MN através do AS, como ilustra a Figura 5.5.

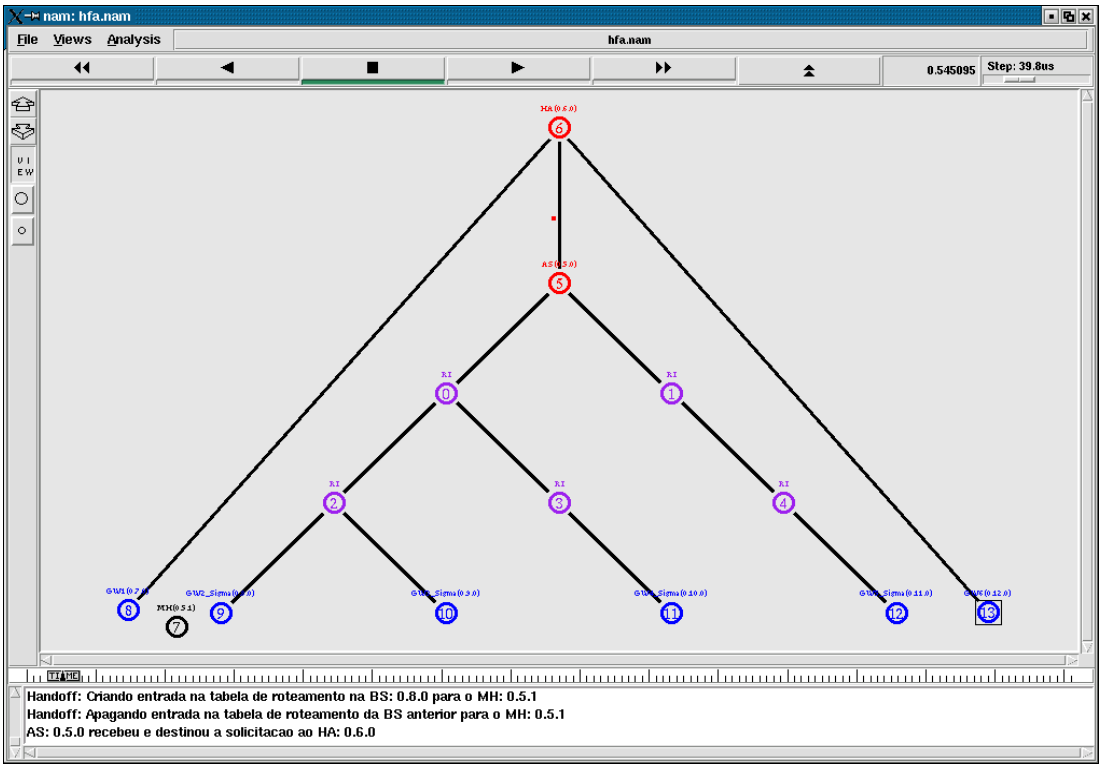


Figura 5.4 - AS recebe solicitação de autenticação/atualização de registro e envia para o HA

Por fim, o MN recebe a resposta de autenticação e verifica se a solicitação foi atendida e verifica a autenticidade do HA, como ilustrado na Figura 5.6.

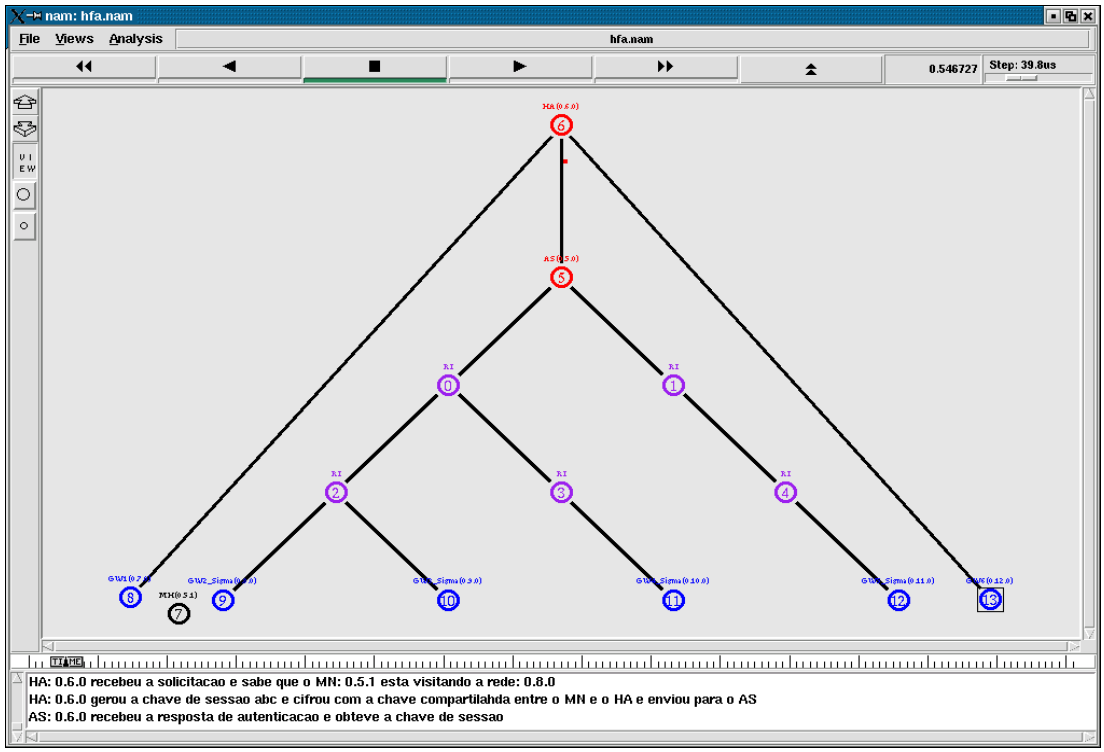


Figura 5.5 - HA envia resposta à solicitação de autenticação/atualização de registro

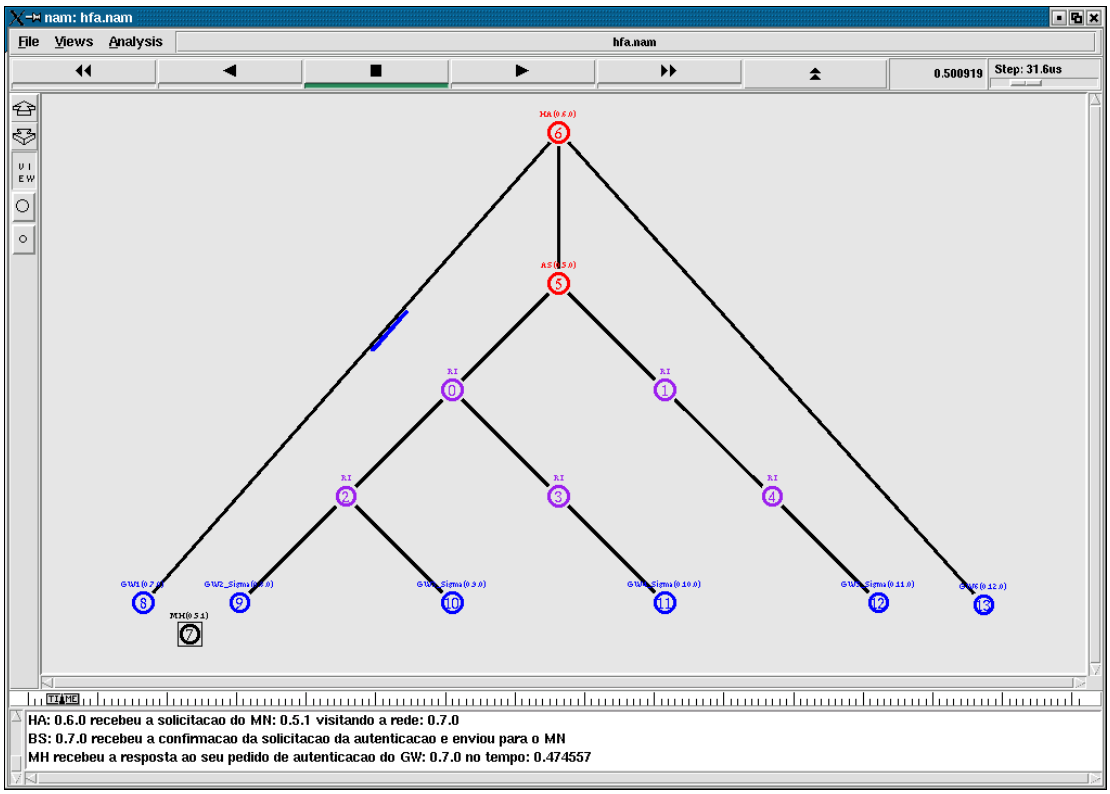
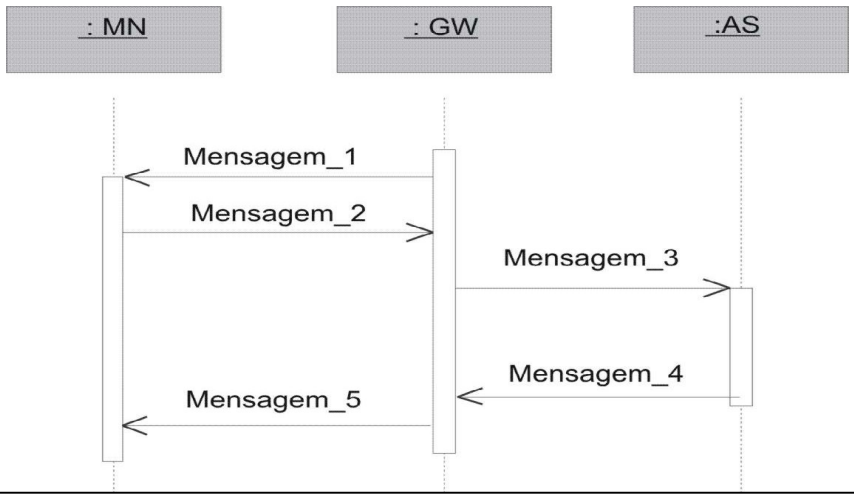


Figura 5.6 - MN recebe resposta da solicitação de autenticação

5.4.2.2 AUTENTICANDO EM UM MESMO DOMÍNIO DE SEGURANÇA

Nessa seção explicaremos em detalhes o funcionamento do processo de autenticação de um MN ao entrar em um domínio administrativo pertencente ao mesmo domínio de segurança em que se encontra o MN. O processo não envolve o *Home Agent*, visto que o Agente de Segurança do domínio visitante já possui informações necessárias para validar a identidade do usuário, obtidas no primeiro processo de autenticação realizado dentro do domínio de segurança, como visto na Seção 5.4.2.1.

Serão apresentadas, nesta seção, as estruturas dos anúncios (Mensagem_1) e das mensagens de solicitação (Mensagem_2 e Mensagem_3) e resposta (Mensagem_4 e Mensagem_5) do processo de autenticação. A Figura 5.7 apresenta o diagrama de seqüência que especifica o protocolo em um nível mais alto de abstração.



Mensagem_1 GW→MN: A_G, ID_{AS}, T_G

Mensagem_2 MN→GW: Aut_tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, T_{MN}, *Autenticador,onde Autenticador*: $K_{MN-AS}[ID_{HA}, ID_{AS}, Hadd, T_{MN}]$

Mensagem_3 GW→AS: $KP_{GW}[KU_{AS}[Aut\_tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, K_{MN-AS}[Hadd, ID_{AS}, ID_{HA}, T_{MN}], T_{GW}]$

Mensagem_4 AS→GW: $KP_{AS}[KU_{GW}[status, K_{MH\_AS}[status, T_{AS}]]]$

Mensagem_5 GW→MN: Hadd, ID_{GW}, status, $K_{MH\_AS}[status, T_{AS}]$, T_{GW}

Figura 5.7 - Solicitação de autenticação de um MN em um mesmo domínio de segurança

5.4.2.2.1 Anúncios

A mensagem de anúncio possui o mesmo formato que o proposto na Seção 5.4.2.1.1, como apresentado a seguir:

$$\text{Mensagem\_1 GW} \rightarrow \text{MN: } A_G,\ ID_{AS},\ T_G$$

5.4.2.2.2 Solicitação de Registro

Esta seção descreve o processo de solicitação de autenticação e atualização de registro de um dispositivo móvel, bem como o formato das mensagens envolvidas nessa solicitação, quando o mesmo não muda de domínio de segurança.

O MN, ao entrar em um domínio administrativo e constatar que não houve mudança de domínio de segurança através do identificador do Agente de Segurança (ID_{AS}), contido na mensagem de anúncio, envia ao *gateway* do domínio sendo visitado uma mensagem de solicitação de autenticação/atualização de registro idêntica à apresentada na Seção 5.4.2.1.2, ou seja:

$$\text{Mensagem\_2 MN} \rightarrow \text{GW: Aut\_tipo, Hadd, } ID_{AS},\ ID_{GW},\ ID_{HA},\ T_{MN},\ \textit{Autenticador}$$

No entanto, o campo *Autenticador* é cifrado utilizando a nova chave compartilhada entre o MN e o AS ($K_{MN\text{-}SA}$), e não com a chave compartilhada entre o MN e o HA, como acontece na autenticação vista na Seção 5.4.2.1.2. Também é necessário indicar na mensagem, através do campo Aut_tipo, que esta é uma solicitação que deve ser tratada localmente, ou seja, pelo AS. O MN pode desejar que a solicitação de autenticação/atualização seja destinada ao HA, mesmo que o AS possua informações suficientes para realizar a autenticação do MN. Nesse caso, isso deve ser indicado pelo campo Aut_tipo.

O *gateway*, por sua vez, encaminha a solicitação ao AS responsável pela gerência de localização e autenticação, como ilustrado na Mensagem_3 a seguir:

$$\text{Mensagem\_3 GW} \rightarrow \text{AS: } KP_{GW}[KU_{AS}[\text{Aut\_tipo, Hadd, } ID_{AS},\ ID_{GW},\ ID_{HA},\ K_{MN\text{-}AS}[\text{Hadd,}ID_{AS},\ ID_{HA},\ T_{MN}],\ T_{GW}]$$

O Agente de Segurança recebe a solicitação e verifica a assinatura do *gateway* através da chave pública do *gateway;* após isso, decifra a mensagem e obtém as informações enviadas. A informação ID_{AS} permite ao AS verificar se a solicitação de atualização de registro/autenticação foi realmente destinada a ele. Já a informação ID_{GW} confirma a identificação do *gateway* emissor da mensagem. O AS verifica se a mensagem é recente através da informação T_{GW}. A última verificação a ser feita é quanto ao tipo de autenticação a ser realizada. No cenário avaliado nessa seção, a autenticação é tratada pelo AS, ou seja, é local.

Em seguida, o AS obtém as informações contidas na mensagem de solicitação de autenticação/atualização de registro, recebida utilizando a chave simétrica compartilhada com o MN. A partir dessas informações, o AS será capaz de se certificar que aquela solicitação é destinada a ele, bem como verificar a identidade do móvel visitante. O AS verifica também a tempestividade da solicitação através da comparação do seu *timestamp* com o *timestamp* enviado pelo MN (T_{MN}). Esta verificação é necessária para proteger o domínio administrativo contra ataques do tipo *replay*.

5.4.2.2.3 Resposta da Solicitação

Após verificar a identidade do MN, o AS realiza a atualização de registro e envia ao *gateway* uma mensagem de resposta à solicitação de autenticação/registro, contendo o resultado da solicitação (*status)* e um *timestamp* (T_{AS}) cifrado com a chave pública do *gateway* e assinada pelo AS, utilizando sua chave privada (KP_{AS}). A estrutura da mensagem é mostrada a seguir:

$$Mensagem\_4\ AS \rightarrow GW:\ KP_{AS}[KU_{GW}[status,\ K_{MH\_AS}[status, T_{AS}]]]$$

Ao receber a resposta da solicitação, o *gateway* confere a assinatura do AS e decifra a informação utilizando sua chave privada. Em seguida, o *gateway* verifica se o *timestamp* recebido (T_{AS}) é recente. Para saber se a solicitação foi aceita pelo HA, o AS verifica o campo *status*. Após realizar as devidas verificações, o *gateway* encaminha a resposta da solicitação para o MN, através da Mensagem_5 a seguir:

$$Mensagem\_5\ GW \rightarrow MN:\ Hadd,\ ID_{GW},\ status,\ K_{MH\_AS}[status, T_{AS}],\ T_{GW}$$

O MN, ao receber a resposta da solicitação, verifica o identificador do *gateway* que originou a mensagem (ID_{GW}) e o resultado da solicitação (*status*). Se a resposta da solicitação for positiva, o MN inicia o uso dos recursos da rede visitada. Caso contrário, o MN toma

conhecimento que não foi possível realizar a autenticação através do AS, e será necessário realizar uma autenticação via HA.

5.4.2.2.4 Especificação Formal Usando Lógica BAN

Nessa seção vamos especificar formalmente o protocolo para o cenário em questão no qual o MN não muda de domínio de segurança. Inicialmente, vamos listar as mensagens do protocolo apresentadas na seção anterior, substituindo o campo *Autenticador* pelas informações que ele representa:

Mensagem_1 $GW \rightarrow MN$: A_G, ID_{AS}, T_G

Mensagem_2 $MN \rightarrow GW$: Aut_tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, T_{MN}, K_{MN-AS}[Hadd,ID_{AS}, ID_{HA}, T_{MN}]

Mensagem_3 $GW \rightarrow AS$: KP_{GW}[KU_{AS}[Aut_tipo, Hadd, ID_{AS}, ID_{GW}, ID_{HA}, K_{MN-AS}[Hadd,ID_{AS}, ID_{HA}, T_{MN}], T_{GW}]

Mensagem_4 $AS \rightarrow GW$: KP_{AS}[KU_{GW}[*status*, K_{MH_AS}[*status*,T_{AS}]]]

Mensagem_5 $GW \rightarrow MN$: Hadd, ID_{GW}, status, K_{MH_AS}[*status*,T_{AS}], T_{GW}

Similarmente à seção 5.4.2.1.4, para especificar formalmente um protocolo de segurança utilizando a lógica BAN, é necessário obter o protocolo idealizado e a partir dos postulados e das suposições iniciais alcançar o objetivo a que o protocolo se propõe. A seguir apresentamos as mensagens do protocolo idealizado, desconsiderando as mensagens 1 e 2, pois são não utilizam criptografia, ou seja, estão em texto claro:

- Mensagem_3: AS recebeu {{Hadd, T_{MN}, novo(T_{MN})}$_{KMN-AS}$, $T_{GW,}$ novo(T_{GW})}$_{KUAS}$}$_{KPGW}$
- Mensagem_4 GW recebeu {{*status*, K_{MH_AS}[T_{AS}]}$_{KUGW}$}$_{KPAS}$
- Mensagem_5 MN recebeu {*status*, K_{MH_AS}[*status*, T_{AS}], T_{GW}}

O objetivo do protocolo é fazer com que um pedido de autenticação feito pelo MN utilizando a chave compartilhada entre o MN e o AS (K_{MN-AS}) seja válido. Para isso, capturamos

as suposições iniciais, de forma implícita ou explicitamente, e aplicamos os postulados da lógica BAN, até concluirmos que o protocolo alcança o objetivo proposto.

Nesse cenário não são englobadas as suposições referentes ao *Home Agente*, pois esta entidade não participa do processo. Dessa forma, existem apenas nove suposições como listadas e detalhadas a seguir:

Tabela 5.2 - Suposições iniciais para o cenário em que o MN continua em um domínio de segurança

Suposição	Descrição da Suposição
S1	MN acredita $MN \leftrightarrow^{k} SA$
S2	SA acredita $MN \leftrightarrow^{k} SA$
S3	GW acredita $\Rightarrow^{K} AS$
S4	AS acredita $\Rightarrow^{K} GW$
S5	AS acredita $\Rightarrow^{K} AS$
S6	GW acredita $\Rightarrow^{K} GW$
S7	AS acredita novo(T_{MN})
S8	AS acredita novo(T_{GW})
S9	MN acredita novo(T_{AS})
S10	GW acredita novo(T_{AS})

As duas primeiras suposições (S1 e S2) garantem que o MN possui uma chave simétrica com o AS e ambos confiam nessa chave. As duas suposições seguintes (S3 e S4) garantem que o *gateway* confia na chave pública do Agente de Segurança e vice-versa. As suposições S5 e S6 garantem que o *gateway* e o AS confiam nas suas respectivas chaves públicas.

No protocolo proposto, todos os participantes devem ter seus relógios sincronizados. Dessa forma, temos as crenças: o AS acredita que T_{MN} e T_{GW} são novos (S7 e S8); o MN acredita que T_{AS} é novo (S9), e o *gateway* acredita que T_{AS} é novo (S10).

Para alcançarmos o objetivo dessa segunda parte do protocolo, vamos analisar cada mensagem do protocolo idealizado aplicando as regras e as crenças iniciais, até alcançarmos o final desse protocolo:

- **Mensagem_3: AS recebeu {{Hadd, T_{MN}, novo(T_{MN})}K_{MN-SA}, T_{GW}, novo(T_{GW})}KU_{AS}}KP_{GW}**

Inicialmente, aplicamos a suposição S4 e a regra do significado da mensagem (R1) na mensagem Mensagem_3, para verificar a assinatura do AS, tendo como resultado:

AS acredita GW disse {Hadd, T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{GW}, novo(T_{GW})}KU_{AS}**(1)**

Em seguida, aplicando novamente a regra do significado da mensagem e a suposição S5 em (1) para obter as informações cifradas com a chave pública do AS, temos que:

AS acredita GW disse {{Hadd,T_{MN}, novo(T_{MN})}K_{MN-HA}, T_{GW}, novo(T_{GW})} **(2)**

Por fim, aplicando a regra da verificação do identificador (R2) e a suposição S8 em (2), temos que:

AS acredita GW acredita {Hadd,T_{MN}, novo(T_{MN})}K_{MN-HA}} **(3)**

Até esse momento, o AS acredita que a mensagem enviada pelo GW foi realmente enviada por ele e que ela é recente, ou seja, não está sendo reutilizada. A seguir, será analisada a mensagem criada e enviada pelo MN, que é parte da mensagem (3).

Aplicando a regra do significado da mensagem (R1) e a suposição S2 na mensagem {Hadd,T_{MN}, novo(T_{MN})}K_{MN-AS}}, temos que:

AS acredita MN Acredita {Hadd,T_{MN}, novo(T_{MN})} **(4)**

Aplicando a regra da verificação do identificador e a suposição S7 em (4), temos que:

AS acredita MN Acredita {Hadd} **(5)**

Dessa forma, temos que o AS acredita que a mensagem foi originada pelo MN e é recente. Após essa verificação, o AS atualiza o registro de localização do MN e envia uma mensagem de resposta para o MN, através do *gateway*, como mostrada na Mensagem_4.

- **Mensagem_4: GW recebeu {{status, { status, T_{AS}}K_{MH_AS} } KU_{GW}} KP_{AS}**

Aplicando a suposição S3 e a regra do significado da mensagem, temos que:

GW acredita AS disse {*status*, {*status*, T_{AS}}K_{MH_AS}} KU_{GW} **(6)**

Aplicando a suposição S6 e a regra do significado da mensagem, temos que:

HA acredita SA disse {*status*, {*status*, T_{AS}} K_{MH_AS} } **(7)**

Ao fim do passo (7), o *gateway* já conhece o resultado da solicitação da autenticação e envia uma mensagem para o MN que contém um *timestamp* (T_{AS}) cifrado com a chave K_{MN-AS}, como mostrado na Mensagem_5.

- **Mensagem_5 MN recebeu {status, {T_{AS}} K_{MH_AS}, T_{GW}}**

Através dessa mensagem, o MN verifica a tempestividade da mensagem (T_{GW}) e o resultado da solicitação de autenticação (*status*). Se o resultado identificar que a autenticação foi realizada com sucesso, então o MN verifica se a permissão partiu do AS através da informação {*status*,T_{AS}}$K_{MN-AS,}$ como detalhado a seguir:

Aplicando a suposição S1 e a regra do significado da mensagem, temos que:

MN acredita AS disse {*status*, T_{AS}} **(8)**

Aplicando a regra da verificação do identificador e a suposição S9, temos que:

MN acredita AS acredita {*status*} **(9)**

Desta forma, temos ao final da análise da troca de mensagens :

- AS acredita que MN gerou a solicitação;
- MN acredita que AS gerou a solicitação.

Portanto, o MN foi autenticado pelo AS, e o AS autenticou o MN como proposto pelo protocolo.

5.4.2.2.5 Simulação

Nessa seção mostramos a simulação do processo de autenticação proposto de um MN ao mudar de domínio administrativo e continuar dentro do mesmo domínio de segurança. Esse cenário não envolve o *Home Agent*, visto que o Agente de Segurança do domínio visitante já possui informações necessárias para validar a identidade do usuário. As Figuras 5.8 5.9 e 5.10 ilustram esse cenário. A notação utilizada para representar os nós da simulação é a mesma da Seção 5.4.2.1.5, isto é:

RI - Roteadores Internos pertencentes à Internet

GW – *gateway* da rede sendo visitada.

AS - Agente de Segurança responsável pelos domínios administrativos GW0, GW1, GW2 e GW3.

MN - *Mobile Node*

A Figura 5.8 ilustra, através de um pacote, um MN entrando em um domínio administrativo (GW2) gerenciado pelo mesmo Agente de Segurança que o domínio administrativo visitado anteriormente pelo MN (GW1). Em um primeiro momento, o MN cria uma solicitação de autenticação e envia ao *gateway*, que, por sua vez, após realizar as verificações necessárias, envia a solicitação ao AS.

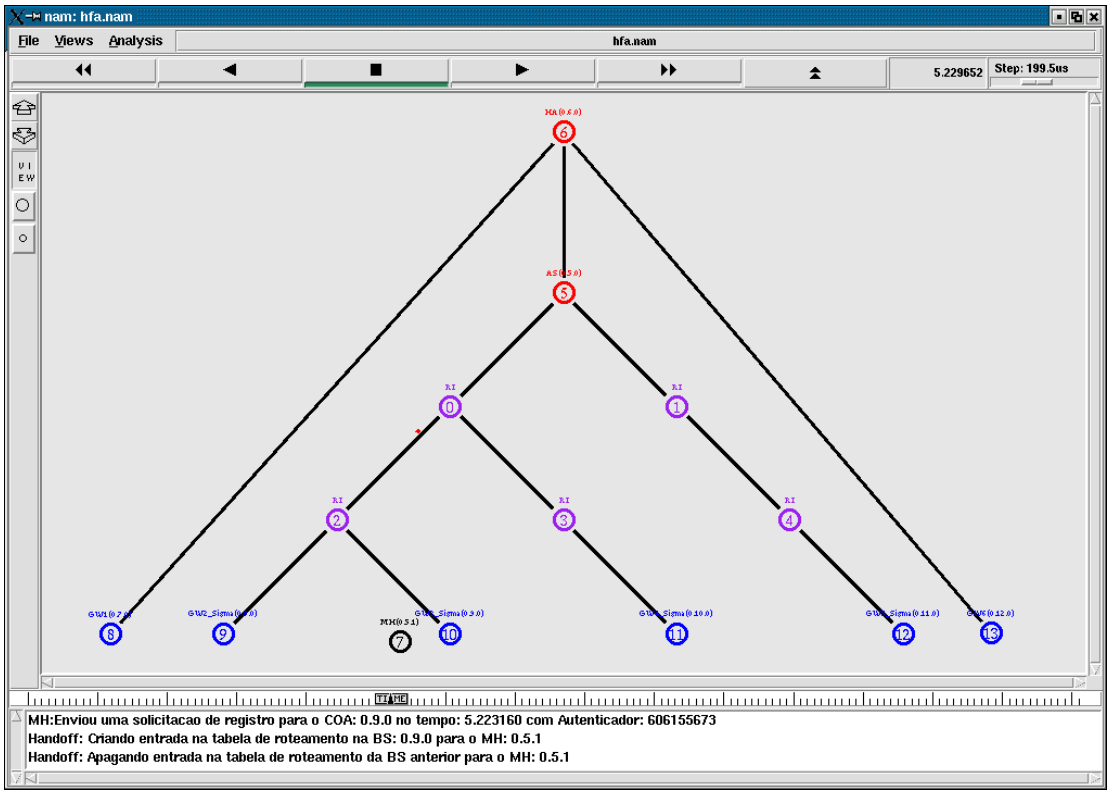


Figura 5.8 - MN envia solicitação de autenticação/atualização de registro interno

A Figura 5.9 ilustra o momento em que o Agente de Segurança responsável pelo domínio de segurança no qual o GW2 faz parte recebe um pacote contendo a solicitação de autenticação enviada pelo *gateway*. Diferentemente do cenário apresentado na Seção 5.4.2.1, o AS trata a solicitação de autenticação/Atualização de registro localmente, ou seja, não envia ao *Home Agent*. Ainda nessa figura, um pacote de dados enviado para o MN é entregue seguindo a nova rota criada.

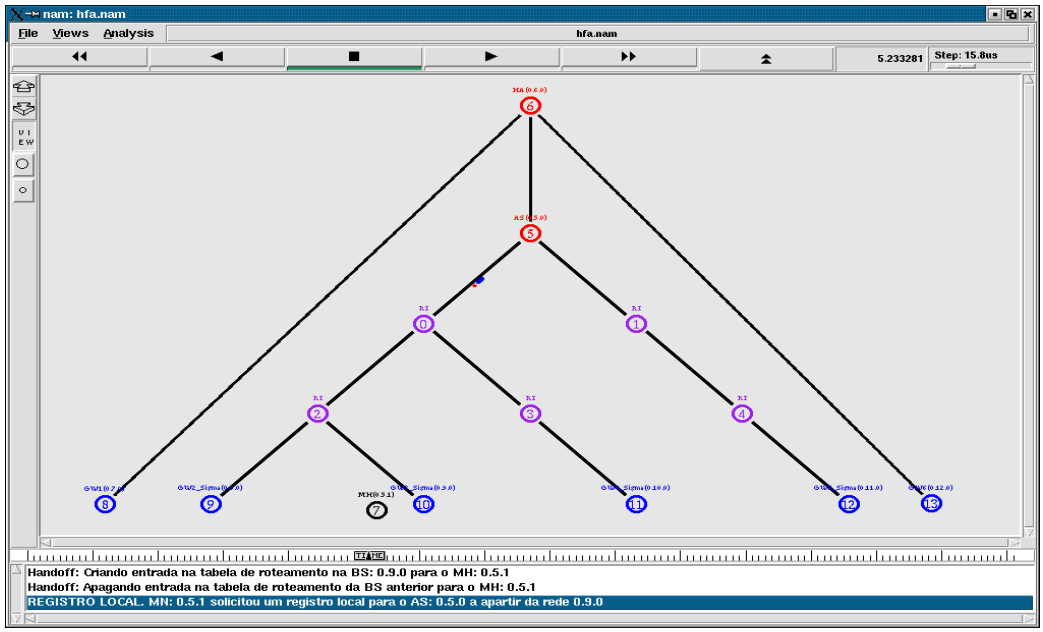


Figura 5.9 - AS recebe pacote de solicitação de autenticação/atualização de registro

Por fim, o MN recebe a resposta da solicitação e verifica se a solicitação foi atendida, além de se certificar da autenticidade do AS, como apresentado na Figura 5.10. O pacote de dados enviado para o MN passa pelo *gateway* (GW2) do novo domínio administrativo, e este, por sua vez, entrega ao MN.

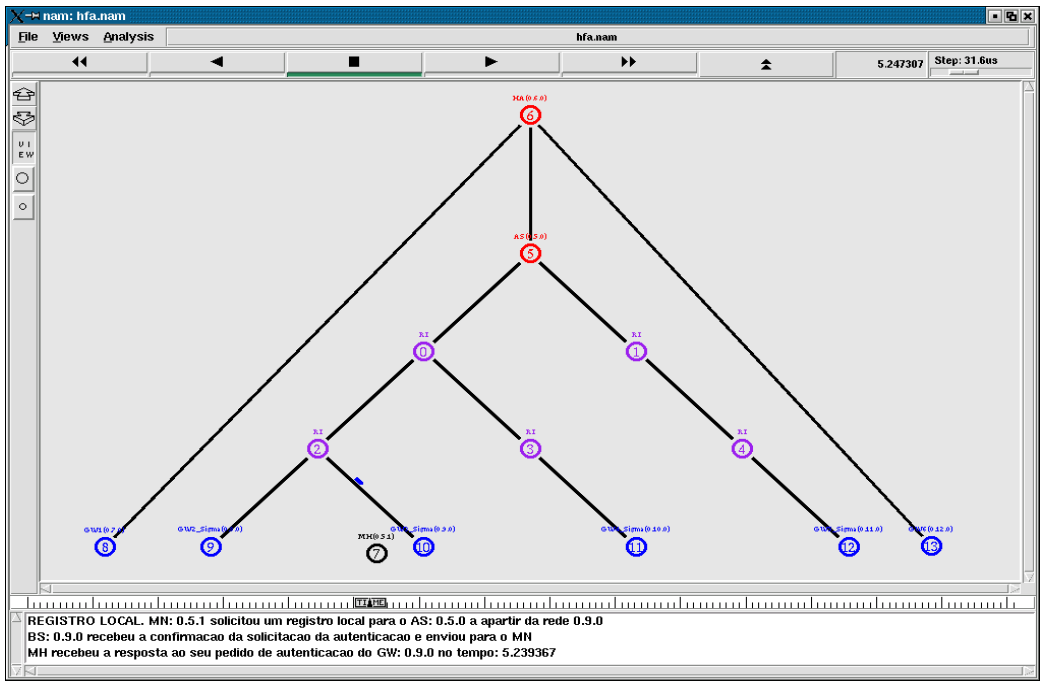


Figura 5.10 - MN recebe resposta da solicitação de autenticação

5.5 PROTOCOLO PROPOSTO *VERSUS* MIP

Nessa seção realizaremos uma comparação entre o protocolo proposto nesta dissertação integrado à proposta apresentada em [ALBANO 2004] [AACA 2003] e a proposta de autenticação e atualização de registro original do *Mobile IP* [PERKINS 2000]. As propostas de segurança para o MIP citada na Seção 3.3 não são comparadas com nosso trabalho, pois estas propostas necessitam acessar o HA a cada mudança de domínio administrativo, o que as tornam, em termos de número de acessos ao HA, idênticas ao MIP original. Por outro lado, a análise desempenho desta proposta com relação às propostas de segurança existentes para o MIP é apresentada como trabalho futuro na Seção 6.3.

5.5.1 AMBIENTE DE SIMULAÇÃO

Para realizar uma comparação entre o MIP e a nossa proposta, consideraremos inicialmente, um MN se movimentando de forma aleatória entre seis domínios administrativos independentes e conectados ao *Home Agent* através da Internet utilizando o protocolo de gerenciamento de mobilidade e segurança do *Mobile IP* original, como ilustrado na Figura 5.11, através do NAM. O significado de cada nó na simulação foi descrito na Seção 5.4.2.1.5.

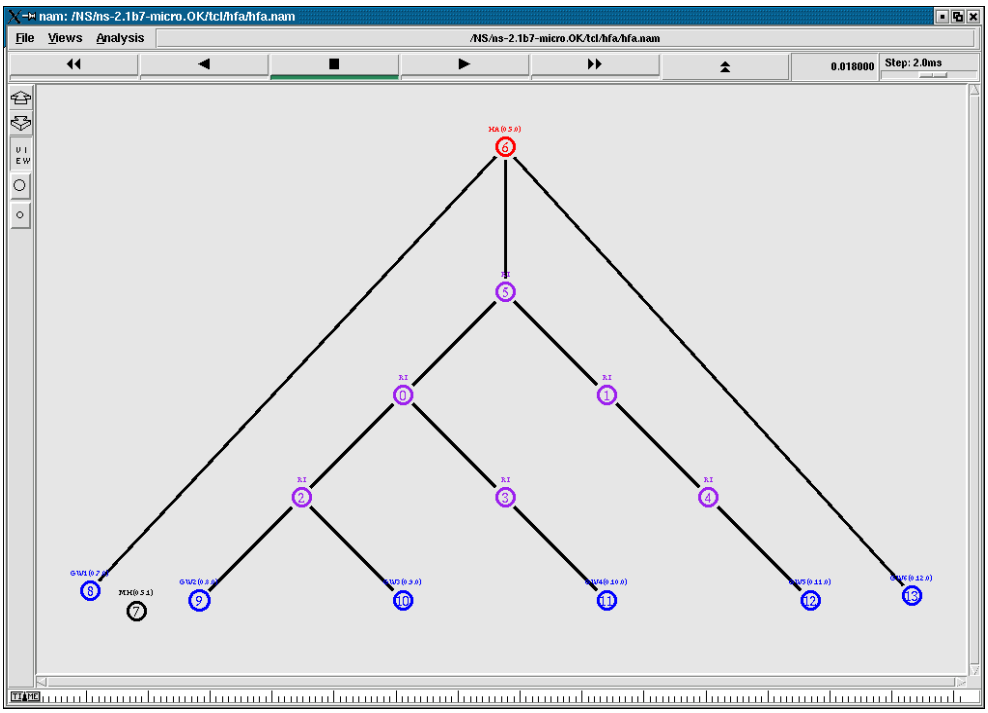


Figura 5.11 - Topologia da rede *Mobile IP* utilizada na análise comparativa

Nesse cenário, a cada mudança de domínio administrativo realizada, uma solicitação de autenticação/atualização de registro é enviada ao *Home Agent* do MN. Dessa forma, teremos o número de solicitações ao HA diretamente proporcional ao número de mudanças de domínios administrativos. Estamos considerando que a área em que o MN se movimenta está sempre contida em um domínio administrativo, não existindo áreas sem cobertura.

Por outro lado, para simular nossa proposta de autenticação, consideremos um domínio de segurança composto por quatro domínios administrativos (nós com rótulos 9, 10, 11 e 12) conectados diretamente ao Agente de Segurança (nó 5), e este, por sua vez, conectado ao HA (nó 6) através da Internet. Também fará parte desse cenário dois domínios administrativos que não fazem parte do domínio de segurança existente (nós com rótulos 8 e 13), como ilustrado na Figura 5.12. Maiores detalhes sobre esses ambientes de simulação podem ser vistos nas Seções 5.4.2.1.5 e 5.4.2.2.5.

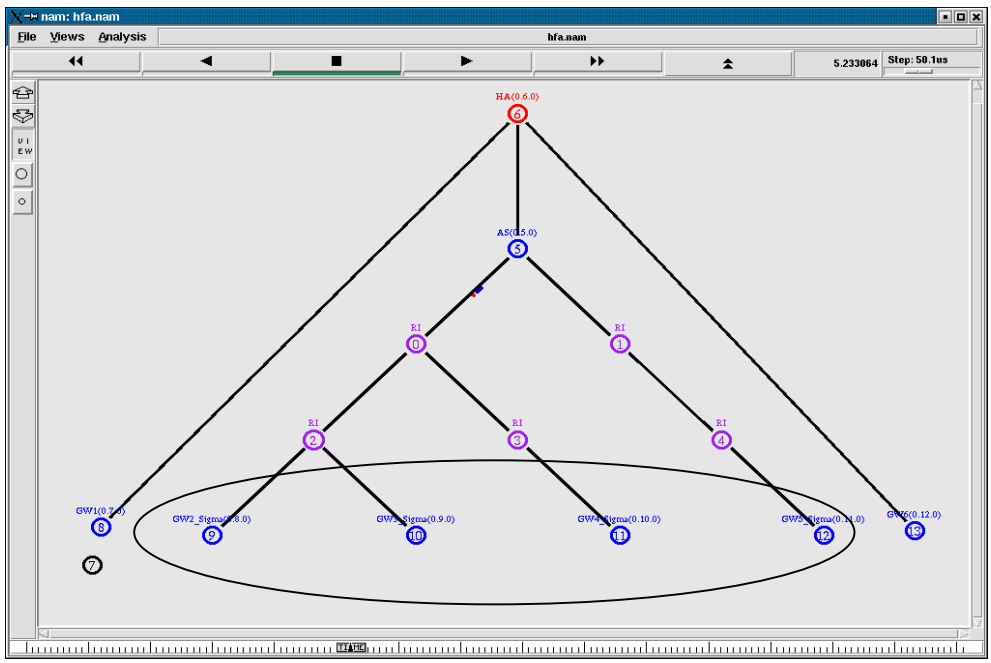


Figura 5.12 - Topologia da proposta utilizada na análise comparativa

A simulação será realizada para os casos de um MN executar 100, 200, 300, 400 e 500 mudanças de domínios administrativos em ambos os cenários. Para cada caso foram realizadas 50 simulações. A movimentação do MN ocorre de forma aleatória entre os domínios administrativos.

Na simulação utilizamos antenas omnidirecionais e o modelo de propagação *Two-Ray Ground*, que considera dois caminhos para a propagação das ondas, o caminho direto e o da reflexão das ondas no solo.

Para realizar as simulações foi utilizado um PC Intel 2GH de freqüência e 256M de memória. O sistema operacional utilizado foi o Conectiva Linux 8.0.

5.5.2 MÉTRICAS

Essa seção apresenta duas métricas a serem utilizadas para realizar a análise de desempenho do protocolo proposto e então compará-las às métricas do MIP. As métricas são as seguintes:

- Número de solicitações encaminhadas ao HA para realizar a autenticação/Atualização de registro de um MN.
- Perda de pacotes enviados para o MN. Essa métrica compara o número de pacotes enviados pelo HA para o MN e o número de pacotes efetivamente recebidos.

Como trabalho futuro seria interessante verificar o tempo de autenticação gasto utilizando os vários algoritmos de autenticação existentes.

5.5.3 RESULTADOS OBTIDOS

Os resultados obtidos são baseados nas métricas descritas na seção 5.5.2 e o ambiente de simulação proposto na seção 5.5.1. A seguir detalhamos cada uma dessas métricas e os resultados que elas forneceram.

5.5.3.1 NÚMERO DE SOLICITAÇÕES AO HA

A Tabela 5.3 ilustra a comparação entre o número de solicitações de autenticação ao HA utilizando o protocolo original do MIP e a proposta desta dissertação realizada por um MN com velocidade de 40 m/s. Pela tabela podemos perceber que o MIP possui o número de acessos ao HA igual ao número de *handoffs*. Por sua vez, a proposta desse trabalho minimiza o número de solicitações ao HA.

Tabela 5.3 - Tabela comparativa entre o número de *Handoffs* do MIP e AS

Número de *Handoffs*	# Acessos ao HA e MIP	% Acessos ao HA e MIP	# Acessos ao HA e MIP+AS+EGM	% Acessos ao HA e MIP+AS+EGM
100	100	100%	69	69,0%
200	200	100%	118	59,0%
300	300	100%	175	58,3%
400	400	100%	230	57,5%
500	500	100%	286	57,2%

A Figura 5.13 ilustra o resultado para o caso de 500 *handoffs* utilizando um gerador de gráficos denominado *Xgraph* [XGRAPH 2003].

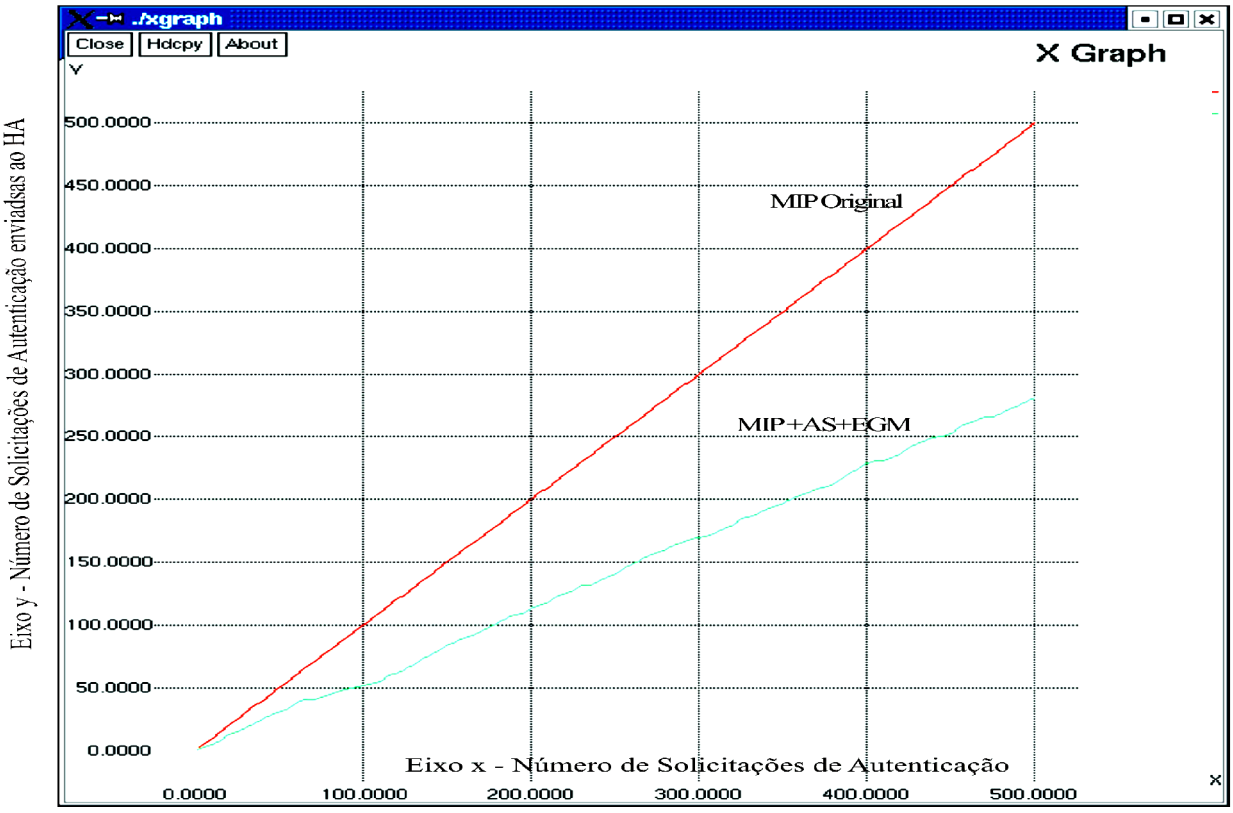


Figura 5.13 - Comparação entre o número de solicitações de autenticação entre o *Mobile IP* original e nossa proposta

Vale ressaltar que apesar do comportamento da nossa proposta possuir, na primeira solicitação de autenticação dentro de um domínio de segurança, semelhança comportamental com

o MIP, existe o diferencial de que a solicitação de autenticação/atualização de registro é enviada primeiramente ao AS, diferentemente do protocolo MIP, que envia diretamente ao HA. No entanto, esse aumento de entidades envolvidas na autenticação será compensado quando um MN realizar várias solicitações de autenticação/atualização de registro dentro do mesmo domínio de segurança.

5.5.3.2 PERDA DE PACOTES

Para obtermos essa métrica nós fixamos a velocidade do MN em 20 m/s e variamos o número de mudanças de domínios administrativos (*handoffs*) do MN em 100, 200, 300, 400 e 500. O fluxo utilizado entre o HA e o MN é o CBR, com tamanho do pacote de 210 *bytes*. A Tabela 5.4 mostra o resultado da simulação através do número de *handoff*, número de pacotes enviados, o número de pacotes perdidos utilizando a proposta *Mobile IP* original e o número de pacotes perdidos empregando a nossa proposta.

Tabela 5.4 - Tabela comparativa da perda de pacotes

Número de *Handoffs*	Número de Pacotes	Perda Pacotes MIP(s)	Perda Pacotes AS(s)
100	47.747	143	124
200	96.071	285	257
300	144.371	399	381
400	192.671	586	507
500	240.970	758	633

Como vimos anteriormente, enquanto o MN permanecer inserido em um domínio de segurança, os pacotes serão endereçados ao AS, que funciona como um gerente de mobilidade de acordo com a proposta em [ALBANO 2004] [AACA 2003]. Dessa forma, a quantidade da perda de pacotes entre o AS e o HA é similar ao número de pacotes perdidos entre o HA e o *gateway* do proposto MIP original.

Por gerenciar localmente as solicitações de autenticação/atualização de registro, um domínio de segurança realiza *handoffs* mais rápidos, o que diminui o número de pacotes perdidos

durante tais *handoff*. Essa idéia é similar às propostas de gerenciamento de micromobilidade descritos no Capítulo 2.

5.6 CONCLUSÃO

Nessa seção apresentamos uma proposta para diminuir o número de solicitações de autenticação realizados por um *Mobile Node* enquanto está se movimentando entre áreas de micromobilidade. Para alcançar esse objetivo, adicionamos uma nova entidade funcional, denominada de *A*gente de Segurança (AS), cujo principal papel é autenticar os MNs de forma rápida e quase independente do *Home Agent*. Foram utilizados diagramas de seqüências para mostrar a troca de mensagens entre a entidades, além de especificar formalmente a proposta utilizando a lógica BAN. Também foram apresentados os resultados obtidos através de simulações utilizando o *Network Simulator*. Utilizamos as métricas: número de acesso ao HA e perda de pacotes; e pelos resultados alcançados verificamos que nossa proposta fornece uma solução eficiente para diminuir o número de acessos ao HA e com uma taxa de perda de pacotes inferior.

CAPÍTULO 6 CONCLUSÃO

Esta dissertação apresenta uma proposta para otimizar a autenticação de dispositivos móveis que se movimentam entre áreas de micromobilidade, através da adição de uma nova entidade funcional, denominada Agente de Segurança, cuja função é gerenciar a autenticação de um dispositivo móvel que visita os domínios administrativos dentro de um domínio de segurança.

6.1 RESULTADOS ALCANÇADOS

Este trabalho introduziu uma entidade funcional denominada Agente de Segurança no *Mobile* IP e mostrou que a inserção dessa entidade diminui o número de acessos ao *Home Agent* para fins de autenticação. Este resultado acarreta em uma melhoria no tempo de resposta a uma solicitação de autenticação realizada por um dispositivo móvel que muda constantemente de domínio administrativo.

Também adaptamos uma metodologia de especificação formal utilizada para o desenvolvimento de software para uma metodologia voltada para o desenvolvimento de protocolos de segurança, consistindo das etapas de definição de requisitos, projeto com especificação formal e simulação. Através dessa metodologia existem ganhos no tempo de desenvolvimento de protocolos de segurança e na legibilidade de tais protocolos.

Utilizamos especificação formal para evitar erros e ambigüidades no protocolo, de forma a concluir que o protocolo é válido e sem erros. As técnicas de especificação formal utilizadas foram diagramas de seqüência e a lógica BAN, métodos formais simples e de rápida especificação.

Verificamos a validade do protocolo através de simulações usando *Network Simulator*. Com isso, asseguramos que há uma significativa redução no número de solicitações ao *Home Agent* e uma melhoria na eficiência do processo de autenticação.

Além disso, esperamos que este trabalho também sirva de referência para um aprofundamento no uso do *Network Simulator*, bem como no conhecimento de lógica BAN para especificar formalmente protocolos de segurança.

6.2 PROBLEMAS ENCONTRADOS

Nesta seção discutiremos os principais obstáculos encontrados para o desenvolvimento desse trabalho.

O primeiro problema encontrado, diz respeito ao desenvolvimento de módulos para realizar simulação de novas tecnologias no *Network Simulator*. Apesar de ser uma ferramenta utilizada em várias pesquisas da academia, o *Network Simulator* não oferece um mecanismo para desenvolver novos módulos, ou até mesmo para adaptar os já existentes. Conseqüentemente, uma grande parte do tempo desta pesquisa foi dedicada para entender o complexo código-fonte do NS.

O segundo diz respeito à aplicação da lógica BAN. A literatura existente não detalha como devemos converter um protocolo existente em um protocolo idealizado, de forma que devemos nos contentar com exemplos às vezes errôneos de como aplicar a lógica BAN.

Apesar das dificuldades encontradas, os resultados previstos nesta dissertação foram alcançados, como mencionado na Seção 6.1. Esperamos que em trabalhos posteriores utilizando NS e lógica BAN, esta dissertação sirva como referência para facilitar o uso do *Network Simulator*, bem como da lógica BAN para especificar formalmente protocolos de segurança.

6.3 TRABALHOS FUTUROS

Esta dissertação considera que o primeiro processo de registro de um MN ao entrar em um domínio de segurança deve ser realizado pelo *Home Agent* do MN. Seria interessante analisar a extensão dessa proposta de forma a criar um mecanismo que proporcione a reutilização de informações de autenticação de Agentes de Segurança vizinhos, o que otimizaria ainda mais o processo de autenticação.

Considerando que a proposta foi simulada para um domínio de segurança possuindo quatro domínios administrativos, é interessante analisar com mais detalhes quantos domínios administrativos poderiam conter em um domínio de segurança sem criar um ‘gargalo’ no Agente de Segurança.

Consideramos ainda como um trabalho futuro à integração total de nossa proposta com a proposta em [ALBANO 2004] [AACA 2003], abrangendo *paging* e conectividade passiva.

Um trabalho futuro seria a implementação de outros serviços de segurança para serem integrados à nossa proposta, como por exemplo, autorização.

Outro tipo de trabalho futuro refere-se à integração desta proposta de autenticação com as várias propostas de micromobilidade existentes realizando uma comparação para verificar qual protocolo de micromobilidade teria melhor desempenho.

Como trabalho futuro seria interessante verificar o tempo de autenticação gasto utilizando os vários algoritmos de autenticação existentes.

Um estudo a ser realizado futuramente é a análise de desempenho de nossa proposta comparando com outras propostas de segurança existentes para o MIP.

Além disso, criar um *framework* que facilitasse o desenvolvimento de módulos para realizar simulações para o NS.

REFERÊNCIA BIBLIOGRÁFICA

[**AAA 2003**] **IETF´s AAA working group**. Disponível em http://www.ietf.org/html.charters/aaa-charter.html. Acessado em julho de 2003.

[**AACA 2003**] Albano, W.; Andrade, R. M. C.; Cavalcanti, F. R.; Allen, R., **Localização e segurança de dispositivos móveis entre Redes Cellular IP**. Newsgeneration, Rio de Janeiro, v. 7, edição especial números 2 e 3, julho 2003. Disponível em: <http://www.rnp.br/newsgen>.

[**AALSY 1999**] Amyot, D.; Andrade, R.; Logrippo, L.; Sincennes, J.; and Yi, Z., (1999) **Formal Methods for Mobility Standards** . IEEE 1999 Emerging Technology Symposium on Wireless Communications & Systems, Dallas, USA, April 12-13, 1999.

[**AD 1994**] AZIZ, A.; DIFFIE, W., **Privacy and Authentication for Wireless Local Area Networks**. IEEE Personal Communications. pp. 25-31.1994.

[**ALBANO 2004**] Albano, W. A., Um elemento para o registro de localização de dispositivos móveis entre redes *Cellular IP*. 2004. 105 f. Dissertação de mestrado em Engenharia Elétrica. Universidade Federal do Ceará, Fortaleza, Ceará, Brazil, 2004.

[**ANDRADE 2001**] Andrade, R. M. C., **Capture, Reuse, and Validation of Requirements and Analysis Patterns for Mobile Systems.** 2001. 226 f. Thesis (Doctor of Philosophy in Computer Science)-School of Information Technology and Engineering (SITE), University of Ottawa-Carleton Institute of Computer Science, Ottawa, Ontario, Canada, 2001.

[**ASACS 2004**] Albano, W.; Sales, W.; Andrade, R.; Cavalcanti, R.; Souza, J. N., **SiGMA: Uma entidade para localização e autenticação de dispositivos móveis entre áreas de micromobilidade**. XXII Simpósio Brasileiro de Redes de Computadores, maio, 2004.

[**ATKINSON 1995/1**] Atkinson, R., **IP Authentication Payload**, IETF RFC 1827, agosto, 1995.

[**ATKINSON 1995/2**] Atkinson, R., **IP Authentication Header**, IETF RFC 1826, agosto, 1995.

[**BALPARDA 2001**] Balparda, D. C., **Segurança de dados com Criptografia Métodos e Algoritmos**. 2. ed. Rio de Janeiro: Ed. Book Express. 2001.

[**BAN 1990**] Burrows, M.; Abadi, M.; Needham, R., **A Logic for Authentication**, Technical Report 39, SRC DIGITAL, 1990.

[**BDHSK 2003**] Byang-Gil Lee; Doo-Ho Choi; Hyun-Gon Kim; Seung-Won Sohn; Kil-Houm Park, **Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography**. Telecommunications, 2003. ICT 2003. 10th International Conference on , v.1, pp.597 603, 2003.

[**BRD 2000**] Braga, A. M.; Rubira, C. M. F.; Dahab, R., **Tropyc: A Pattern Language for Cryptographic Software**. Pattern Languages of Program Design 4 (PLoPD4), N.D. Harrison, B. Foote, and H. Rohnert, eds., Addison-Weslev, pp. 337-371, 2000.

[**BV 1998**] Blunk, L.; Vollbrecht, J., **PPP Extensible Authentication Protocol**, IETF RFC 2284, março, 1998.

[**CASTELLUCIA 2000**] Castellucia, C., **A Hierarchical Mobile IPV6 Proposal**. ACM Mobile Computing and Communication Review (MC2R), abril, 2000.

[**CFV 2002**] Cappiello, M.; Floris, A.; Veltri, L., **Mobility amongst heterogeneous networks with AAA support**. Communications, 2002. ICC 2002. IEEE International Conference on, v.4, pp.2064 2069,2002.

[**CG 2001**] Campbell, A. T.; Gomes-Castellanos, J., **IP MicroMobility Protocols**. ACM SIGMOBILE Mobile Comp. Commum Rev., 2001.

[**CGKVCT 2000**] Campbell, A. T.; Gomez, J.; Kim, S.; Valko, A. G.; CHIEH-YIH WAN; TURANYI, Z.R. **Design, Implementation, and Evalution of Cellular IP**. IEEE Personal Communications, v.7, n.4, pp. 42 49, agosto, 2000.

[**CGV 1999**] Campbell, A. T.; Gomez, J.; Valko, A. G., **An Overview of Cellular IP.** Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE, New Orleans, v. 2, pp. 606 610, setembro, 1999.

[**CKK 2002**] Chiussi, F. M.; Khotimsky, D. A.; Krishnan, S., **Mobility Management in Third-Generation All-IP Networks**. IEEE Communications Magazine, p. 124-135, setembro, 2002.

[CRAIGER 2002] Craiger, J., **802.11, 802.1x, and Wireless Security.** SANS Institute, junho, 2002.

[**DGGVS 2000**] De Laat, C.; Gross, G.; Gommans, L.; Vollbrecht, J.; Spence, D., **Generic AAA Architecture**, RFC 2903, agosto, 2000.

[**DH 1995/1**] Deering, S.; Hinden, R., **Internet Protocol, Version 6 (IPv6). Specification**, IETF RFC 1883, dezembro, 1995.

[**DH 1995/2**] Deering, S.; Hinden, R., **IP Version 6 Addressing Architecture**, IETF RFC 1884, dezembro, 1995.

[**DROMS 1993**] Droms, R., **Dynamic Host Configuration Protocol**, IETF RFC 1541, outubro, 1993.

[**GEN 2001**] Grilo, A.; Estrela, P.; Nunes, M., **Terminal Independent Mobility for IP (TIMIP)**, IEEE Communications Magazine, pp. 34-41, dezembro, 2001.

[**GJP 2002**] Gustafsson, E.; Jonsson, E.; Perkins, C., **Mobile Ipv4 Regional Registration**, Internet Draft, draft-ietf-mobileip-reg-tunel-06.txt, março, 2002.

[**GLOMOSIM 2003**] **GlomoSim Web Site**. Disponível em http://pcl.cs.ucla.edu/projects/glomosim/. Acessado em maio de 2003.

[**GSG 1999**] GRITZALIS, S.; SPINELLIS, D.; GEORGIADIS, P., **Security protocols over open networks and distributed systems: formal methods for their analysis, design and verification**. Computer Communications, vol. 22, n o 8, pp. 697-709. Maio 1999.

[**IETF 2003**] **Internet Engineering Task Force**. Disponível em http://www.ietf.org. Acessado em maio 2003.

[**IIFO 1997**] Inoue, A.; Ishiyama, M.; Fukumoto, A.; Okamoto, T., **Secure mobile IP using IP security primitives**. Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997, Proceedings Sixth IEEE workshops on , pp. 235 241, junho, 1997.

[**JP 2000**] Jonhson, D. B.; Perkins, C., **Route Optimization in Mobile IP**, draft-ietf-mobileip-optim-10.txt, novembro, 2000.

[**JP 2004**] Jonhson, D. B.; Perkins, C., **Mobility Support in IPv6,** IETF RFC 3775, junho, 2004.

[**MEADOWS 1994**] MEADOWS, C., **Formal verification of cryptographic protocols: A survey**. ASIACRYPT 94: Advances in Cryptology International Conference on the Theory and Application of Cryptology pp 133-150. 1995. Disponível em http://citeseer.nj.nec.com/134868.html

[**MEADOWS 2000**] MEADOWS, Catherine. **Open Issues in Formal Methods for Cryptographic Protocol Analysis**. DISCEX 2000: Proceedings of the DARPA Information Survivability Conference and Exposition, v. 1, p. 237-250. IEEE Computer Society Press. Janeiro 2000.

[**MONTENEGRO 1998**] Montenegro, G., **Reverse Tunneling for Mobile IP**, IETF RFC 2344, maio, 1998.

[**NAM 2003**] **Network Animator Web Site**. Disponível em http://www.isi.edu/nsnam/nam. Acessado em abril 2003.

[**NS 2003**] **Network Simulator Web Site**. Disponível em http://www.isi.edu/nsnam/ns. Acessado em abril 2003.

[**OMNET 2003**] **OMNet Web Site**. Disponível em http://whale.hit.bme.hu/omnetpp/. Acessado em maio de 2003.

[**OPNET 2003**] **OPNet Web Site**. Disponível em http://www.opnet.com/. Acessado em maio de 2003.

[**PERKINS 1996**] Perkins, C., **IP Encapsulation within IP**, IETF RFC 2003, outubro, 1996.

[**PERKINS 1997**] Perkins, C., **Mobile IP**, IEEE Communications Magazine, v.35, n.5, pp.66-82, maio, 1997.

[**PERKINS 1998**] Perkins, C., **Mobile networking through Mobile IP.** Internet Computing, IEEE, v.2, n.1, pp.58 69, janeiro/fevereiro, 1998.

[**PERKINS 1999**] Perkins, C., **Mobile IP and security issue: an overview.** Internet Technologies and Services, 1999. Proceedings. First IEEE/Popov Workshop on, pp.131 148, outubro, 1999.

[**PERKINS 2000**] Perkins, C., **Mobile IPv4 Challenge/Response Extensions**, IETF RFC 3012, novembro, 2000.

[**PERKINS 2002**] Perkins, C., **Mobile IP**. IEEE Communications Magazine, v.40, n.5, pp.66-82, maio, 2002.

[**PP 2002**] Pagtzis, T.; Perkins C., **Performance issues for localised IP mobility management**. Networks, 2002. ICON 2002. 10th IEEE International Conference on, pp.211 216, 2002.

[**RBU 2002**] Ringapin, A.; Ben-Othman, J.; Urien, P., **Mobility and security in IP network**. Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on, v.1, pp.280-284, 2002.

[**RLTVS 1999**] Ramjee, R.; La Porta, T.; Thuel, S.; Varadhan, K; Salgarelli, L., **IP micro-mobility support using HAWAII**, Internet Draft, draft-ietfmobileip-hawaii-00, junho, 1999.

[**RS 2000**] Racherla, G.; Saha, D., **Security and Privacy Issues in Wireless and Mobile Computing**. IEEE International Conference. pp. 17-20, dezembro, 2000.

[**SIMUL 2003**] **Simuladores**. Disponível em http://www.slashcat.com/Computers/Data_Communications/Software/. Acessado em maio de 2003.

[**SK 1999**] Sufatrio; Kwok Yan Lam, **Mobile IP Registration Protocol: A Security Attack And New Secure Minimal Public-Key Based Authentication**. Proceedings of 4th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 99), Perth/Fremantle, Australia, June, IEEE Computer Society, pp. 364-369. 1999.

[**SOMMERVILLE 2000**] Sommerville, I., **Engenharia de Software**, 6a. edição, USA, Editora: Addison-Wesley, 2000.

[**STALLINGS 2000**] Stallings, W., **Network Security Essentials: Applications And Standards**. 1. ed. New Jersey: Ed. Prentice-Hall, Inc. 2000.

[**WEB 2002**] Wisely, D.; Eardley, P.; Burness, L., **IP on 3G Networking Technologies for Mobile Communications**. ed. John Wiley & Sons, 2002.

[**XGRAPH 2003**] **Xgraph Web Site**. Disponível em http://www.isi.edu/nsnam/xgraph. Acessado em abril 2003.