Uma Arquitetura para Suporte a Segurança e Mobilidade 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
Tel: (021) 260-5010 Fax (021) 290-6626
(2) Departamento de Eletrônica/EE-UFRJ
(3) Diretoria de Sistemas de Armas da Marinha/DSAM

Resumo

Este trabalho apresenta a proposta de uma Arquitetura para Suporte de Segurança e Mobilidade sobre o serviço IPv6, integrando protocolos e conceitos sobre autenticação e criptografia. Como resultado, obteve-se uma plataforma que busca permitir a operação de uma aplicação genérica, de maneira escalável e segura, mesmo quando os nós se deslocam de suas redes de origem. Cenários de interoperação são apresentados, para ilustrar o funcionamento da arquitetura.

Abstract

This work presents a proposal of an Architecture for Security and Mobility support over the IPv6 service, integrating protocols and concepts on authentication and cryptography. As a result, we obtained a platform that searches for the operation of any generic application, on a secure and scalable way, even when hosts move away from their home networks. Interoperation scenes are showed to ilustrate the operation of the architecture.

1 Introdução

A mobilidade de nós que se comunicam através da Internet vem sendo um assunto de grande interesse, em função da redução do porte dos equipamentos e da melhoria dos enlaces sem fio. Sua implementação implica na necessidade de um suporte robusto para segurança das informações em tráfego, possivelmente via rádio, facilitando a atividade de intrusos em escuta passiva. A autenticação de mensagens é também um aspecto vital, uma vez que os nós móveis podem acessar suas redes de origem a partir de qualquer rede que forneça suporte à mobilidade.

As propostas mais aceitas encontradas na literatura indicam a absorção do suporte para mobilidade e segurança pela camada IP (*Internet Protocol*), pois assim, uma aplicação genérica pode usufruir de seus benefícios sem implementações adicionais específicas a estas aplicações. As discussões conduzidas pelo IETF (*Internet Engineering Task Force*) voltadas para o desenvolvimento de uma nova versão do IP levaram em consideração o suporte à mobilidade, e principalmente o suporte à segurança [1]. Além disso, podem ser encontrados vários trabalhos de implementação nesta área, como os projetos das Universidades de Stanford [2], Carnegie Mellon [3] e Portland [4]. A proposta de Portland, em particular, já apresenta como resultado um protocolo IP seguro (IPSEC) portado para *FreeBSD*. Na BBN *Corporation* vem sendo implementado um IP com mobilidade e segurança baseada em chaves públicas armazenadas numa extensão ao DNS [23]. No Brasil, pode ser citada a pesquisa sobre o desempenho do protocolo em mobilidade VIP, feito na Universidade Federal de Pernambuco [5]. Estes trabalhos são, de uma forma geral, concentrados apenas no protocolo IP, sem uma visão mais arquitetural do problema, com exceção da proposta da BBN.

Este trabalho apresenta uma arquitetura com os seguintes pré-requisitos de construção: uso dos mecanismos de segurança oferecidos pelo IPv6, para aproveitar a ocasião de sua iminente utilização, em substituição ao IPv4; uso dos protocolos auxiliares em discussão no âmbito do IETF; uso de mecanismos assimétricos para geração de chaves de sessão, para não prescindir 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 números IP, visando as aplicações comerciais/pessoais. Outro objetivo foi desenvolver o projeto com o uso de uma abordagem formal.

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 mostrados alguns cenários de funcionamento e na seção 5 encontram-se os comentários finais.

2 Mobilidade e Segurança

Nós Internet dotados de mobilidade exigem características especiais visando conferir segurança às transações. A capacidade de movimentarem-se, e mesmo assim continuarem a manter conexões com outros nós facilitam a ação de intrusos na falsificação da identificação de usuários junto a outros nós. Neste contexto, utiliza-se a autenticação e a criptografia de mensagens como procedimentos adequados a evitar-se a ação de intrusos [17]. A abordagem adotada para o emprego de autenticações e para a criptografia de mensagens na arquitetura proposta utiliza mecanismos assimétricos e estruturas hierárquicas de certificação. Estes conceitos encontram-se detalhados a seguir.

2.1 Mobilidade no IPv6

O ponto de partida para o desenvolvimento do projeto da arquitetura, no que concerne a mobilidade, foi a opção pela adoção de alguns conceitos básicos, acompanhados de sua respectiva nomenclatura. Estes conceitos foram extraídos de propostas que implementam a mobilidade na camada de rede [2,3,9,12,13,23,27,28].

Nos trabalhos usados como referência, observa-se que o princípio básico é o de se manter o endereço IP mesmo quando o nó móvel estiver visitando uma outra rede, pertencente a outro domínio. Com isso, conexões oriundas de aplicações que buscam um determinado endereço pré-configurado não seriam quebradas. Este endereço é conhecido como *home address*, que permanece inalterado independentemente de alterações do ponto de conexão do nó à Internet. Os mecanismos padrão de roteamento [22] enviam todos os pacotes destinados ao nó móvel para a sub-rede indicada por este endereço. Qualquer nó com o qual o nó móvel está se comunicando é denominado nó correspondente, que por sua vez pode ser móvel ou estacionário.

A localização corrente do nó móvel que encontra-se fora de sua rede local é conhecida por endereço *care-of*, que é um endereço adquirido pelo nó móvel na rede por ele visitada, denominada de rede estrangeira. A associação entre o *home address* e o seu endereço *care-of* é chamado de *binding*.

Um roteador na rede de origem do nó móvel atua como seu *home agent*, mantendo um registro do seu *binding* corrente. O *home agent* então intercepta os pacotes endereçados para o *home address* do nó móvel e os envia via *tunnel* por encapsulamento para o endereço *care-of* do nó móvel. Uma vez que o nó correspondente possua um *binding* para o nó móvel, este então poderá passar a enviar os pacotes diretamente para o endereço *care-of* do nó móvel, eliminando assim uma das maiores dificuldades observadas na provisão do suporte a mobilidade, conhecida como triângulo de roteamento, ilustrado na figura 1. A consequência desta situação é a caracterização de uma rota não-ótima, com aumento na carga da rede e nos retardos na entrega de pacotes.

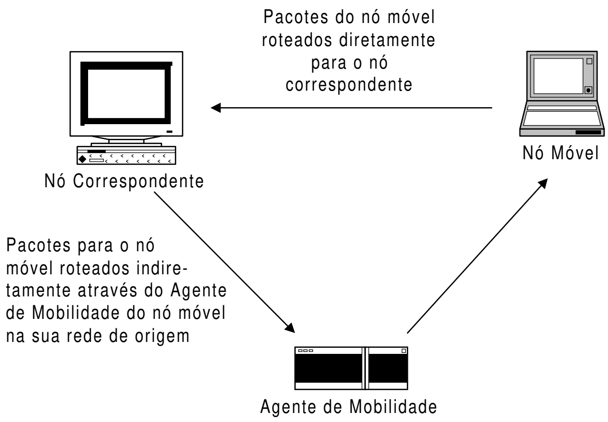

Figura 1 – Triângulo de roteamento.

Para as funções descritas acima, pode-se empregar os mecanismos disponíveis no IPv6 [6], com alguns passos extras destinados ao armazenamento e utilização dos endereços *care-of* para cada nó móvel com o qual ele esteja se comunicando, uma vez que a sobrecarga provocada por estes passos é muito pequena [12]. Além disso, o suporte à mobilidade no IPv6 introduz um conjunto de novas opções de destino, chamadas *binding request*, *binding update* e *binding acknowledgement* , para gerenciar as entradas dos *cache bindings*, que são as estruturas de dados responsáveis pelo armazenamento dos *bindings*.

A implementação de um suporte confiável de segurança para estas mensagens é outro aspecto de vital importância, uma vez que para conferir mobilidade a nós os procedimentos devem ser tão automatizados quanto possível, visando prover agilidade nos registros do nó móvel com seus *home agents*. Toda esta automatização facilita a tarefa de especialistas em invasão de sistemas, pois um *hacker* que conseguisse escutar passivamente uma mensagem de registro (*binding update*), poderia reutilizá-la caso não houvesse uma autenticação eficiente. Transmissão de informações sigilosas, da mesma forma, ficariam sujeitas ao acesso por terceiros caso não houvesse a possibilidade de criptografá-las. Após a análise da adequabilidade dos mecanismos de segurança do IPv6 empregados em mobilidade [18], adotou-se então estes mecanismos em substituição às extensões originalmente propostas nesta arquitetura [13].

2.2 Segurança no IPv6

Todas as mensagens de *binding* devem obrigatoriamente ser autenticadas. Para este fim, será utilizado o cabeçalho de Autenticação (AH) do IPv6. Este cabeçalho provê meios para que o pacote IP possa incluir dados de autenticação da mensagem, utilizando, por exemplo, uma função de *hash* como no *MD5* [8]. A inclusão destes dados permite que o destinatário do pacote possa verificar a autenticidade do emissor do mesmo, além de proteger contra sua modificação em trânsito, uma vez que um pacote modificado será visto pelo receptor da mesma forma que um pacote forjado, ou seja, emitido por alguém que não possui a chave secreta do emissor. Este cabeçalho é ilustrado na figura 2.

0 8 16 31

Próximo Cabeçalho	Comprimento	Reservado
Índice de Parâmetros de Segurança (SPI)		
Dados de Autenticação (Número variável de palavras de 32 bites)		

Figura 2 – Cabeçalho de autenticação do IPv6.

O cálculo dos dados de autenticação é controlada por uma Associação de Segurança, que representa todo o contexto referente à metodologia de criptografia empregada entre um emissor e um receptor. Esta Associação é identificada no cabeçalho de autenticação por um SPI (*Security Parameters Index*) e um endereço de destino, e é, por definição, unidirecional.

As aplicações que necessitem do uso de sigilo em suas comunicações podem empregar o cabeçalho ESP (*Encapsulating Security Payload*), que provê o suporte necessário baseado também nas Associações de Segurança.

2.3 Mecanismos Assimétricos e sua Infra-estrutura de Suporte

A forma mais usual de implementar o compartilhamento de segredos entre nós nas propostas observadas na literatura [2, 3, 12, 23] vem sendo o estabelecimento manual das chaves para as Associações de Segurança. O motivo deste procedimento é a inexistência de uma infraestrutura padronizada de distribuição de chaves, que permita a um nó acessar informações públicas de outros nós com garantia de que elas sejam realmente confiáveis.

O IETF vem realizando trabalhos com o objetivo de implantar esta infraestrutura [16], e podem ser observados projetos, propostas e investimentos feitos por consórcios com este fim [14, 15, 16]. Estes aspectos motivaram a opção pelo suporte a mecanismos assimétricos considerado neste trabalho. Mecanismos assimétricos utilizam partes privadas e públicas entre dois nós comunicantes para o estabelecimento de uma chave secreta. Dois importantes exemplos destes mecanismos são os algoritmos Diffie-Hellman [17] e o RSA (*Rivest-Shamir-Andler*) [17].

Num ambiente com suporte a segurança global, será comum o estabelecimento de relacionamentos entre nós que não possuem segredos compartilhados, necessários para operações de autenticação e criptografia. Uma das propostas deste trabalho é direcionar a arquitetura para a utilização dos certificados especificados para serviço de diretórios X.509 [17]. A recomendação ISO/ITU-T X.509 é parte das recomendações X.500 que definem um serviço de diretório. Este serviço de diretório é, efetivamente, um servidor ou conjunto de servidores distribuídos que mantém uma base de dados de informações sobre usuários. Essas informações incluem um mapeamento a partir de um *user name* para endereços de rede, entre outros atributos. O diretório serve então como repositório para as partes públicas de algoritmos assimétricos, que estarão contidas em certificados autenticados por uma confiável autoridade de certificação. A figura 3 ilustra o formato genérico de um certificado .

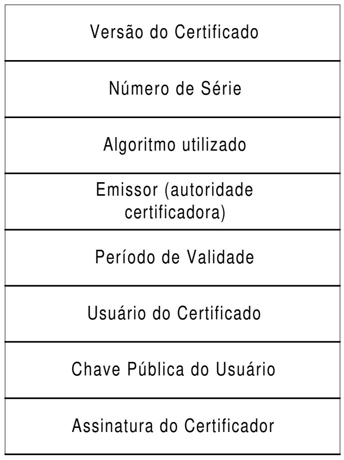

Figura 3 - Formato genérico de um certificado X-509.

A hierarquia entre as autoridades de certificação provê a escalabilidade desejada ao esquema proposto, de forma que num cenário global, com inúmeros nós móveis, seja possível acessar a chave pública de um determinado nó, disponível em um certificado autenticado. Esta chave pode ser utilizada no processo de geração de autenticadores ou na criação de chaves para criptografar mensagens. Uma mensagem criptografada com a chave pública de um determinado nó somente poderá ser decifrada através da chave secreta associada à chave pública originalmente utilizada. Para autenticações, pode-se criptografar uma chave de sessão e enviá-la ao nó correspondente. Concatenando-se esta chave com a mensagem, e em seguida aplicando-se o *Keyed-MD5* (ou similar), o autenticador obtido é enviado junto com a mensagem. Ao recebê-la, o nó correspondente realiza procedimento simétrico, certificando-se que a mensagem foi originada por um nó que possui a mesma chave de sessão.

Na figura 4 é ilustrada uma situação hipotética, onde um usuário A deseja obter o certificado de um usuário B pertencente a outro nível de certificação. Uma vez que as autoridades de certificação possuem também seus certificados, que são autenticados pela instância imediatamente superior, a verificação de autenticidade do certificado obtido é trivial. A notação X<<A>> representa que a autoridade X é responsável pela autenticação do certificado de A.

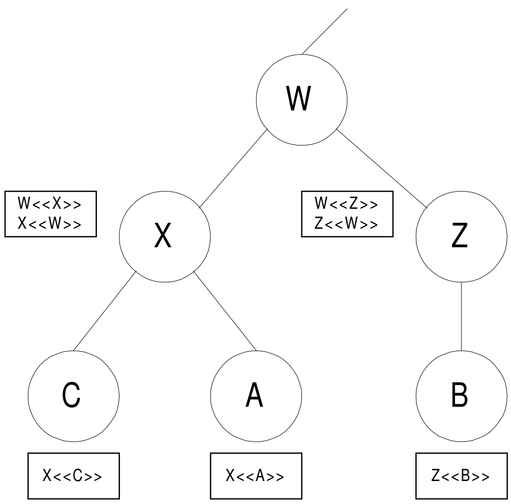

Figura 4 - Hierarquia de certificação.

Perdendo sua validade, por expiração de validade ou por comprometimento das chaves privadas, o certificado é revogado e incluído em uma lista de revogação.

3 Uma Arquitetura para Suporte a Segurança e Mobilidade sobre IPv6

A arquitetura proposta toma como base os mecanismos descritos na seção anterior, de forma que possam ser atendidas as necessidades das aplicações, utilizando protocolos já discutidos isoladamente na literatura juntamente com o IPv6 *mobility-aware*. Foi também adotado o mecanismo assimétrico para o estabelecimento de chaves de sessão. Estas chaves são usadas para autenticar ou criptografar um único pacote, e são derivadas a partir de uma chave secreta entre os nós e os números de sequência dos datagramas, procedimento adotado em função das fragilidades na segurança de um ambiente que suporte a mobilidade de nós.

Na arquitetura BBN, que representa um dos trabalhos mais completos no suporte a mobilidade e segurança, optou-se pela utilização de uma extensão ao DNSSec, com a criação de novos registros para armazenar não apenas as chaves públicas de nós, como especificado inicialmente pelo IETF, mas todo um certificado. Este procedimento tem como vantagem a ampla utilização do DNS no ambiente Internet. Além disso, as comunicações entre entidades de rede são freqüentemente estabelecidas com DNS *lookups*, e as obtenções de certificados poderiam ser facilmente feitas em *piggybacking* com estes contatos regulares. Este sistema, no entanto, possui a desvantagem de conduzir um volume maior de dados que os registros de chave pública do DNSSec. Desta maneira, a obtenção de certificados deverá, possivelmente, requerer conexões TCP no lugar das comunicações UDP entre servidores DNS.

Outro aspecto da arquitetura proposta pela BBN é a utilização dos endereços IP dos nós como identificadores dos usuários possuidores dos certificados. O motivo principal desta decisão foi a intenção de permitir a emissão de certificados para interfaces, no lugar de nós, privilegiando os casos de nós *multi-homed*, como no caso de hosts que atuam como *home agents* e também oferecem serviços de mobilidade para nós visitantes. Esta decisão possui a inconveniência de demandar reemissões de certificados, no caso da alteração de endereços IP dos possuidores de certificados.

A arquitetura BBN foi uma das referências para o desenvolvimento da arquitetura proposta neste trabalho. As principais diferenças encontradas nesta arquitetura proposta são resultantes da opção pelo IPv6, pela compatibilidade com os diretórios X.500 da ISO para obtenção de certificados e pela utilização de identificadores "amigáveis" para busca dos certificados, abordagens não utilizadas na arquitetura BBN.

3.1 A Arquitetura Proposta

Neste trabalho foi adotado o uso dos *distinguished names* [20] para identificar os usuários dos certificados, visando uma utilização mais pessoal e amigável pelas aplicações, inclusive as voltadas para finalidades comerciais. Os *distinguished names* são usados como chaves primárias para entradas no diretório OSI (X.500).

A figura 5 apresenta os módulos principais da arquitetura proposta.

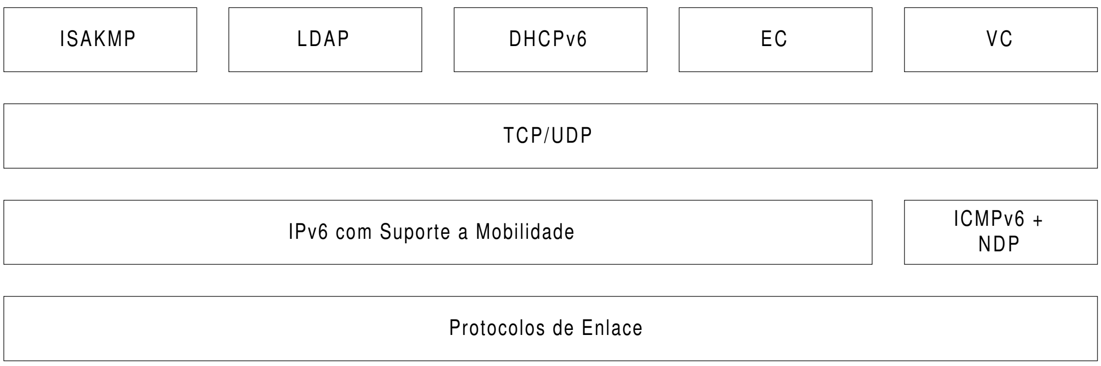

Figura 5 - Arquitetura proposta.

Esta arquitetura combina blocos funcionais, visando o emprego de módulos que realizem funções específicas. Este procedimento facilita a formalização, a implementação e posteriormente a manutenção da arquitetura, permitindo que, caso necessário, todo um módulo seja substituído desde que possua todas as interfaces necessárias. Nesta figura são apresentados os protocolos auxiliares DHCPv6 [10], LDAP [21], ISAKMP [19] , ICMPv6 [25] e NDP [11], já padronizados ou com padronização iminente, além do VC e do EC, desenvolvidos para atingir objetivos específicos da arquitetura proposta. Estes módulos são detalhados a seguir.

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

Este protocolo foi adotado pelas seguintes razões: sua especificação e desenvolvimento vêm sendo coordenados pelo IETF dentro do contexto do IPSEC *Working Group*, e, apesar do status de *draft* e de algumas questões a definir, foi considerado como trabalho mais consistente para emprego nesta arquitetura. O ISAKMP define procedimentos e formatos de pacotes para estabelecer, negociar, modificar e remover Associações de Segurança. Conforme explanado na seção anterior, as Associações de Segurança contêm todas as informações requeridas para a execução dos vários serviços de segurança em rede, como os providos pelo IPv6 (cabeçalho de autenticação e ESP), além de se auto-proteger durante a negociação inicial, através de um mecanismo de *cookies*. Outra característica importante do ISAKMP é prover independência das técnicas de geração de chaves, algoritmos de criptografia e mecanismos de autenticação, fornecendo assim a robustez necessária para suportar a evolução das técnicas de segurança empregadas [24].

As interações entre as entidades ISAKMP são feitas via UDP e, dentro do contexto da arquitetura proposta este módulo interfaceará com o módulo VC (verificador de certificados) e com o IPv6 para o gerenciamento das Associações de Segurança. Uma das formas de se estabelecer a Associação de Segurança entre dois nós é por troca "agressiva", ilustrada na tabela 1. Esta negociação possui a vantagem de utilizar um número reduzido de mensagens entre os nós, porém não provê proteção de identidade nas mensagens que trafegam no meio. Sendo necessária, a proteção pode ser provida pelo modo *Identity Protection*, ao custo de um número maior de mensagens necessárias para o estabelecimento da Associações de Segurança.

Tabela 1 - Troca agressiva no ISAKMP.

Iniciador	Respondedor	Comentários
HDR; SA; KE; NONCE; ID_{INIC}		Início do estabelecimento das SA e a troca de chaves
	HDR; SA; KE; NONCE; ID_{RESP}; AUTH	O respondedor verifica a identidade do iniciador; Chave estabelecida; SA aceita pelo respondedor
HDR *; AUTH		O iniciador verifica a identidade do respondedor; SA estabelecida.

Na tabela 1, HDR é o cabeçalho das mensagens, SA identifica as Associações de Segurança, KE é o insumo para geração de uma chave de sessão, NONCE é uma informação gerada randomicamente para proteção contra o uso de mensagens copiadas por intrusos para re-utilização posterior (ataques por *replay*) [17], ID são as identidades dos pares e AUTH os autenticadores das mensagens. HDR* significa que apenas a partir deste ponto os *payloads* das mensagens podem ser criptografados. Uma boa maneira de se usar esta troca é fazer KE como a informação pública do algoritmo Diffie-Hellman.

Uma vez que um dos objetivos da arquitetura proposta é permitir o estabelecimento de Associações de Segurança a partir de informações publicamente disponíveis e acessíveis independentemente do local de acesso à Internet, optou-se pelo uso das estruturas hierárquicas de certificação. Neste escopo encontra-se o diretório X.500 da OSI [17], onde podem ser armazenados os certificados com todas as informações necessárias. A obtenção destas informações é feita num modelo cliente-servidor, onde é necessário um *front-end* para o acesso ao diretório. As normas X.500 definem o DAP (*Directory Access Protocol*) com este fim. O DAP é direcionado para operação no modelo de referência de sete camadas da OSI, requerendo assim uma quantidade significativa de recursos computacionais. Para permitir que o cliente opere diretamente sobre TCP, provendo as funcionalidades do DAP com menor custo, foi desenvolvido na Universidade de Michigan o *LDAP (Lightweight Directory Access Protocol*), padronizado na RFC 1777 [21] e com implementação disponível pela Internet, cujo detalhamento será apresentado a seguir.

3.1.2 LDAP - *Lightweight Directory Access Protocol*

O modelo geral adotado pelo LDAP consiste em clientes executando operações do protocolo com servidores. Neste modelo, um cliente transmite um *request* descrevendo a operação a ser executada para um servidor, que então é responsável por executar as operações necessárias no diretório. Uma vez completadas estas operações, o servidor retorna uma resposta contendo os resultados desejados ou os erros ocorridos para o cliente. Caso a informação não esteja disponível no servidor acessado, um ponteiro para outro servidor pode ser recebido como resposta. A figura 6 ilustra a operação tradicional do LDAP interagindo com o serviço de diretórios X.500. Neste caso, o servidor atua em benefício do cliente para buscar uma informação. Os X.500 DSA são os *Directory System Agents* que gerenciam o serviço de diretórios.

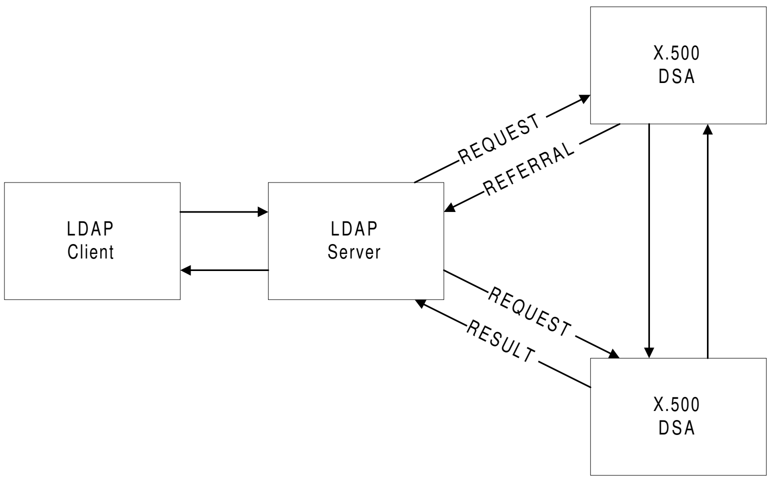

Figura 6 - Operação entre cliente e servidor LDAP.

O acesso aos atributos de uma determinada entidade pode realizado através do seu *distinguished name* , que deve referir-se a uma entrada distinta no diretório. Os *distinguished name* são representados pela forma mais comum de se identificar um usuário, através de atributos-chave, de forma que a interface é o mais amigável possível, conforme o exemplo a seguir:

CN=João da Silva, O=ACME, C=BR.

Nesta representação em forma de *string* de um *distinguished name*, *CN* representa o nome do usuário, *O* representa o nome da organização a qual o usuário está vinculado e *C* o nome do seu país. Esta forma foi adotada na arquitetura proposta por estar mais próxima do formato utilizado pelas aplicações na interface com o usuário. Além disso, os extensos endereços usados pelo IPv6 dificultam a perfeita identificação dos usuários. Neste caso, os endereços IP são meros atributos de usuários.

A troca de mensagens do protocolo LDAP para obtenção de certificados é feita via TCP, conforme ilustrado na tabela 2. No contexto da arquitetura proposta, o LDAP interfaceia com o módulo VC (verificador de Certificados).

Tabela 2 – Transações do LDAP.

Cliente	Servidor	Comentários
Bind Request		Início da sessão. O Cliente se autentica com o Servidor
	Bind Response	Resposta com o *status* da sessão solicitada
Search Request		Pedido de busca
	Search Response	Resposta do servidor
Unbind Request		Término da sessão do protocolo.

A autenticação do Cliente com o Servidor é feita através de *passwords* para obtenção de certificados, uma vez que a informação neles contida é pública. Havendo necessidade de maior segurança, o LDAP pode estabelecer autenticação forte, fazendo-o interfacear com o módulo EC (Engenho Criptográfico) para geração dos autenticadores. Tal procedimento seria necessário, por exemplo, no caso de inclusões e eliminações de entradas no diretório.

Conforme explanado na seção sobre mobilidade, o suporte a mobilidade no IPv6 prevê um mecanismo para obtenção de endereços *care-of*, usados para identificação e endereçamento temporário de um nó móvel. Para executar esta função na arquitetura proposta foi escolhido o DHCPv6 [10], devido à maior disponibilidade de endereços com o advento do IPv6 e pela grande utilização do DHCP nas redes atuais [12]. O DHCPv6 é uma versão aprimorada do DHCP, para interação com o IPv6. Este protocolo será apresentado a seguir.

3.1.3 DHCPv6 - *Dynamic Host Configuration Protocol version 6*

O protocolo DHCPv6 provê um mecanismo para passagem de informações de configuração a nós IPv6. Oferece a capacidade de alocação automática de endereços de rede "reutilizáveis", e uma flexibilidade de configuração adicional.

Da forma que foi proposto, o DHCPv6 é construído num modelo cliente-servidor, onde servidores DHCPv6 alocam endereços de rede e transmitem automaticamente parâmetros de configuração para clientes dinamicamente configuráveis, através de seu protocolo. As mensagens do DHCPv6 são as seguintes: *DHCPSolicit*, do tipo *multicast*, enviada por um cliente DHCPv6 a um ou mais Agentes DHCPv6 (servidores ou *relays*, que operam em benefício de um servidor, tal qual um *proxy*); *DHCPAdvertise*, que é uma mensagem *unicast* enviada por um Agente DHCPv6 em resposta a um *DHCPSolicit*; *DHCPRequest*, *unicast*, enviada por um cliente DHCPv6 a um servidor DHCPv6 para requerer parâmetros de configuração em uma determinada rede; *DHCPReply*, *unicast*, enviada por um servidor ou *relay* DHCPv6 em resposta a um *DHCPRequest*; *DHCPRelease*, *unicast*, enviada por um cliente DHCPv6 para informar que está liberando os recursos anteriormente concedidos, e *DHCPReconfigure*, *unicast* ou *multicast*, enviada por um servidor DHCPv6 para informar a um ou mais clientes que o servidor tem novas informações de configuração. Esta mensagem gera nova negociação através da transação *request/reply*.

Para encontrar um servidor, um cliente envia uma mensagem *DHCPSolicit* através de sua interface a configurar. O cliente então aguarda um *Advertise*, que provê o endereço IP de um servidor DHCPv6. Transações são iniciadas por um cliente através de um *DHCPRequest*, que pode ser emitido logo após o cliente obter o endereço IP do servidor. A resposta (*DHCPReply*) é enviada através de um servidor ou de seu *relay*. O protocolo prevê retransmissões de mensagens de *request* até que o *reply* correspondente seja recebido, ou até que um determinado *timeout* seja alcançado.

O DHCPv6 usa o protocolo UDP para as comunicações entre clientes e servidores, sendo então a sua confiabilidade provida pelo esquema de retransmissões descrito acima.

Visando reduzir o número de mensagens do protocolo na arquitetura proposta, o *Router Advertisement* emitido periodicamente pelos Agentes de Mobilidade já deverão conter o endereço IP do servidor DHCPv6 responsável pela cessão dos endereços *care-of*. Este procedimento possibilita a instalação do DHCPv6 em outras máquinas que não o próprio Agente de Mobilidade. Viabiliza também a emissão de um *DHCPRequest* diretamente para o Servidor DHCPv6 indicado pelo Agente de Mobilidade.

Caso se deseje, a autenticação de mensagens entre os servidores e clientes DHCPv6, no caso da mobilidade, pode ser provida pelo cabeçalho de autenticação do IPv6 (subseção 2.2).

3.1.4 EC - Engenho Criptográfico

Uma característica importante a ser observada no suporte a segurança é a manutenção das operações criptográficas, seus algoritmos e tecnologias em separado dos protocolos de suporte a comunicação principal. O motivo disso é a rápida evolução do poder computacional das máquinas que podem ser empregadas para a quebra de segredos, facilitada pela redução do custo do *hardware*. Com isso, chaves maiores precisam ser usadas, ou até mesmo a substituição de uma metodologia de criptografia e autenticação pode ser indicada. Outro fator importante é a possibilidade de se implementar todo um algoritmo em *hardware*, tornando ainda mais rápidas as operações necessárias para a implementação da segurança nos protocolos [26]. Visando o atendimento destas questões, foi idealizado para esta arquitetura um módulo específico para operações de criptografia e autenticação. Limitações de exportação determinarão, de uma maneira geral, quais algoritmos serão suportados por este módulo. Para o atendimento dos objetivos principais deste trabalho, serão inicialmente desenvolvidas as funções de *hash* necessárias nas operações de autenticação, baseadas no *Keyed-MD5* [7]. O motivo desta opção foi o fato do mesmo ter sido especificado como algoritmo *default* para as operações de autenticação para o IPv6 [6]. Na arquitetura proposta, o Engenho Criptográfico interfaceará com o IPv6. Opcionalmente, pode-se eventualmente alterar o ISAKMP e o LDAP para também tornarem-se clientes do EC. Da forma que estão especificados e disponibilizados, usam suas próprias funções criptográficas para autenticação e privacidade.

Devido a incorporação do LDAP e do ISAKMP na arquitetura proposta, foi necessária a criação de um módulo para verificação dos certificados obtidos no diretório pelo LDAP, antes de disponibilizá-lo para uso no estabelecimento das Associações de Segurança pelo ISAKMP. Desta forma, foi então criado o módulo VC (Verificador de Certificados), cujo funcionamento será descrito a seguir.

3.1.5 VC - Verificador de Certificados

Todo certificado obtido pelo LDAP deve, obrigatoriamente, possuir um campo que contenha o autenticador deste certificado. Este autenticador é produzido com base na assinatura magnética da autoridade de certificação local, cujo certificado o nó também deve possuir. Conforme ilustrado na subseção 2.3, caso o certificado obtido pertença a outro escopo de certificação, o certificado da autoridade local deverá ser obtido recursivamente, para sua perfeita verificação. Todo este gerenciamento é feito pelo VC, que interage com os módulos LDAP e ISAKMP, visando não somente a integração destes bem como a garantia que os certificados são autênticos.

3.1.6 IPv6 com Suporte a Mobilidade

Conforme análise apresentada em [18], os cabeçalhos de autenticação, privacidade, roteamento e opções de destino possuem funções que se coadunam com as necessidades do suporte a mobilidade e segurança, com poucas alterações. No caso dos *binding updates*, no lugar da criação de mensagens para envio via UDP com extensões para autenticação [13], podem ser criadas novas opções para uso com o cabeçalho de opções de destino, juntamente com o cabeçalho de autenticação. Da mesma maneira que no suporte previsto para o IPv4 [3, 9, 13,], incorpora-se aos nós a capacidade de armazenar em *cache* os *bindings*, permitindo assim o roteamento para os endereços *care-of* dos nós móveis. Os procedimentos para encapsulamento e estabelecimento de túneis são os mesmos especificados para o IPv6, independentemente do suporte a mobilidade.

Equipamentos exercendo funções de roteamento deverão ter funções específicas para provisão de mobilidade, possivelmente junto com outras funções. São os Agentes de Mobilidade, nas redes locais e em redes estrangeiras. Visando torná-los mais seguros, vem sendo proposta na literatura a instalação deste tipo de suporte nos *firewall* das redes corporativas [3, 12, 23].

O principal fator motivador do uso do IPv6 para incorporação destas características é a iminente substituição do IPv4 pelo IPv6, que torna mais provável a sua larga utilização, devido às vantagens já definidas, como o maior espaço de endereçamento e o aprimorado suporte *multicast*.

Algumas questões vêm sendo tratadas e estudadas para solução a nível de IP. O mais importante destas questões é o tratamento dos *handoffs*, ou seja, das situações em que o nó móvel muda de uma rede para outra, ou mais especificamente, quando o enlace utilizado é do tipo "sem fio" e a mudança de célula ocorre durante a existência de uma conexão entre o nó móvel e um nó correspondente. Não havendo tratamento especial para este cenário, os pacotes destinados ao nó móvel continuarão sendo enviados pelo nó móvel (ou pelo Agente Local, caso o nó correspondente não possua um *binding* para o *care-of* do nó móvel) para a rede visitada anterior à sua locomoção, provocando assim a perda da conexão. A maneira mais direta de se abordar este problema é possibilitar que o nó móvel detecte rapidamente esta mudança de localização, providenciando assim o envio de um *binding update* para o nó correspondente, Agente Local e Agente de Mobilidade Estrangeiro. Isto possibilita que a pronta mudança no roteamento dos pacotes não interfira na conexão a nível de transporte, que "desconhece" a existência da mobilidade. Para que questões como esta sejam passíveis de solução, foi incorporado o protocolo NDP (*Neighbor Discovery Protocol*) [11] juntamente com o ICMPv6 (*Internet Control Message Protocol version 6*) [25] cujas características serão apresentadas a seguir.

3.1.7 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 5. Havendo uma mensagem ICMP a transmitir, a mesma é incluída no pacote logo a seguir aos cabeçalhos 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.

3.1.8 NDP - *Neighbor Discovery Protocol*

O NDP é um protocolo que define mensagens com várias finalidades. Dentre elas, algumas são particularmente interessantes para a arquitetura proposta. 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 meio que no caso do ARP, além de tornar possível o uso dos mecanismos de segurança do IPv6. Além dessa finalidade, 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*. O NUD confere mais robustez à arquitetura no caso de falha em roteadores e locomoção de nós, pois indica com mais rapidez a falha (ou mudança de localização) em comparação ao controle pelo TCP [12], permitindo assim a interrupção do fluxo e a busca de um novo roteador.

Todos os módulos integram-se na arquitetura proposta visando o pleno atendimento não só das situações normais de comunicação entre nós através da Internet como do suporte a mobilidade e segurança. Para melhor ilustrar as situações de operação nesta arquitetura, serão demonstrados 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 entre os Módulos

A primeira etapa no processo de formalização foi a elaboração de cenários de interoperação entre os módulos. Os cenários apresentados a seguir ilustram a interação entre os módulos componentes da arquitetura nos casos do registro de um nó móvel com o seu Agente de Mobilidade na rede de origem. São representados também o emprego de uma aplicação genérica por um nó móvel e a utilização do suporte a segurança com otimizações de roteamento. Estes cenários são o primeiro passo na direção da especificação formal para simulação da arquitetura proposta.

4.1 Registro de Um Nó Móvel

A fase mais importante do suporte a mobilidade é o registro 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 *care-of*. A figura 7 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 .

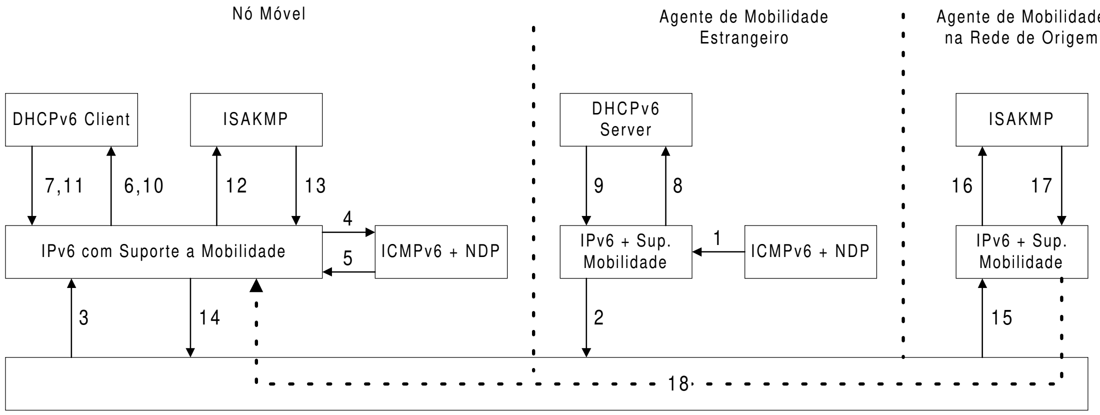

Figura 7 – Registro de um nó móvel na Arquitetura Proposta.

Ao movimentar-se para fora dos limites de sua rede local, o nó móvel perde suas conexões. Ao entrar em contato com outra rede (estrangeira), que forneça 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), o IP inicializa o cliente DHCPv6 (6), que cumprirá a rotina descrita na tabela 3.

Tabela 3 – Transações do DHCPv6.

Cliente	Servidor	Estado do Cliente
		Início - INITIALIZE
DHCPSOLICIT		SELECT
	DHCPADVERTISE	SELECT
DHCPREQUEST		REQUEST
	DHCPREPLY	BOUND
DHCPRELEASE		UNBOUND

Nesta tabela estão ilustradas as primitivas da máquina de estados do DHCPv6, com alguns detalhes omitidos, como a expiração do tempo de cessão de um determinado endereço IP para uma máquina. Na especificação original do DHCP, o protocolo cliente entra no estado de INITIALIZE assim que o Sistema Operacional da máquina é inicializado (*boot*). No caso de nós móveis, no contexto da arquitetura proposta, isso só deverá ocorrer quando o nó móvel receber um *Agent Advertisement*. Outra idéia é implementar a máquina de estados apenas para nós móveis a partir do DHCPREQUEST, uma vez que o endereço IP do Servidor DHCPv6 responsável por fornecer os endereços *care-of* pode ser informado em um *Agent Advertisement*, conforme explanado no detalhamento do DHCPv6 na seção 3.

Após a negociação com o DHCPv6 Server (7, 8, 9, 10), e a obtenção do endereço *care-of* pelo nó móvel via DHCPv6 (11), o IP inicializa o módulo ISAKMP (12) para seleção da Associação de Segurança adequada (13). Como ele deve obrigatoriamente possuir o certificado do Agente de Mobilidade em sua rede de origem, a autenticação da mensagem de registro (*binding update)*, pode ser enviada no mesmo datagrama que conduzirá a Associação de Segurança proposta (14). Ao recebê-lo (15), o Agente de Mobilidade em sua rede de origem aciona o módulo ISAKMP (16), verifica a autenticidade do *binding update,* registra a Associação de Segurança negociada, e manda a resposta (17) junto com um *binding acknowledgement* para o nó móvel (18), representado pela seta tracejada na figura 7.

4.2 Operação de uma Aplicação Genérica

Todo o suporte para mobilidade e segurança é provido pela camada Internet, fornecendo assim segurança independentemente de um suporte específico às aplicações. Na figura 8 são ilustradas as interações entre os módulos, com a finalidade de prover não só a segurança desejada para as aplicações, bem como as otimizações no roteamento entre o nó móvel e o nó correspondente, seja este móvel ou estacionário.

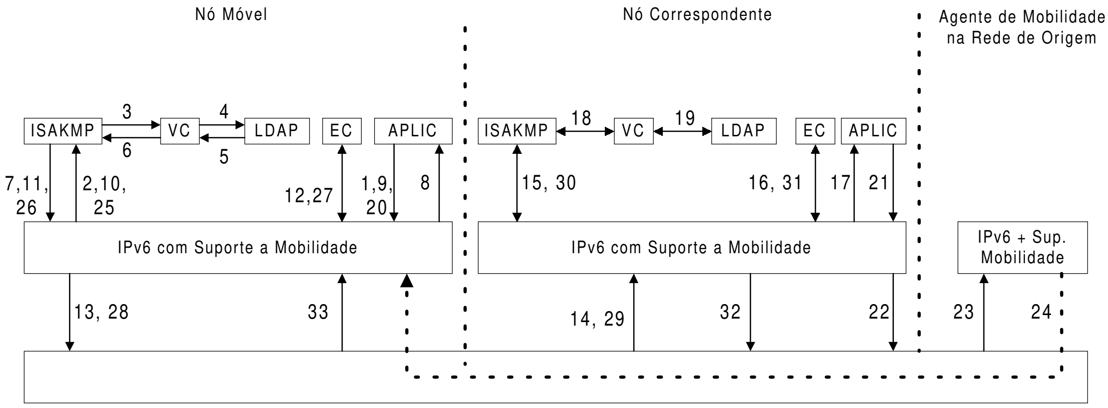

Figura 8 – Aplicação genérica operando com segurança e otimizações no roteamento.

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 pelo IPv6, serão realizadas as seguintes interações: Ao indicar esta necessidade (1), o IP do nó móvel realiza as operações para verificar junto ao ISAKMP (2) 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 (3), que por sua vez aciona o cliente LDAP (4) para obtê-lo na hierarquia de certificação através do servidor LDAP. Os passos do protocolo LDAP são os mesmos descritos na seção 3.

Neste cenário, considera-se que o nó móvel já está registrado com o seu Agente de Mobilidade na rede de origem, 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, este é verificado pelo VC (5) e entregue ao ISAKMP (6). O ISAKMP do nó móvel negocia então com o ISAKMP do nó correspondente, via UDP, uma Associação de Segurança para este relacionamento. As operações do ISAKMP são as seguintes:

- fase 1: início da negociação do ISAKMP AS (Associação de Segurança);
- fase 2: resposta da negociação do ISAKMP AS;
- fase 3: início na negociação de uma AS para um determinado DOI; e
- fase 4: resposta da negociação de uma AS para um determinado DOI.

O DOI, *domain of interpretation*, é um contexto dentro do qual são definidas características como formatos de *payloads*, conjunto de políticas de segurança e algoritmos a serem suportados, e a sintaxe para a especificação dos serviços de segurança e seus atributos, propostos em uma SA. O DOI definido para a Internet pode ser suficiente para atender os requisitos de segurança da comunidade usuária. Porém, alguns grupos específicos podem precisar adicionar um diferente conjunto de algoritmos criptográficos, definindo outros DOI. No caso do suporte a mobilidade, o DOI definido para a Internet é satisfatório, por incluir a utilização dos algoritmos assimétricos e hierarquias de certificação.

Nas fases 1 e 2, a ISAKMP AS é particular ao protocolo ISAKMP, e é baseada em *cookies* [19], evitando assim os ataques por repetição [17]. Nas fases 3 e 4 o ISAKMP acessa ao VC para a obtenção dos certificados necessários.

O IP então, ao receber a sinalização do ISAKMP que já existe uma AS para o nó móvel (7), indica para a aplicação que o relacionamento já está seguro (8). Ao receber uma mensagem da aplicação (9), o IP acessa o ISAKMP (10) para obter o Índice de Parâmetros de Segurança (SPI), definido na AS negociada (11). O IP então pode acessar o módulo responsável pelas operações de criptografia e autenticação, o Engenho Criptográfico (EC), para realizar as proteções necessárias (12). O IP monta o datagrama e o envia para o nó correspondente (13). Ao recebê-lo (14), o IP do nó correspondente verifica junto ao ISAKMP o SPI indicado (15), e ao receber sua confirmação, acessa o EC (16) para realizar as verificações de autenticidade e/ou decifragens e retornar a resposta ao IP, que entrega a mensagem à aplicação já devidamente tratada (17).

Pela especificação do IPv6 [6], 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 na direção inversa, ou seja, do nó correspondente para o nó móvel. Neste caso, não é necessária a obtenção do certificado, pois o mesmo já foi obtido no contato anterior entre as entidades (18,19).

4.3 Otimizações no Roteamento

Após o estabelecimento do relacionamento seguro entre o nó móvel com o nó correspondente, a aplicação deste último envia sua mensagem (20). 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 (21, 22 e 23). O Agente de Mobilidade captura o pacote, o encapsula, e reenvia para o nó móvel via túnel (24). O IP do nó móvel então, ao desencapsular o 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 (25,26); acesso ao EC (27) para cálculo do autenticador do *binding update* a ser enviado em um datagrama com o cabeçalho de opções de destino, além do cabeçalho de autenticação (28). Ao recebê-lo (29), o IP do nó correspondente realiza procedimento simétrico, acessando o ISAKMP (30), EC (31), e verificando a autenticidade do *binding update* recebido; registra então 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 (32,33). 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 Comentários

A arquitetura proposta tem como objetivo principal a provisão de um suporte à mobilidade e à segurança no ambiente Internet, utilizando como base o serviço IPv6. Esta arquitetura utiliza mecanismos de chaves assimétricas para autenticação e criptografia, e adota estruturas hierárquicas para a obtenção de certificados padrão OSI, de forma a conferir um alto nível de escalabilidade ao modelo. Esta escalabilidade será atingida num modelo global, com autoridades de certificação estabelecidas em vários pontos estrategicamente localizados no planeta.

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*, permitindo assim o endereçamento de um nó móvel à partir de seu endereço fixo (*home address*), e as interfaces com os módulos EC e ISAKMP. 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 (NUD)* do que os controles de fluxo intrínsecos ao TCP, uma vez que o NUD opera na camada IP, detectando mais rapidamente uma falha; o uso de um protocolo auxiliar 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* como chaves de busca para identificação de usuários, e não nos extensos endereços do IPv6, privilegia aplicações com finalidades comerciais e bancárias, com características mais pessoais, permitindo a consulta de certificados de forma mais amigável.

Esta arquitetura está sendo atualmente especificada formalmente para validação, com o uso das ferramentas adequadas.

Agradecimentos

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

Referências

[1] S. Bradner e A. Mankin. “RFC-1752 - The Recommendation for the IP Next Generation Protocol”. *Internet RFC.* janeiro de 1995.
[2] S. Cheshire e M. Baker. “Internet Mobility 4 x 4”. *SIGCOMM'96*, agosto de 1996.
[3] 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.
[4] J. R. Binkley e J. Mc. Hugh. “Secure Mobile Networking - Winter 1997”. *Technical Report*, Portland State University, abril de 1997.
[5] 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.
[6] W. Stallings. “IPv6: The New Internet Protocol”. *IEEE Comunications Magazine*, setembro de 1996.
[7] Metzer e Simpson. “RFC-1828 - IP Authentication using *Keyed* MD5”. *Internet RFC*, agosto de 1995.
[8] R. Rivest. “RFC-1321 - The MD5 Message-Digest Algoritm”. *Internet RFC*, abril de 1992.
[9] C. Perkins. “Mobile IP”. *IEEE Communications Magazine*, maio de 1997.
[10] J. Bound e C. Perkins. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”. *Internet Draft*, novembro de 1997.
[11] T. Narten , E. Nordmark e W. Simpson. “RFC-1970 - Neighbor Discovery Protocol”. *Internet RFC*, agosto de 1996.
[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] C. Perkins. “RFC-2002 - IP Mobility Support”. *Internet RFC*, setembro de 1996.
[14] 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.

[15] 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

[16] 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.

[17] W. Stallings. “Network and Internetwork Security”. *Prentice-Hall*, 1995.

[18] 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.

[19] 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.

[20] S. Kille. “RFC-1779 - A String Representation of distinguished Names”. *Internet RFC*, março de 1995.

[21] W. Yeong, T. Howes e S. Kille. “RFC-1777 – Lightweight Directory Access Protocol”. *Internet RFC*, março de 1995.

[22] C. Huitema. “Routing in the Internet”. *Prentice-Hall*, 1995.

[23] 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.

[24] R. M. Needham. “The Changing Environment for Security Protocols”. *IEEE Network*, maio/junho de 1997.

[25] A. Conta e S. Deering. “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”. *Internet RFC*, dezembro de 1995.

[26] 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.

[27] F. Teraoka, K. Uehara, H. Sunahara e J. Murai. “VIP: A Protocol Providing Host Mobility”. *Communications of the ACM*, agosto de 1994.

[28] A. Myles e D. Skellern. “Comparing four IP based mobile host protocols”. *Computer Networks and ISDN Systems*, 26 (1993) 349-355.