Um Suporte Escalável a Mobilidade e Segurança sobre IPv6 †

Frederico Sauer Guimarães Oliveira (1,3)
fsauer@gta.ufrj.br

Aloysio de Castro Pinto Pedroza (1,2)
aloysio@gta.ufrj.br

(1) Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro (UFRJ)
COPPE/PEE – Programa de Engenharia Elétrica
C.P. 68504 – CEP 21945-970 – Rio de Janeiro – RJ – Brasil
(2) Departamento de Eletrônica/EE-UFRJ
(3) Diretoria de Sistemas de Armas da Marinha/DSAM

Resumo

Este trabalho apresenta uma arquitetura para o suporte de mobilidade e segurança sobre o protocolo IPv6, incorporando técnicas de autenticação escaláveis e um gerenciamento de mobilidade transparente para o usuário final. Características como a escalabilidade e a confiabilidade das chaves de criptografia e autenticação são obtidas pela adoção das estruturas hierárquicas de certificação e algoritmos assimétricos. A estratégia de implementação, direcionada para a construção de uma especificação legível e correta, tem apresentado resultados promissores, validados através de ferramentas disponíveis.

Abstract

This work presents an architecture for mobility and security support over the IPv6 network layer protocol, incorporating scalable autentication techniques and a transparent mobility management to the end user. Features like scalability and the reliability of the cryptography and autentication keys are obtained with the adoption of hierarquical certification structures and symmetrical algorithyms. The implementation strategie, towards the construction of a correct and legible specification, presents promissing results, validated with available tools.

1 Introdução

As arquiteturas propostas para mobilidade de nós suportada na camada Internet oferecem, de uma maneira geral, mecanismos para a manutenção de conexões de transporte transparentemente à mudança de localização física dos nós. Uma das dificuldades no provimento deste suporte é a garantia da escalabilidade, de forma que num modelo global, com inúmeros nós móveis, a necessidade de compartilhar segredos para a geração de autenticadores e textos criptografados não inviabilize a adoção da arquitetura original proposta. Este trabalho apresenta uma arquitetura que busca prover um suporte para mobilidade e segurança de nós com transparência às aplicações, e escalabilidade nas mudanças de sub-rede, através do acesso a estruturas hierárquicas de certificação.

Alguns grupos de pesquisa vêm desenvolvendo projetos nesta área. O principal grupo é o coordenado pelo IETF (*Internet Engineering Task Force*), subdividido em dois *workgroups* distintos, um sobre mobilidade (*Mobile IP*) e o outro sobre segurança com cabeçalhos especiais (*IPSec*), abordagem empregada na especificação do IPv6 [1, 2]. Os projetos pioneiros encontrados na literatura são os da Universidade de Columbia, Rutgers e Brown iniciados em meados dos anos 90 [3], que muito contribuíram para os trabalhos atuais. Podem ser também observadas as propostas das Universidades de Stanford [4], Carnegie Mellon [5] e Portland [6], com implementações disponíveis. No Brasil, verificam-se trabalhos

† Este trabalho foi realizado com recursos da UFRJ, FUJB, PROTEM-CC, CNPq, CAPES, COFECUB e DSAM.

interessantes sobre avaliação de desempenho em ambientes móveis [7], e implementação de mobilidade em sistemas de distribuição [8], realizados na Universidade Federal de Pernambuco. Uma fonte de referência relacionada ao trabalho aqui apresentado encontra-se em J. Zao e outros [9], onde é proposta uma arquitetura completa, com a busca da escalabilidade através de extensões ao DNS (*Domain Name System*), incluindo nos registros de um nó a informação necessária à geração de uma chave de sessão.

Este trabalho considera os seguintes pré-requisitos de construção: uso dos mecanismos de segurança oferecidos pelo IPv6; uso de protocolos auxiliares já padronizados ou cuja discussão venha sendo conduzida pelo IETF; e o uso de mecanismos assimétricos para geração de chaves de sessão, não prescindindo assim de contatos diretos entre usuários para troca de "segredos".

Os mecanismos assimétricos devem ser utilizados em função de estruturas hierárquicas de certificação e identificação de usuários por nomes, e não por endereçamento IP, visando aplicações comerciais/pessoais. Além destes aspectos, a arquitetura proposta neste trabalho está sendo desenvolvida com o uso de uma abordagem formal, sendo especificada, validada e implementada com o uso de técnicas e de ferramentas adequadas de suporte ao projeto de sistemas concorrentes.

Este artigo está organizado da seguinte forma. A seção 2 deste trabalho destaca os principais conceitos sobre mobilidade e segurança na camada IP. A seção 3 apresenta a arquitetura proposta, com aspectos peculiares a cada protocolo empregado. Na seção 4 são demonstrados cenários de interoperação, na seção 5 a estratégia de implementação e na seção 6 as considerações finais.

2 Segurança e Mobilidade

Um ambiente móvel implica em requisitos mais severos e específicos do que os encontrados nos ambientes tradicionais. A autenticação de mensagens encontra importância especial, e a mobilidade requer um esquema que possibilite o roteamento de mensagens direcionadas a um nó móvel de maneira transparente às aplicações. Os conceitos empregados neste trabalho para o atendimento destes requisitos são apresentados a seguir.

2.1 Segurança no IPv6

Um dos aspectos da especificação do protocolo Internet para substituição ao IPv4, cuja maior deficiência é o limitado espaço de endereçamento, é o suporte para autenticação e privacidade [1, 2]. Desta maneira, aplicações genéricas podem usufruir deste suporte, sem a necessidade de implementações adicionais. São definidos conceitos específicos como o das Associações de Segurança, referenciados por seus respectivos índices (SPI - *Security Parameters Index*), que identificam univocamente um determinado contexto para o relacionamento seguro entre dois nós. Este contexto inclui o algoritmo utilizado, a chave para criptografia ou autenticação, validade, e outros. O cabeçalho de Autenticação (AH), que implementa este suporte, é ilustrado na figura 1. O escopo da autenticação engloba todo o datagrama, provendo garantia de autenticidade para qualquer aplicação cuja Associação de Segurança com um nó correspondente tenha sido previamente estabelecida. Na figura 2 é ilustrado um exemplo de utilização do cabeçalho para implementação de privacidade (ESP - *Encapsulating Security Payload*), na sua forma mais adequada num ambiente com suporte a mobilidade, onde o pacote criptografado foi previamente autenticado pelo nó correspondente.

O esquema de segurança provido por este novo protocolo é adequado à implementação da mobilidade a nível IP [10].

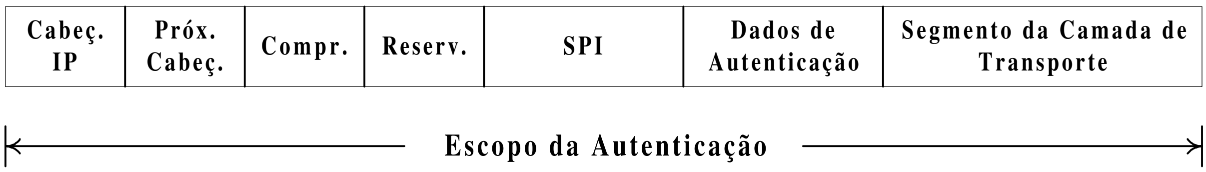

Figura 1 - Datagrama com Cabeçalho AH

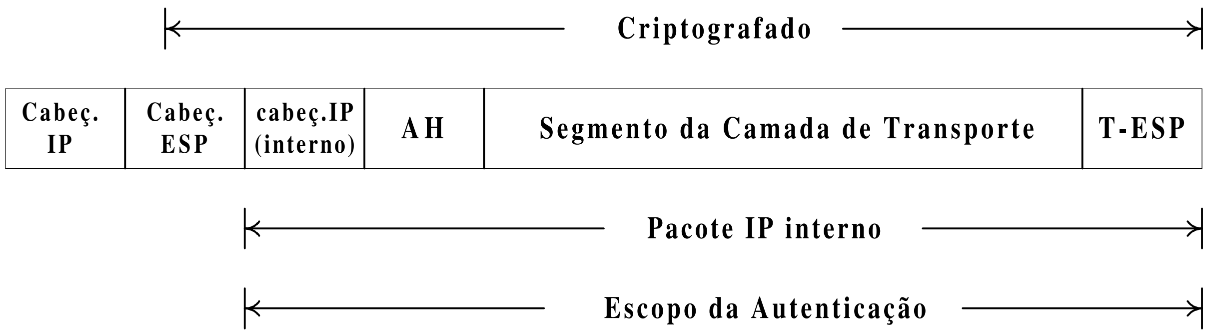

Figura 2 - Datagrama com cabeçalho ESP - modo túnel.

Para a geração de autenticadores de datagramas, foi padronizado como *default* o algoritmo *Keyed-MD5* [11]. Este algoritmo usa um segredo compartilhado entre os nós envolvidos na comunicação (*Key*) e a mensagem, de tamanho variável. A saída deste algoritmo é uma palavra de tamanho fixo. Ao chegar no destino final, a comparação entre o autenticador recebido e o calculado pelo receptor garante que o datagrama foi enviado por alguém que possui o segredo compartilhado, e que o datagrama não foi alterado no trânsito entre a origem e o destino.

As implementações citadas na literatura empregam, de uma maneira geral, o compartilhamento deste segredo através de um contato pessoal (telefonema, por exemplo) [3,4,5,9,12]. Tal esquema não apresenta a escalabilidade requerida a um ambiente de mobilidade global, onde espera-se que o suporte possa ser provido e tarifado por uma sub-rede visitada qualquer, de maneira transparente. Com tal finalidade, adota-se neste trabalho as estruturas hierárquicas de certificação, cujos investimentos tanto da comunidade científica como comercial as tornam bastante promissoras [13,14,15,16]. O principal objeto a ser adquirido nesta hierarquia é um certificado digital, que consiste em um documento autenticado por uma determinada autoridade de certificação. Este certificado possui, entre outras informações, uma informação pública de seu possuidor. Esta informação, usada em conjunto com a sua correspondente parte secreta, possibilita que operações de autenticação e criptografia de chaves sejam realizadas entre dois usuários. Para obtenção dos certificados, a hierarquia é acessada, e, caso um usuário pertença a uma outra esfera de certificação, a autoridade imediatamente superior é responsável pela verificação de sua autenticidade.

2.2 Mobilidade no IPv6

A arquitetura proposta emprega diversos conceitos para a manutenção de conexões durante e após o movimento de nós [3,4,5,9,17,18,19,20]. Como premissa fundamental buscou-se reduzir o número de alterações necessárias em protocolos padronizados, conduzindo à solução adotada. Alguns aspectos importantes da nomenclatura peculiar ao assunto são os seguintes: para que um nó possa alterar o seu ponto de acesso à Internet, é necessário que o mesmo possua dois endereços. O primeiro endereço é o *Home Address*, obtido em sua rede de origem, que identifica univocamente o nó. O segundo endereço é o *Care-of Address*, que deve ser adquirido em cada sub-rede que esteja prestando suporte de mobilidade ao nó móvel. A associação entre estes endereços são denominadas *bindings*, que devem ser armazenados em *cache bindings*. Na situação mais trivial, dois agentes de mobilidade são necessários. O Agente na rede de origem é o *Home Agent*, e o Agente na rede visitada é o *Foreign Agent*. Ao receber um pacote endereçado ao nó móvel, o Home Agent encapsula este pacote e o envia ao nó móvel, endereçado ao seu respectivo endereço *Care-of*. Tendo em vista esta rota deficiente entre o nó móvel e seu correspondente, uma mensagem de atualização de *binding* pode ser enviada pelo nó móvel para o nó correspondente, possibilitando uma otimização no roteamento dos pacotes.

Para implementação deste suporte, são definidas quatro opções especiais a serem enviadas no cabeçalho de opções de destino do IPv6. São elas:

- *Binding Request* - mensagem destinada a solicitar uma atualização de *binding*. Pode ser usada, por exemplo, por *Home Agent* que possua uma entrada desatualizada na sua *binding cache*;
- *Binding Update* - opção que possibilita a criação ou a atualização de uma entrada no *binding cache*. Visando conferir privacidade de localização de nós móveis, apenas estes podem emitir *binding updates*;
- *Binding Acknowledgment* - usado para reconhecer positiva ou negativamente um *Binding Update*; e
- *Home Address* - opção criada para evitar um grande problema encontrado na filtragem por *firewalls* [12], onde um pacote cujo endereço de origem não pertença à sub-rede onde foi originado é descartado. Assim, o nó móvel pode utilizar o seu endereço *Care-of* como origem, e indicar o seu *Home Address* na respectiva opção, permitindo que nós correspondentes que não possuam *binding* para o nó móvel possam identificar o origem do pacote.

Um aspecto importante é a obrigatoriedade de se autenticar os *binding updates*, pois estes permitem o redirecionamento de pacotes de um endereço original para um temporário. Uma vez que não seja comprovada sua autenticidade, o *binding update* deve ser descartado.

3 A Arquitetura Proposta

A adoção de mecanismos assimétricos para obtenção de chaves de autenticação e criptografia implica na obtenção, de maneira segura, da informação pública de um nó qualquer. Além disso, a aquisição de endereços temporários em redes estrangeiras também requer atenção especial, pois a padronização de um mecanismo facilita questões como a tarifação por serviços prestados. Visando atender a estes e a outros pré-requisitos, foi definida a arquitetura proposta. Uma visão direcionada à construção de blocos funcionais é apresentada na figura 3. Nesta figura são apresentados os protocolos auxiliares DHCPv6 [21], LDAP [22], ISAKMP [23] , ICMPv6 [24] e NDP [25], já padronizados ou com padronização iminente, e VC, EC e MS, desenvolvidos para atingir objetivos específicos da arquitetura proposta. Nesta representação, as linhas cheias indicam trocas de mensagens entre módulos pertencentes a entidades pares, em diferentes máquinas, usando os serviços providos pelas camadas inferiores. As linhas tracejadas simbolizam mensagens de sinalização entre módulos de uma mesma máquina.

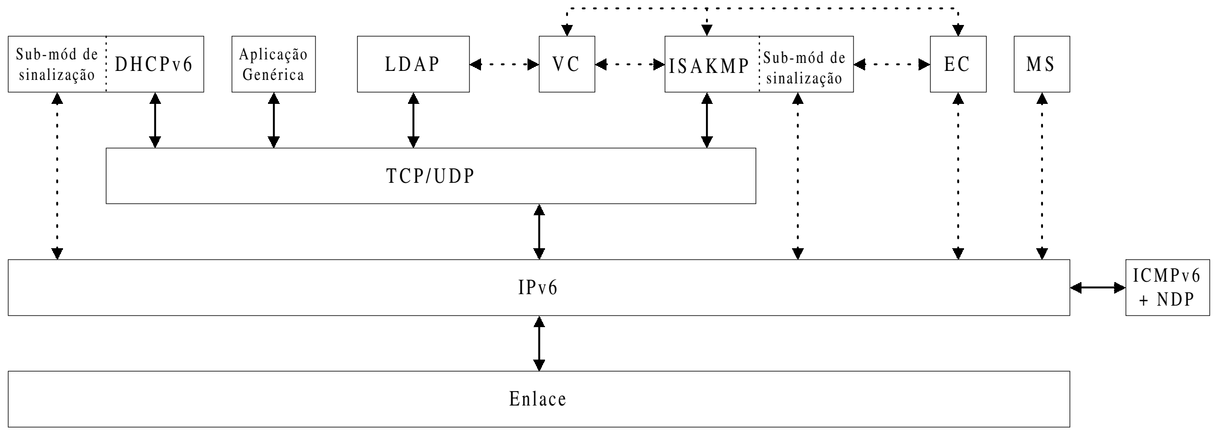

Figura 3 - A Arquitetura Proposta.

As implementações da pilha de protocolos TCP/IP não são tipicamente segmentadas em camadas [26], porém este tem sido um dos objetivos buscados. Tal procedimento facilita a formalização de especificações de protocolos, privilegiando assim a manutenção ou até mesmo a substituição de módulos componentes. As principais características e funções desempenhadas por cada um dos módulos são apresentadas a seguir.

3.1 DHCPv6 - *Dynamic Host Configuration Protocol version 6*

Este protocolo, ainda em discussão no âmbito do IETF, foi adotado na arquitetura proposta com a finalidade de prover aos nós móveis um mecanismo de obtenção de endereços *Care-of*, válidos durante a permanência do nó móvel no alcance de uma rede visitada. Outros mecanismos poderiam ser utilizados, como o *stateless autoconfiguration protocol* [12], por exemplo, mas o DHCPv6 possui um controle mais efetivo sobre a concessão e a posterior liberação de endereços de rede, adequando-se de maneira ideal a tarifação de serviços prestados.

Sua mecânica básica é baseada num modelo cliente/servidor, com mensagens enviadas via UDP. No protótipo em implementação para validação da arquitetura proposta optou-se pela instalação dos servidores DHCP nos *Foreign Agents*, situação que tipicamente deve ocorrer num ambiente real. O DHCP*v6* representa a sua adequabilidade para operação sobre IPv6 e seus endereços de 128 octetos.

3.2 LDAP - *Lightweight Directory Access Protocol*

Uma vez adotadas as estruturas de certificação como repositório de chaves públicas, optou-se por utilizar um protocolo simples para a obtenção de certificados, o LDAP. Este protocolo foi desenvolvido com base no DAP, *Directory Access Protocol*, definido segundo os padrões OSI e direcionado para acesso ao diretório X.500. O LDAP opera diretamente sobre TCP, realizando buscas solicitadas por um cliente através de um servidor, baseadas nos *distinguished names* [27]. Estas chaves de busca permitem uma maior legibilidade às aplicações, além de fornecer a transparência necessária com relação aos extensos endereços IPv6. Uma chave de busca possível seria:

```
CN=João da Silva, O=ACME, C=BR.
```

Estas informações básicas sobre um determinado usuário, nome, organização e país, são suficientes para a obtenção do certificado caso o mesmo exista, e o endereço IP do seu equipamento seria um dos atributos deste documento.

Na arquitetura proposta, este módulo se utiliza de uma interface especificamente definida para verificar a validade de certificador obtidos, o VC (Verificador de Certificados), detalhado a seguir.

3.3 VC - Verificador de Certificados

Os certificados obtidos pelo LDAP cliente possuem informações sobre o usuário cujo relacionamento seguro é requerido. Desta forma, o Verificador de Certificados realiza a validação do mesmo. Caso seu autenticador tenha sido emitido por uma autoridade cujo certificado ainda não esteja armazenado, o mesmo deve ser recursivamente obtido e validado para garantia da autenticidade do certificado desejado. Além disso, este módulo provê a interface de sinalização necessária a outro módulo, o ISAKMP.

3.4 ISAKMP - *Internet Security Association and Key Management Protocol*

A especificação do IPv6 observa que os protocolos para estabelecimento de Associações de Segurança, criação e gerenciamento de chaves de sessão entre nós seguramente correspondentes deve ser definida à parte do IP. Tal preocupação se justifica pela necessidade de manter um acompanhamento mais próximo dos mecanismos de criptografia e autenticação, que evoluem em função do *hardware* disponível para seu processamento [28]. Entre algumas propostas encontradas na literatura, destaca-se a do ISAKMP, por sua detalhada especificação e algumas implementações disponíveis.

Este módulo realiza as seguintes operações:

- obter o certificado do nó correspondente, via VC;
- possuindo a informação pública do nó correspondente, gerar a chave de sessão através do EC (detalhado no próximo sub-ítem) e enviá-la criptografada ao nó correspondente;
- esta chave criptografada é enviada junto com outros detalhes deste relacionamento, como algoritmo a ser usado e a validade da Associação de Segurança (AS), entre outras informações, definindo todo um contexto identificado por um SPI; e
- após a verificação da autenticidade da mensagem recebida, o nó correspondente envia uma mensagem de resposta aceitando ou não a AS proposta.

Um aspecto importante a ser ressaltado é que esta AS é unidirecional, e caso a aplicação respondedora deseje enviar pacotes (de maneira segura) para o nó iniciador, uma outra AS neste sentido deve ser negociada e estabelecida.

3.5 Engenho Criptográfico (EC)

O Engenho Criptográfico contém os algoritmos a serem implementados na arquitetura. A princípio, o *Keyed-MD5* foi escolhido para autenticação e uma interface para o IDEA (possivelmente em *hardware* [29]) para criptografia. É importante ressaltar que isso não elimina a possibilidade da incorporação de outros algoritmos. Além de prestar serviços ao ISAKMP e VC, o EC também é usado internamente para geração de autenticadores e criptografia de datagramas para o IPv6 local.

3.6 Suporte a Mobilidade com Segurança (MS)

As propostas encontradas na literatura direcionam a solução para o problema de prover a mobilidade através incorporação desse suporte ao *Kernel* do sistema operacional. A figura 4 ilustra uma possível arquitetura de implementação para este suporte.

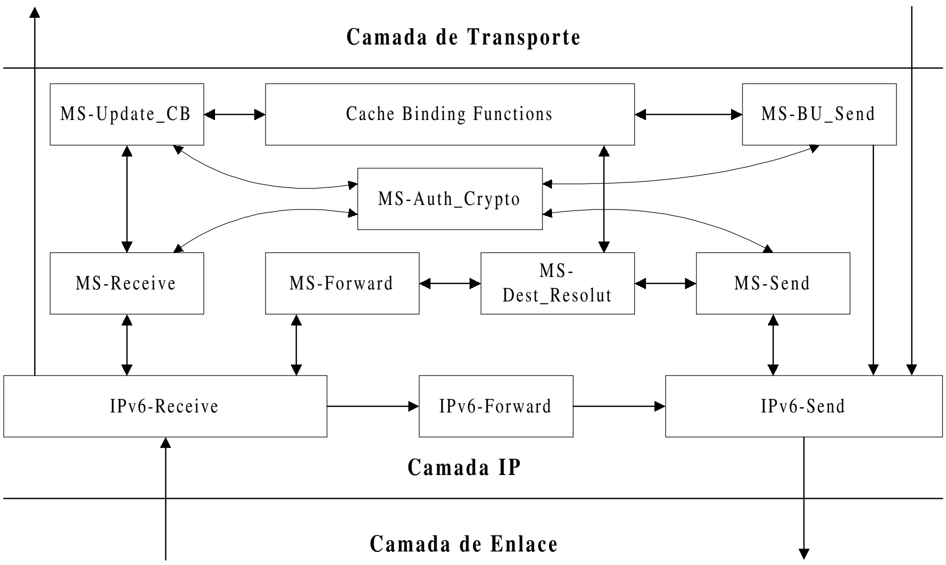

Figura 4 - Implementação de mobilidade no IP.

Nesta arquitetura de implementação, os blocos funcionais IPv6-Receive e IPv6-Send, usuais ao IPv6 especificado, possuem interfaces com outros blocos responsáveis por gerenciar mobilidade, realizando as seguintes funções:

- MS-Receive - possuindo uma das opções de destino citadas no sub-ítem 2.2, o datagrama seria entregue a este módulo para tratamento;
- MS-Update_CB - tratando-se de um *binding update*, este módulo se encarregaria de realizar o acesso às tabelas (*cache binding*) para atualização;
- MS-Auth_Crypto - módulo de interface para a obtenção de autenticadores para o envio em datagramas e para a sua comparação a um recebido;
- Cache Binding Functions - funções de manutenção interna do *cache binding*, por exemplo, como a verificação da expiração de *timeouts*;
- MS-Send - tratando-se de um datagrama para enviar uma das opções de destino relacionadas à mobilidade, este módulo se encarrega de construí-las;
- MS-BU_Send - caso o datagrama deva ser enviado a um nó móvel, esta função consulta o *cache binding* para verificar a existência de um *binding* para o endereço de destino;
- MS-Forward - função usada para re-roteamento de datagramas, para consulta prévia ao *binding cache*, visando o seu envio a um nó móvel (tipicamente realizada pelos *Home Agents*); e
- MS-Dest_Resolut - função que efetivamente resolve o endereço *Home Address* de um nó móvel em um endereço *Care-of*.

Dessa maneira, caso um datagrama não possua opções de destino relacionadas com mobilidade, é entregue à “camada” de transporte. Caso contrário, é tratado pelos sub-módulos acima, peculiares ao protocolo MS. Como estratégia de validação, optou-se por modelar estas funções à parte do IPv6, abstraindo-se de funções já exaustivamente tratadas, como fragmentação, roteamento, etc.

As funções a serem exercidas pelo módulo MS são basicamente as seguintes:

- ao receber um anúncio de disponibilidade de um Agente de Mobilidade, buscar a obtenção de um endereço *Care-of*;
- após obter este endereço, registrá-lo junto ao seu *Home Agent*;
- ao receber uma mensagem de uma aplicação genérica, buscar o estabelecimento de uma Associação de Segurança (AS) com o nó correspondente;
- ao receber datagramas de um nó correspondente encapsulados pelo *Home Agent*, otimizar o roteamento com o envio de um *binding update* ao nó correspondente;
- após o estabelecimento da AS, ao receber uma mensagem da aplicação, buscar a geração de um autenticador para o datagrama que o conduzirá; e
- ao retornar para sua rede de origem, o nó móvel se registra novamente com o *Home Agent*, passando assim a receber diretamente os pacotes endereçados ao seu *home address.*

Estas funções espelham o comportamento do protocolo como iniciador da comunicação. Além dessas funções, todo o procedimento como respondedor também é previsto no seu detalhamento. Deve-se também ressaltar que o gerenciamento da tabela de *cache bindings* é realizado por este módulo.

3.7 IPv6 - Internet Protocol version 6

Em adição às características já especificadas para o novo protocolo *Internet*, salienta-se a criação das novas opções, já apresentadas no sub-ítem 2.2. Destas opções, para um suporte global a mobilidade, na verdade apenas a *Home Address* é mandatória. Não havendo o reconhecimento das mensagens de *binding*, o único inconveniente é o roteamento deficiente. Porém, caso todos os nós reconheçam a opção *Home Address*, nós móveis sempre poderão destinar datagramas a nós correspondentes usando os endereços *Care-of* como fonte, pois a opção de destino presente permitirá o reconhecimento correto do nó de origem e seu devido tratamento pelas aplicações. Outro aspecto importante é o da utilização dos cabeçalhos de autenticação e de encapsulamento para a provisão do nível de segurança da arquitetura proposta.

3.8 ICMPv6 - *Internet Control Message Protocol version 6*

O protocolo de mensagens de controle é conceitualmente posicionado na pilha TCP/IP na camada Internet, conforme ilustrado na figura 3. Havendo uma mensagem ICMP a transmitir, a mesma é encapsulada em um datagrama IP, da mesma forma que uma mensagem UDP ou TCP.

A principal diferença entre o ICMP para o IPv4 e o ICMPv6 é a incorporação das funções exercidas anteriormente pelo IGMP (*Internet Group Management Protocol*), visando um suporte global ao *multicast*. Sua função é reportar erros encontrados no processamento de pacotes e executar outras funções do nível de rede, como diagnósticos (*ping*). Sua implementação é mandatória para nós IPv6.

Visando o suporte à descoberta de Agentes pelos nós móveis, bem como o tratamento dos *handoffs*, optou-se pela incorporação das mensagens do NDP pelo ICMPv6 na arquitetura proposta.

3.9 NDP - *Neighbor Discovery Protocol*

O NDP é um protocolo que define mensagens particularmente interessantes para a arquitetura proposta. Com o NDP, a resolução de endereços passa a ser feita na camada Internet, em substituição ao ARP (*Address Resolution Protocol*), que nas arquiteturas tradicionais funciona a nível de enlace. Isto é feito através de uma mensagem *Neighbor Solicitation*, que é respondida por um *Neighbor Advertisement* contendo o endereço de enlace do nó. Este procedimento é vantajoso, pois com o posicionamento da resolução de endereços na camada ICMP, a arquitetura fica mais independente do enlace que no caso do ARP, além de tornar possível o uso dos mecanismos de segurança do IPv6 nas suas mensagens. Além disso, as mensagens de descoberta de roteadores (*router discovery*) são ferramentas de grande utilidade para que o nó móvel descubra sua visita a uma rede estrangeira e seu retorno à rede de origem. As mensagens do procedimento de *Neighbor Unreachability Detection* (NUD) são responsáveis pelo rápido tratamento dos *handoffs* [12]. Isso confere mais robustez à arquitetura no caso de falhas em roteadores e locomoção de nós, uma vez que o NUD indica com mais rapidez a falha (ou mudança de localização) em comparação ao controle pelo TCP, permitindo assim a interrupção do fluxo e a busca de um novo roteador.

A arquitetura proposta integra os módulos visando o pleno atendimento não só das situações normais de comunicação entre nós através da Internet como do suporte a mobilidade e segurança. Para ilustrar as situações de operação nesta arquitetura, serão apresentados a seguir três cenários típicos da mobilidade de nós: o registro de um nó móvel com o Agente de Mobilidade em sua rede de origem, após uma locomoção para outra rede, o uso do suporte em questão na operação de uma aplicação qualquer e a implementação de otimizações no roteamento entre o nó móvel e o nó correspondente.

4 Cenários de Interoperação

O objetivo de definir módulos delimitados, com funções peculiares e interações bem definidas, é permitir o emprego de técnicas formais de validação, extremamente úteis por evitar que as implementações possuam inconsistências com o modelo original. Serão apresentados a seguir cenários de interoperação entre os módulos, primeiro passo para a simulação da arquitetura proposta.

4.1 Registro de Um Nó Móvel

A fase preliminar do suporte a mobilidade é o registro autenticado do nó móvel com um Agente de Mobilidade em sua rede de origem. A partir deste registro, os pacotes endereçados a um nó que tenha se movimentado para outra rede podem ser redirecionados para o seu endereço *Care-of*. A figura 5 ilustra as interações entre os módulos da arquitetura envolvidos neste procedimento. As numerações que acompanham as setas buscam permitir o acompanhamento da sequência das interações.

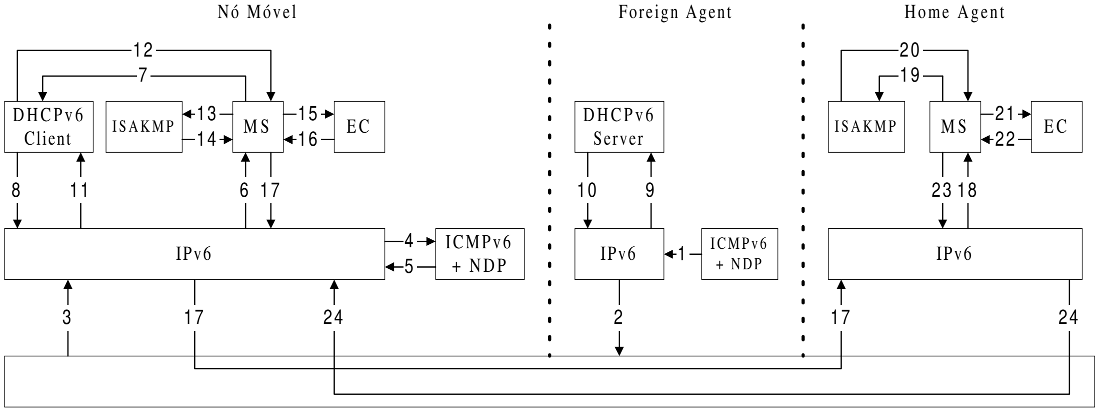

Figura 5 – Registro de um nó móvel na Arquitetura Proposta.

Ao sair do alcance de sua rede local, o nó móvel perde suas conexões. Ao entrar em contato com outra rede (estrangeira), que fornece serviços de mobilidade, o nó móvel pode requisitar explicitamente um *Agent Advertisement* através do ICMPv6 ou receber um dos periódicos *Agent Advertisement* emitidos por um Agente de Mobilidade na rede estrangeira (1,2). O IP do nó móvel recebe este datagrama (3), que é processado pelo ICMPv6 (4). Uma vez interpretado como um *advertisement* (5,6), o módulo MS inicializa o cliente DHCPv6 (7), que realizará os passos necessários à obtenção do endereço *Care-of*, retornando-o ao MS (12), após a negociação com o DHCPv6 Server (8, 9, 10, 11). Após isso, o MS inicializa o módulo ISAKMP (13) para seleção da Associação de Segurança com o *Home Agent* adequada (13,14), que já existe neste cenário hipotético. O MS obtém o autenticador da mensagem de registro (*binding update)* junto ao EC (15, 16). O datagrama é então enviado ao *Home Agent* (16, 17) que, ao recebê-lo, aciona o módulo ISAKMP (18, 19). Em seguida, o MS do nó correspondente seleciona a Associação de Segurança entre o nó móvel e ele (20), obtém o autenticador do datagrama que contém o *binding update* através do EC (21, 22), compara-o ao autenticador enviado, e manda um *binding acknowledgement* ao nó móvel (23, 24).

4.2 Operação de uma Aplicação Genérica

Para melhor ilustrar o suporte de segurança da arquitetura proposta para a operação de aplicações genéricas, a figura 6 apresenta as possíveis interações entre um nó móvel, seu correspondente e o *Home Agent* do nó móvel.

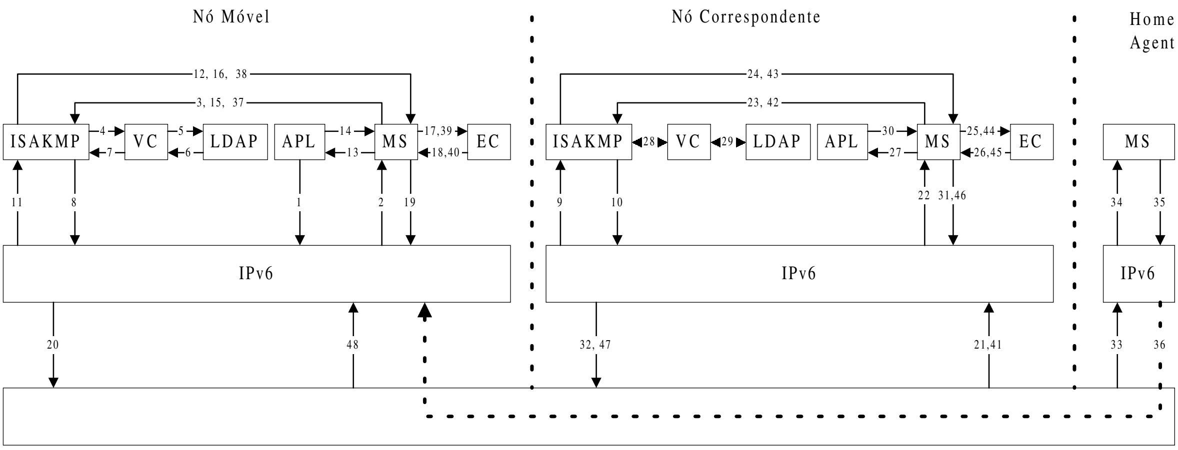

Figura 6 - Aplicação Genérica na Arquitetura Proposta

Supondo-se que uma determinada aplicação qualquer de um nó móvel deseja contactar a aplicação de um nó correspondente, usando o serviço de segurança provido pela arquitetura proposta, serão realizadas as seguintes interações: o IP do nó móvel, ao indicar esta necessidade (1), aciona o MS (2), que realiza as operações para verificar junto ao ISAKMP (3) se há uma Associação de Segurança válida para o nó de destino. Supondo-se que a mesma ainda não exista, e que o nó móvel não possua um certificado válido para o nó correspondente, o ISAKMP o solicita para o VC (4). Este, por sua vez, aciona o cliente LDAP (5) para obtê-lo na hierarquia de certificação através do servidor LDAP.

Neste cenário, considera-se que o nó móvel já está registrado com o seu *Home Agent* de acordo com os procedimentos ilustrados no cenário anterior. Desta forma, o servidor LDAP a ser consultado é o da sua rede de origem. Uma vez obtido o certificado desejado (6), este é verificado pelo VC e entregue ao ISAKMP (7). O ISAKMP do nó móvel negocia então com o ISAKMP do nó correspondente, via UDP, uma Associação de Segurança para este relacionamento. Estas transações são representadas de forma simplificada por 8, 9, 10, e 11.

O MS, então, ao receber a sinalização do ISAKMP que já existe uma AS para o nó móvel (12), indica para a aplicação que o relacionamento já está seguro (13). Ao receber uma mensagem da aplicação (14), o MS acessa o ISAKMP (15) para obter o Índice de Parâmetros de Segurança (SPI), definido na AS negociada (16). O MS então pode acessar o módulo responsável pelas operações de criptografia e autenticação (EC) para realizar as proteções necessárias (17, 18). O datagrama conduzindo a mensagem da aplicação é enviada para o nó correspondente (19, 20). Ao recebê-lo (21, 22), o MS do nó correspondente verifica junto ao ISAKMP o SPI indicado (23, 24), e ao receber sua confirmação, acessa o EC (25, 26) para realizar as verificações de autenticidade e/ou decifragens, repassando a mensagem já devidamente tratada à aplicação (27).

Pela especificação do IPv6 [2], as AS são unidirecionais, isto é, caso a aplicação do nó correspondente deseje retornar mensagens para a aplicação do nó móvel com segurança, procedimento simétrico ao detalhado acima deve ser executado, ou seja, do nó correspondente para o nó móvel. Neste caso, não é necessária a obtenção do certificado, pois o mesmo já teria sido obtido no contato anterior entre as entidades (28, 29).

4.3 Otimizações no Roteamento entre o Nó Correspondente e o Nó Móvel

Após o estabelecimento do relacionamento seguro entre o nó móvel com o nó correspondente, a aplicação deste último envia suas mensagens já com o suporte de segurança da arquitetura proposta. No sentido inverso, como o nó correspondente não possui o endereço *Care-of* do nó móvel, o pacote é roteado para a sua rede de origem (30, 31, 32, 33). O Agente de Mobilidade captura o pacote, o encapsula, e reenvia para o nó móvel via túnel (34, 35, 36). O MS do nó móvel então, após o desencapsulamento do pacote, além de efetuar as operações de verificação de autenticidade e/ou criptografia através do EC, e entregá-lo à aplicação, iniciará a seguinte operação de otimização no roteamento: acesso ao ISAKMP para obtenção do SPI (37, 38); acesso ao EC (39) para cálculo do autenticador do *binding update* a ser enviado em um datagrama com o cabeçalho de opções de destino, no cabeçalho de autenticação (40).

O MS do nó correspondente, ao receber o datagrama (41), realiza procedimento simétrico ao apresentado acima, acessando o ISAKMP (42, 43), EC (44, 45), e verificando a autenticidade do *binding update* recebido. Em seguida, registra este endereço *Care-of* e envia um datagrama autenticado para o nó móvel com o *binding acknowledgement* no cabeçalho de opções de destino, diretamente para o nó móvel (46, 47, 48). Deste ponto em diante, os datagramas do nó correspondente para o nó móvel podem ser roteados para o endereço *care-of*, otimizando a rota de entrega dos pacotes.

Convém observar no cenário descrito a simetria obtida nas interações entre os módulos componentes da arquitetura, tornando assim menos particular uma implementação dos protocolos, de acordo com a função exercida pelo *host* (nó móvel ou estacionário).

5 Estratégia de Implementação

Como estratégia para implementação da arquitetura proposta, optou-se por uma abordagem formal, com validações realizadas em cada fase do desenvolvimento do projeto. Para isso, foram definidas as seguintes etapas:

- construção das máquinas de estados finitos (MEF) dos protocolos (módulos funcionais), baseadas nas especificações informais;
- tradução das MEF obtidas em Redes de Petri, com a subseqüente validação por intermédio de ferramentas disponíveis;
- especificação detalhada em Estelle das máquinas de estado validadas no passo anterior;
- simulação e submissão a seqüências de testes da especificação obtida através de ferramentas específicas para o desenvolvimento de protocolos; e
- após validada e exaustivamente testada a especificação, implementação semi-automática da arquitetura.

Para exemplificar a aplicação da metodologia acima, as figuras 7 e 8 ilustram, respectivamente, as máquinas de estado de iniciador e respondedor do protocolo MS. A Rede de Petri que traduz estas máquinas foi construída a partir dos estados e transições destas máquinas, e a sua validação foi realizada através da ferramenta ARP [30], disponível por ftp. Os resultados obtidos foram os seguintes:

- rede com 363 estados alcançáveis;
- viva;
- reinicializável;
- estritamente conservativa;
- sem *livelocks* ou *deadlocks*, ou seja, com todas as boas propriedades que são esperadas de um protocolo corretamente especificado.

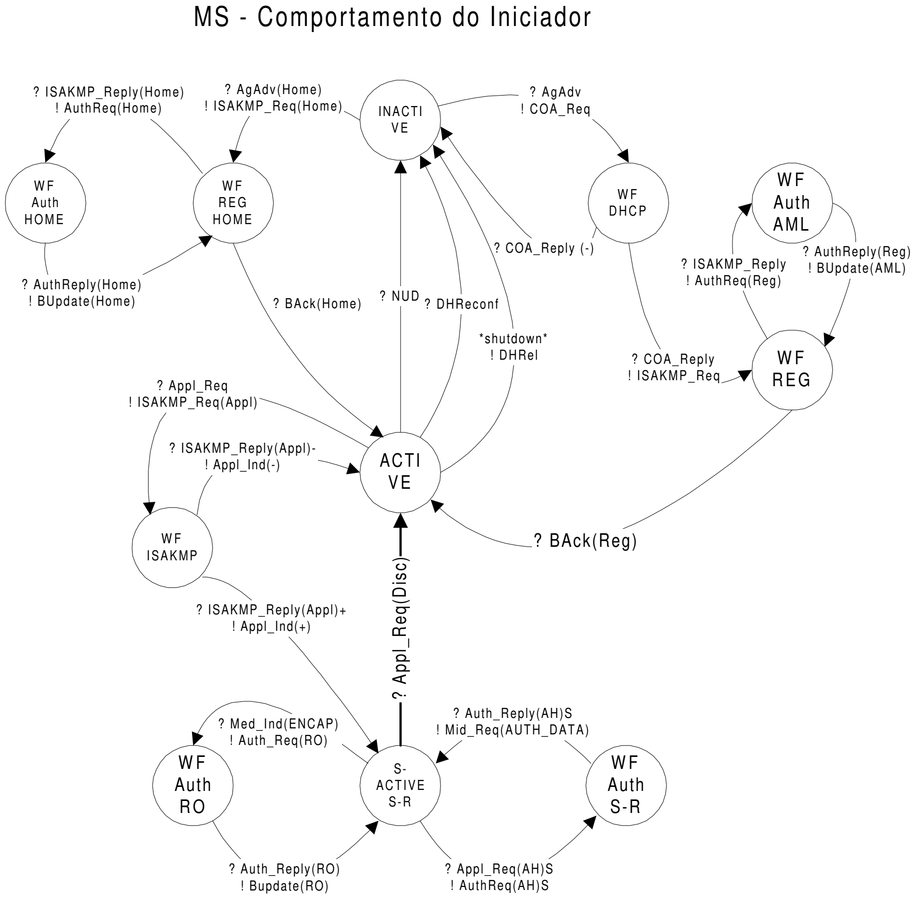

Figura 7 - MEF do protocolo MS - Comportamento do Iniciador.

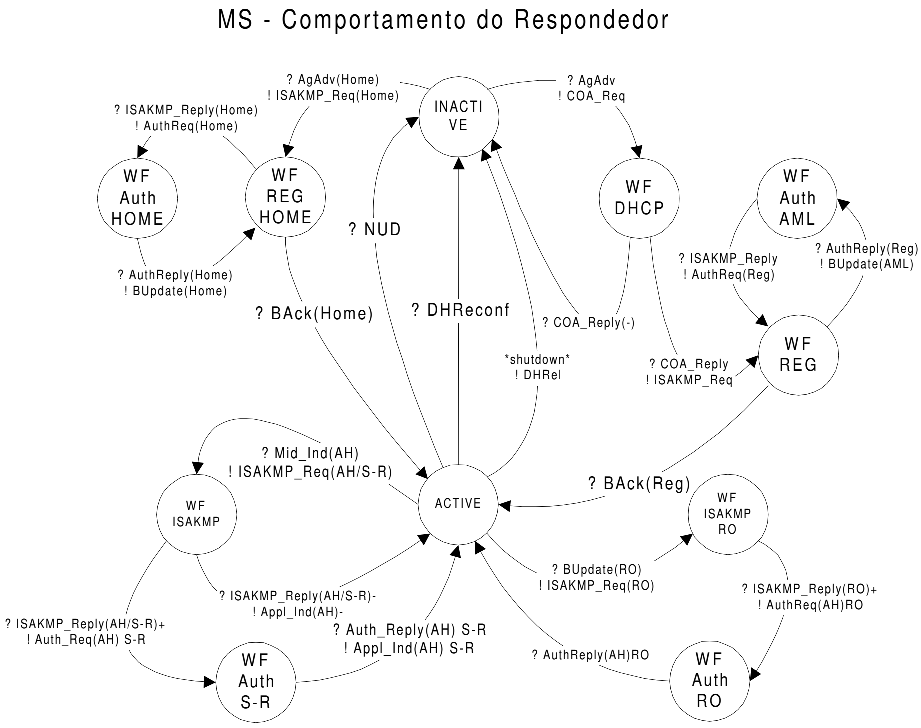

Figura 8 - MEF do protocolo MS - Comportamento do Respondedor

6 Considerações Finais

A arquitetura proposta visa a provisão do suporte a mobilidade e segurança no ambiente Internet, utilizando como base o IPv6. Esta arquitetura se baseia nos conceitos empregados nos mecanismos assimétricos para autenticação e criptografia, e no uso de estruturas hierárquicas de certificação para o uso de certificados padrão OSI, de forma a conferir um alto nível de escalabilidade ao modelo.

Podem ser citadas como vantagens nesta arquitetura: as únicas modificações a serem feitas no IPv6 são a capacidade de armazenar e consultar os *cache bindings*, o reconhecimento de novas opções de destino e as interfaces com os módulos auxiliares. O restante do suporte é provido pelos cabeçalhos já definidos. O uso do ICMPv6 com as mensagens do NDP dão uma característica mais apta a administrar conexões via *Neighbor Unreachability Detection* em comparação aos controles de fluxo intrínsecos ao TCP. O uso de um protocolo para busca e gerenciamento de certificados, o LDAP, foi adotado devido aos esforços e investimentos realizados no sentido de viabilizar uma estrutura hierárquica de certificação, bem como a compatibilidade com o esquema de diretórios X.500 da OSI. O embasamento nos *distinguished names* para identificação de usuários, e não nos extensos endereços do IPv6, privilegia aplicações com finalidades comerciais e bancárias, com características mais pessoais, podendo consultar os certificados de forma mais amigável.

A estratégia de implementação, definida em função da exaustiva validação passo-a-passo dos módulos da arquitetura proposta, tem conduzido a resultados bastante promissores, a nível de simulação da interoperação entre os protocolos componentes, privilegiando a construção de um modelo global de arquitetura com uma especificação legível e correta, capaz de ser implementada em qualquer linguagem de programação. Este trabalho encontra-se atualmente na fase final das validações das Redes de Petri que traduzem as máquinas de estados finitos (MEF) dos protocolos.

Referências

[1] S. Bradner e A. Mankin, "RFC-1752 - The Recommendation for the IP Next Generation Protocol". *Internet RFC.* janeiro de 1995.

[2] W. Stallings, "IPv6: The New Internet Protocol". *IEEE Comunications Magazine*, setembro de 1996.

[3] C. E. Perkins, "Mobile IP: Design, Principles and Practices". *Addison-Wesley*, 1998.

[4] S. Cheshire e M. Baker, "Internet Mobility 4 x 4". *SIGCOMM'96*, agosto de 1996.

[5] D. B. Jonhson, A. Myles e C. Perkins, "A Mobile Host Protocol supporting Route Optimization and Autentication." *IEEE Journal of Selected Areas in Communications*, junho de 1995.

[6] J. R. Binkley e J. Mc. Hugh, "Secure Mobile Networking - Winter 1997". *Technical Report*, Portland State University, abril de 1997.

[7] R. W. S. Rodrigues, A. A.Souza e J. A. S. Monteiro, "Simulando um Protocolo da Camada de Rede que Suporta a Comunicação Móvel". *Anais do 14º Simpósio Brasileiro de Redes de Computadores*, 1996.

[8] A. A. de Souza, "Uma Extensão da Plataforma de Distribuição ANSAware para Suportar a Computação Móvel".*Dissertação de Mestrado* - UFPE, 1996.

[9] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan e I. Castineyra, "A Public-Key Based Secure Mobile IP". *Proceedings of the Third Annual International Conference on Mobile Computing and Networking - MOBICOM 97*, setembro de 1997.

[10] F. S. G. Oliveira e A. C. P. Pedroza, "Suporte para Segurança e Mobilidade no IPv6". *Anais do 2º Seminário Franco-Brasileiro de Sistemas Informáticos Distribuídos*, novembro de 1997.
[11] Metzer e Simpson, "RFC-1828 - IP Authentication using *Keyed* MD5". *Internet RFC*, agosto de 1995.
[12] C. Perkins e D. B. Johnson, "Mobility Support in IPv6". *Proceedings of the Second Annual International Conference on Mobile Computing and Networking - MOBICOM 96*, novembro de 1996.
[13] M. Gehrke e T. Hetschold, "Management of a Public Key Certification Infraestructure - Experiences from the DeTeBerkom project BMSec". *Computer Networks and ISDN Systems* 28 (1996) 1901-1914.
[14] S. Kolletzki, "Secure Internet banking with Privacy Enhanced mail - A protocol for reliable exchange of secured order forms". *Computer Networks and ISDN Systems* 28 (1996) 1891-1899
[15] D. W. Chadwick, A. J. Young e N. K. Cicovic, "Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model". *IEEE Network*, maio/junho de 1997.
[16] W. Stallings. "Network and Internetwork Security". *Prentice-Hall*, 1995.
[17] C. Perkins, "Mobile IP". *IEEE Communications Magazine*, maio de 1997.
[18] C.Perkins, "RFC-2002 - IP Mobility Support". *Internet RFC*, setembro de 1996.
[19] F. Teraoka, K. Uehara, H. Sunahara e J. Murai, "VIP: A Protocol Providing Host Mobility". *Communications of the ACM*, agosto de 1994.
[20] A. Myles e D. Skellern, "Comparing four IP based mobile host protocols". *Computer Networks and ISDN Systems*, 26 (1993) 349-355.
[21] J. Bound e C. Perkins, "Dynamic Host Configuration Protocol for IPv6 (DCHPv6)". *IETF Working Draft (work in progress)*, novembro de 1997.
[22] W. Yeong, T. Howes e S. Kille, "RFC-1777 – Lightweight Directory Access Protocol". *Internet RFC*, março de 1995.
[23] D. Maughan, M. Schertler, M. Schneider e J. Turner, "Internet Security Association and Key Management Protocol", *IETF IPSEC Working draft (work in progress)*, julho de 1997.
[24] A. Conta e S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification". *Internet RFC*, dezembro de 1995.
[25] T. Narten, E. Nordmark e W. Simpsom, "RFC-1970 – Neighbor Discovery for IP Version 6 (IPv6)". *Internet RFC*, agosto de 1996.
[26] C. Huitema, "Routing in the Internet". *Prentice-Hall*, 1995.
[27] S. Kille, "RFC-1779 - A String Representation of distinguished Names". *Internet RFC*, março de 1995.
[28] R. M. Needham, "The Changing Environment for Security Protocols". *IEEE Network*, maio/junho de 1997.
[29] S. L. C. Salomão, "Uma Proposta em Hardware para o Algoritmo Criptográfico IDEA".*Tese de Mestrado* – PEE/COPPE/UFRJ, Rio de Janeiro, dezembro de 1997.
[30] ARP - Analisador de Redes de Petri - Laboratório de Controle e Microinformática do Departamento de Engenharia Elétrica da Universidade Federal de Santa Catarina - 1995.