A Arquitetura AMoS – Uma Nova Abordagem para o Provimento de Segurança em Ambientes com Suporte à Mobilidade

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 provimento de segurança em ambientes com suporte à mobilidade sobre o protocolo IPv6, incorporando técnicas de autenticação escaláveis e um gerenciamento 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 validada, produziu uma especificação formal da arquitetura proposta, cujo desenvolvimento foi auxiliado por ferramentas disponíveis.

Abstract

This work presents an architecture for supplying the safety in atmospheres with mobility support over the IPv6 protocol, incorporating scalable authentication techniques and a transparent management for the final user. Characteristics as the scalability and the reliability of the cryptography keys and authentication are obtained by the adoption of the hierarchical structures of certification and asymmetric algorithms. The implementation strategy, addressed for the construction of a readable and validated specification, produced a formal specification of the architecture proposal, whose development was aided by available tools.

1 Introdução

Um dos maiores desafios a serem superados no fornecimento de serviços através da Internet é a fragilidade da segurança. São cada vez mais freqüentes os anúncios de invasões a sistemas, pela descoberta de falhas em sistemas operacionais e aplicativos que usuários habilidosos conseguem explorar para superar as precárias barreiras à acessos não autorizados que hoje são implementadas. Este fato compromete a credibilidade da rede junto ao público, que poderá vir a ter grandes vantagens, em termos de comodidade e rapidez, principalmente na área de comércio eletrônico, com um suporte de segurança eficaz.

Este trabalho apresenta uma arquitetura que se concentra no provimento de segurança em um ambiente onde o suporte à mobilidade é intrínseco aos seus nós. O IETF (*Internet Engineering Task Force*) vem considerando obrigatório o suporte a mobilidade em implementações do IPv6 [1], a nova versão do protocolo Internet, e várias universidades vem se empenhando em defini-lo [2, 3, 4, 5]. O grande problema observado nestes trabalhos é a ausência de propostas bem definidas para a segurança das mensagens que trafegarão pelo meio [6, 7]. Atualmente, os equipamentos portáteis (*laptops* e congêneres) possuem capacidade de armazenamento e de processamento inimagináveis em épocas passadas, e a

tecnologia de enlaces sem-fio vem apresentando resultados satisfatórios. Neste ambiente, a fragilidade é incrementada, tanto pela facilidade de se capturar as informações em trânsito como pela dificuldade em se identificar um usuário em visita à uma rede, fora do ambiente de sua rede original. Esquemas de segurança baseados nas tradicionais senhas não são aplicáveis, pois num suporte global à mobilidade, qualquer usuário poderia visitar qualquer rede, à princípio. Esta realidade obriga a busca de soluções escaláveis, onde a identificação correta de um usuário qualquer possa ser obtida de maneira segura e rápida, sem prescindir de contatos pessoais para troca de senhas.

Este projeto foi direcionado para o emprego de uma metodologia de desenvolvimento de protocolos de comunicação com validação passo-a-passo, através de ferramentas disponíveis. Como resultado obteve-se um código de especificação da arquitetura proposta em ESTELLE [8], simulada através de vários cenários possíveis, e alguns menos comuns, propostos por um gerador de seqüências de testes para protocolos de comunicação, o GASTPC [9]. A implementação da especificação poderá ser feita à partir deste código e dos vários protocolos utilizados, com códigos-fonte disponíveis, à exceção de dois protocolos, que deverão ser implementados à parte.

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 passos intermediários de validação da arquitetura através de Máquinas de Estados Finitas convertidas em Redes de Petri, na seção 5 a especificação da arquitetura em ESTELLE, com a respectiva simulação e resultados, e na seção 6 encontram-se os comentários finais.

2 Segurança e Mobilidade - Principais Conceitos

Prover segurança em um ambiente com suporte à mobilidade é um grande desafio. A maioria das propostas disponíveis na literatura propõe mecanismos *default*, sem contudo entrar mais a fundo na questão do estabelecimento prévio de segredos entre os nós que vão trocar mensagens, deixando estes aspectos para definição à parte [10, 11, 12]. Uma possibilidade do estabelecimento destes segredos é o uso de mecanismos assimétricos, onde uma informação pública referente a um nó é usada, juntamente com uma informação secreta, para a combinação de chaves de sessão, que podem ser usadas nos procedimentos de autenticação e criptografia.

A grande fragilidade existente nos ambientes com suporte à mobilidade demanda preocupações adicionais quanto à segurança. Questões peculiares ao suporte à mobilidade, bem como aspectos básicos sobre a metodologia escolhida para o suporte à segurança são descritos à seguir.

2.1 Mobilidade na Internet

As propostas mais discutidas e apontadas como virtual solução para o provimento de mobilidade [10, 11] apontam para a implementação deste suporte na camada Internet. Optou-se por direcionar o trabalho ao suporte no IPv6, substituto da versão atual do IP. 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* [10], 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 reenvio de pacotes de um endereço original para um temporário. Uma vez que não seja comprovada sua autenticidade, o *binding update* deve ser descartado.

A figura 1 ilustra uma típica situação de suporte à mobilidade.

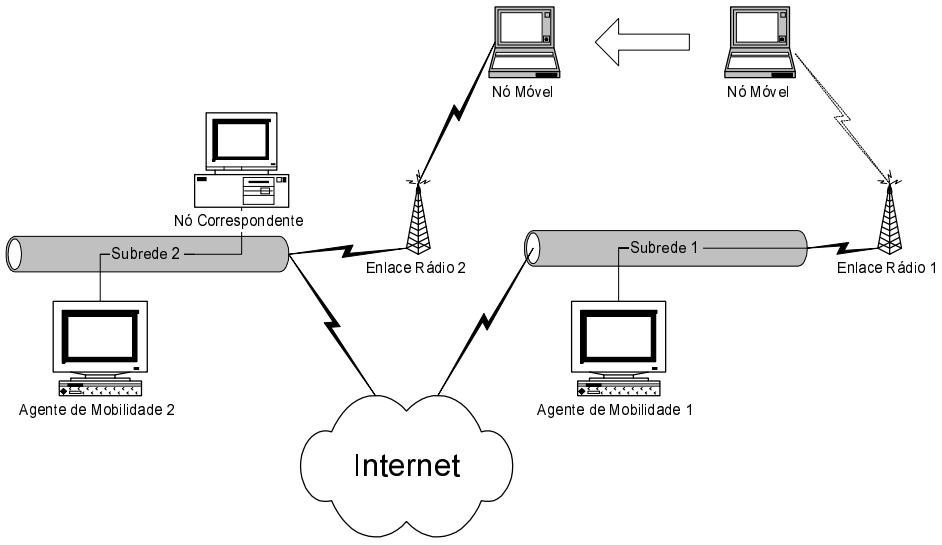

Figura 1: Movimentação de um nó entre duas sub-redes.

Nesta figura, o nó móvel, antes suportado pela sua rede de origem (sub-rede 1), movimenta-se e passa a receber mensagens *Agent Advertisement* do Agente de Mobilidade na

sub-rede 2, provenientes do seu NDP (*Neighbor Discovery Protocol*) [13]. Segundo a tática adotada neste trabalho, o nó móvel obtém um endereço na sub-rede 2 através do DHCP (*Dynamic Host Configuration Protocol*), pois uma das questões ainda pouco tratadas é a tarifação dos serviços de mobilidade prestados. Com o DHCP é possível um controle efetivo do tempo de conexão de um nó na rede visitada, em comparação ao mecanismo mais indicado na literatura, o *Stateless Autoconfiguration Protocol*. Após a obtenção deste endereço, denominado COA (*Care-of Address*) o nó móvel envia então uma mensagem de *binding update* ao Agente de Mobilidade na sub-rede 1. Todas as mensagens enviadas ao endereço fixo do nó móvel (seu *home address*) serão então redirecionadas por este Agente ao seu endereço COA. Deve-se salientar que, caso não se possua um mecanismo robusto para autenticação da mensagem *binding update*, qualquer nó poderá passar a receber mensagens destinadas ao nó móvel. Na figura 1 ilustrou-se propositadamente o seguinte cenário: O nó móvel está temporariamente sendo suportado pela mesma sub-rede que o nó correspondente. Nesta situação, ocorre o que se chama de triângulo de roteamento, pois os pacotes enviados pelo nó correspondente serão roteados para a rede de origem do nó móvel (sub-rede 1), quando são recebidos pelo Agente de Mobilidade 1, encapsulados e enviados de volta à sub-rede 2, porém com endereço de destino preenchido com o COA. Neste cenário se indica uma operação de otimização no roteamento, com o nó móvel enviando um *binding update* ao seu nó correspondente. Para a autenticação desta mensagem, não é muito razoável prescindir de um contato prévio entre os operadores dos nós, para a troca de segredos. Propõe-se então neste trabalho a utilização dos mecanismos assimétricos e as estruturas hierárquicas de certificação, cujos conceitos são explanados a seguir.

2.2 Segurança em Ambientes com Suporte à Mobilidade

A maioria dos trabalhos na área de mobilidade na camada IP disponíveis [14] não implementaram segurança, ou utilizaram *passwords* para o uso na geração de dados de autenticação. Num ambiente com suporte global à mobilidade, com milhares de nós podendo comunicar-se com milhares de outros, o número de chaves toma proporções absurdamente grandes. O armazenamento e o gerenciamento destas *passwords* em servidores nas redes se tornaria inviável em pouco tempo. Para contornar este problema, indica-se o emprego de mecanismos assimétricos. Estes mecanismos possuem a grande vantagem de garantir com razoável segurança que apenas o possuidor da chave privada correspondente a uma determinada chave pública poderá realizar operações de decifração e/ou verificação de assinaturas destinadas ao usuário possuidor desta chave. Para utilizar este mecanismo, é necessária uma estrutura hierárquica de certificação, que é um repositório onde as informações públicas são mantidas, e podem ser obtidas por qualquer usuário que as deseje. Optou-se pela utilização de certificados X.509 v.3 para o armazenamento das informações públicas, devido aos esforços do IETF e de instituições comerciais na implementação desta infra-estrutura [15, 16].

Para conduzir os dados de autenticação de mensagens, e para o envio de mensagens criptografadas adotou-se os mecanismos disponíveis no IPv6 [17], os cabeçalhos AH (*Authentication Header*) e ESP (*Encapsulating Security Payload*), ilustrados nas figuras 2 e 3.

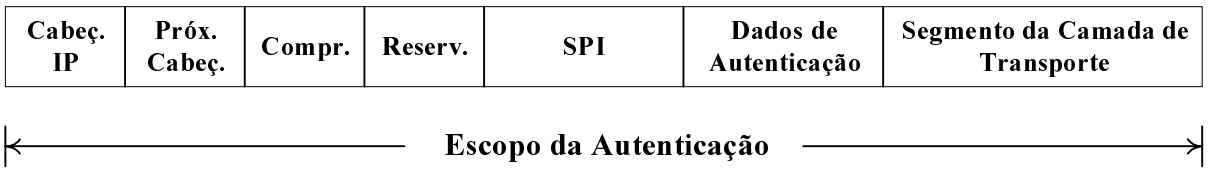

Figura 2: *Authentication Header* do IPv6.

Na figura 2 é ilustrado um campo denominado SPI (*Security Parameters Index*), que é um índice (32 bits) que identifica todo um contexto de segurança, denominado de Associação de Segurança. Contém informações como o algoritmo utilizado, a(s) chave(s) usada(s) neste algoritmo, o prazo de expiração desta(s) chave(s), etc. O campo "Dados de Autenticação" conterá tipicamente uma *string* obtida através de uma função de *hash*, como o MD-5 [18], que garanta que o pacote não foi alterado no caminho entre o origem e o destino, e que o origem é realmente que diz ser.

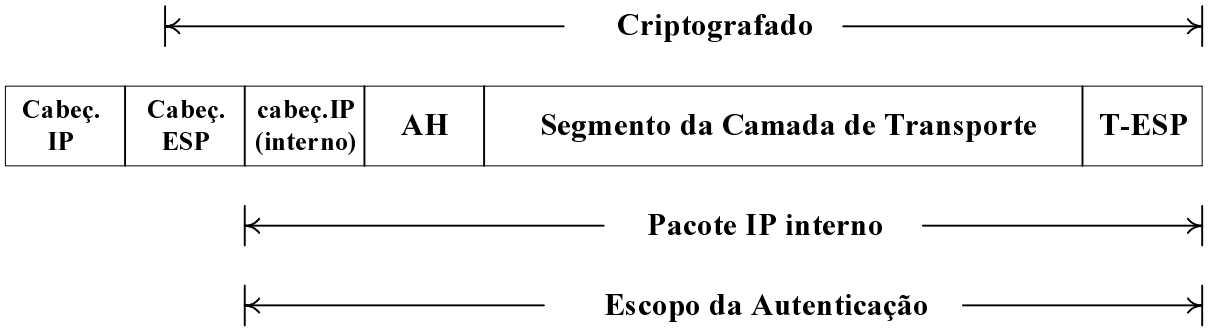

Figura 3: *Encapsulating Security Payload* do IPv6.

Na figura 3, é apresentado o cabeçalho ESP do IPv6, onde todo um datagrama pode ser criptografado e enviado a um nó que compartilhe uma Associação de Segurança com o nó de origem. Pode-se observar que a área criptografada não abrange todo o datagrama. Isto porque é necessário manter-se em forma legível o cabeçalho IP externo, para permitir o roteamento, e os campos SPI e IV (*Initialization Vector*) do cabeçalho ESP também legíveis, para permitir a decifração do restante. O IV é usado em operações de CBC (*Cipher Block Chaining*) juntamente com o algoritmo DES (*Data Encryption Standard*), mecanismo *default* para criptografia nas especificações do IPv6.

Estes conceitos foram empregados na concepção da arquitetura proposta neste trabalho. Serão descritos a seguir detalhes desta arquitetura, seus componentes e cenários visados.

3 Uma Nova Arquitetura para Provimento de Segurança em Ambientes com Suporte à Mobilidade

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 [19], LDAP [20], ISAKMP [21] , ICMPv6 [22] e NDP [13], 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.

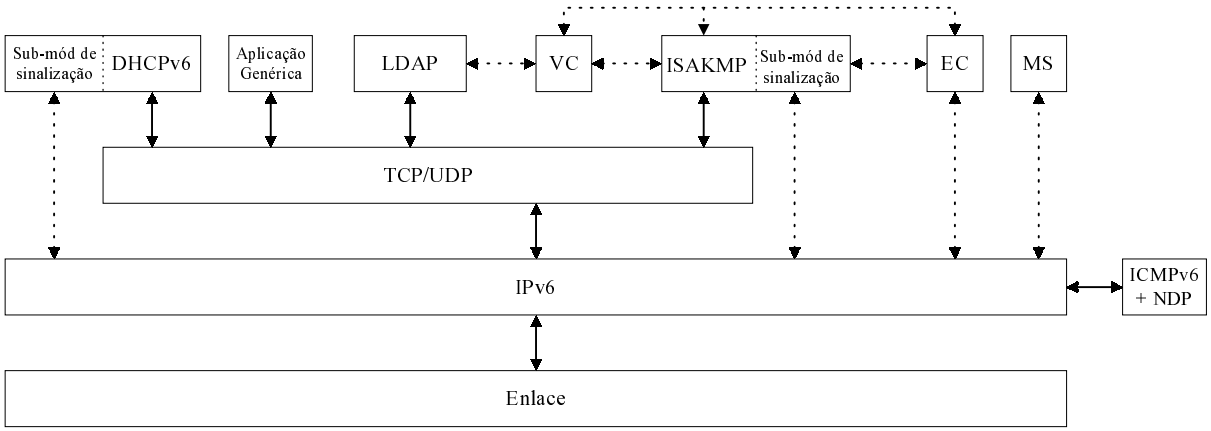

Figura 3 - A Arquitetura Proposta.

As implementações da pilha de protocolos TCP/IP não são tipicamente segmentadas em camadas [23], porém este foi um dos objetivos buscados neste trabalho. 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 Dynamic Host Configuration Protocol version 6 (DHCPv6)

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* [10], 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 para validação da arquitetura proposta implementado optou-se pela instalação dos servidores DHCP nos *Foreign Agents*, situação que tipicamente deve ocorrer num ambiente real. O *v6* representa a sua adequabilidade para operação sobre IPv6 e seus endereços de 128 octetos.

3.2 Lightweight Directory Access Protocol (LDAP)

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* [24]. Estas chaves de busca permitem uma maior legibilidade nas 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.

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

3.3 Verificador de Certificados (VC)

Os certificados obtidos pelo LDAP cliente possuem informações sobre o usuário cujo relacionamento seguro é requerido, e o Verificador de Certificados realiza a validação do mesmo. Caso os dados de autenticação contidos no certificado obtido tenham sido emitidos 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 Internet Security Association and Key Management Protocol (ISAKMP)

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 se manter um acompanhamento mais próximo dos mecanismos de criptografia e autenticação, que evoluem em função do *hardware* disponível para seu processamento [25]. 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 na próxima subseção) 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.

3.5 Engenho Criptográfico (EC)

O Engenho Criptográfico deve conter os algoritmos a serem implementados na arquitetura. A princípio, são indicados o *Keyed-MD5* para autenticação e uma interface para o IDEA (possivelmente em *hardware* [26]) 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 dados de autenticação e criptografia de datagramas para o IPv6 local.

3.6 Internet Protocol version 6 (IPv6) e o Módulo MS

Em adição às características já especificadas para o novo protocolo *Internet*, salienta-se a criação das novas opções. Destas opções, para um suporte global a mobilidade, na verdade apenas a *Home Address* é obrigatória, no caso de nós fixos. 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 o conseqüente tratamento adequado pelas aplicações. Outro aspecto importante é o da utilização dos cabeçalhos de autenticação e de encapsulamento para a provisão de segurança na arquitetura proposta.

Para permitir a concentração de funções específicas aos objetivos deste trabalho, foi idealizado o módulo MS. As funções a serem exercidas por este módulo 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 Internet Control Message Protocol version 6 (ICMPv6) e Neighbor Discovery Protocol (NDP)

O protocolo de mensagens de controle é conceitualmente posicionado na camada Internet da pilha TCP/IP, 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*). 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.

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 MAC do nó. Este procedimento é vantajoso, pois com o posicionamento da resolução de endereços na camada ICMP, a arquitetura fica mais independente do tipo de enlace que no caso do ARP, além de tornar possível o uso dos mecanismos de segurança do IPv6 nas suas mensagens. As mensagens de descoberta de roteadores (*router discovery*) também são ferramentas de grande utilidade, pois permitem 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* [10]. 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 à segurança em mobilidade. A próxima seção apresenta a modelagem da arquitetura em Máquinas de Estados Finitas e em Redes de Petri, e a sua validação intermediária com o uso de ferramentas disponíveis.

4 Validação Intermediária da Arquitetura para Segurança em Mobilidade através de Máquinas de Estados Finitas e Redes de Petri

Após a execução de um detalhado projeto conceitual do sistema a ser desenvolvido, deve-se construir um protótipo de alto nível, que permita a verificação dos critérios adotados no projeto [27]. Um protótipo originado de um bom projeto, realizado segundo estes princípios bem definidos, será facilmente expansível, resolvendo toda uma classe de problemas no lugar de resolver apenas uma situação específica. Para atingir este objetivo foram inicialmente elaborados modelos dos módulos em Máquinas de Estados Finitas (MEF), que incorporam todo o comportamento de um protocolo.

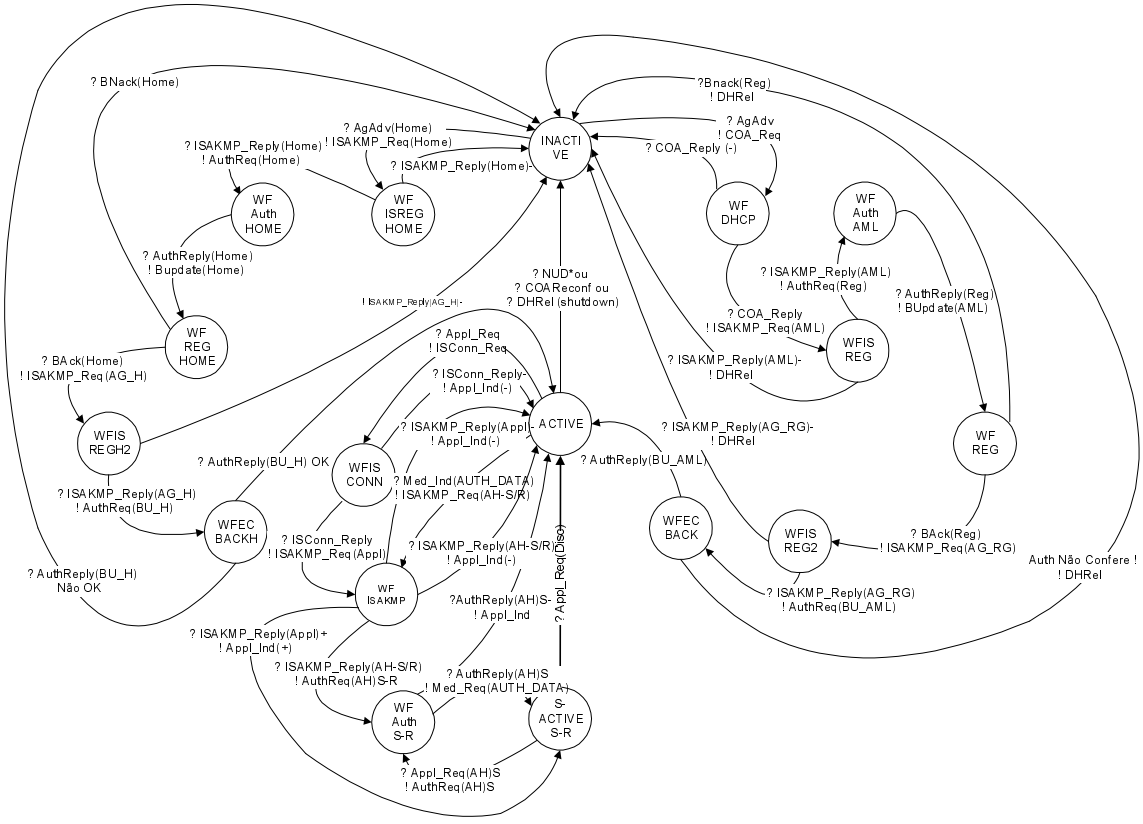

Figura 4: MEF do módulo MS de nós móveis.

A figura 4 ilustra a MEF do módulo MS de nós móveis, que incorpora as funções necessárias para a coordenação do suporte à segurança em mobilidade oferecido pela arquitetura proposta. Os rótulos das condições e ações correspondentes a uma mudança de

estado são mnemônicos dos protocolos envolvidos, precedidos por ? para uma recepção de mensagem e por ! para uma emissão. Esta figura ilustra a MEF do comportamento de iniciador e respondedor integrados numa mesma máquina. Os principais estados de um nó móvel são INACTIVE, ACTIVE e S-ACTIVE-SR. Seu estado inicial é o INACTIVE, donde após o recebimento de uma mensagem de *Agent Advertisement (AgAdv)*, já tratada pelo ICMPv6 (NDP), dois procedimentos distintos poderão ser realizados. Em caso de um Agente em sua rede de origem (*Agadv(Home)*), o MS busca uma AS junto ao ISAKMP (*ISAKMP_Req(Home)*), que após obtida, será utilizada para a geração de dados de autenticação para a mensagem de registro junto ao seu Agente. Cabe aqui ressaltar a observância na especificação do protótipo da utilização das AS unidirecionais, conforme determinado na documentação pertinente [17]. Após o seu registro com sucesso, o protocolo passa para o estado ACTIVE. Outra possibilidade é o registro em rede estrangeira, onde serão necessários alguns passos preliminares. Antes da busca da AS com o Agente na rede de origem, é necessário que se obtenha um endereço COA, solicitado ao cliente DHCP através da mensagem *COA_Req*. Obtido o endereço (*COA_Reply*) e efetuado o registro (*Binding Update*) com sucesso (*BAck(Reg)*), e sua validação, o protocolo vai para o estado de ACTIVE. À partir deste estado, uma aplicação qualquer pode solicitar uma AS com outro nó, via ISAKMP, para o envio de mensagens autenticadas ou criptografadas. A MEF da figura 4 apresenta os passos necessários para atingir este objetivo, que culminam com o estabelecimento do estado S-ACTIVE-SR, no qual existe uma AS válida entre os nós, possibilitando a obtenção de chaves de sessão para a geração de dados de autenticação e a criptografia de mensagens.

Após a obtenção das MEF de todos os módulos componentes da arquitetura, foi feita a sua conversão para Redes de Petri. O motivo desta decisão foi a grande utilidade das Redes de Petri no projeto de protocolos, pela capacidade que estas possuem de descrever sistemas concorrentes [28]. Ao contrário das máquinas de estado, em que apenas um lugar pode estar "com ficha" (com uma transição sensibilizada, habilitada para ocorrer), as Redes de Petri permitem que mais de um lugar esteja com ficha. Os lugares com fichas evoluem de forma independente e assíncrona. Com esta característica, é possível modelar duas máquinas de estado separadamente (iniciador e respondedor, cliente e servidor) e posteriormente sincronizá-las.

Para a análise das Redes de Petri originadas da modelagem dos protocolos componentes da arquitetura foi utilizado o *software* ARP (Analisador de Redes de Petri) versão 2.4 [29], desenvolvido no Laboratório de Controle e Microinformática da Universidade Federal de Santa Catarina e disponibilizado para uso acadêmico. Este *software* permite a análise das características buscadas nas redes que modelam os protocolos, entre outras facilidades.

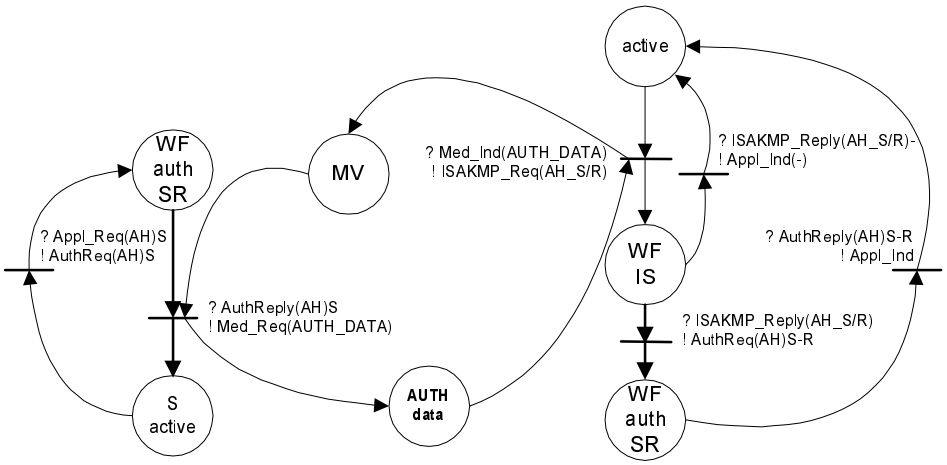

Figura 5: Detalhe da sincronização entre as Redes de Petri do iniciador e do respondedor do protocolo MS

Para ilustrar a metodologia empregada, a figura 5 apresenta um detalhe retirado do modelo usado para a validação do módulo MS de nós móveis, entre o iniciador e o respectivo respondedor. Na conversão da MEF em Rede de Petri, visando determinados cenários, é possível conferir uma característica dinâmica ao modelo. O modelo utilizado para este protocolo inclui os cenários de movimentação do nó móvel, com suporte por um Agente de mobilidade em uma rede estrangeira (visitada), seu registro com um Agente de Mobilidade na rede de origem e sua comunicação segura com outro nó qualquer, inclusive outro nó móvel. Na figura 5, pode-se observar a utilização de um lugar denominado *MV* (Meio Vazio), para evitar-se acúmulo de fichas em lugares. No disparo da transição *? AuthReply(AH)S/ ! Med_Req(AUTH_DATA)* a ficha é retirada do lugar *MV* e colocada no lugar *AUTH Data*, além do lugar *S-active*. Desta forma habilita-se o disparo da transição *?Med_Ind(AUTH_DATA)/ ! ISAKMP_Req(AH_S/R)*, pois em fases anteriores a esta detalhada, já se inseriu uma ficha no lugar *active* da rede do respondedor. Ao ser disparada esta transição pelo respondedor, simbolizando a recepção da mensagem autenticada enviada pelo iniciador, uma ficha é colocada em *MV*, habilitando mais uma vez a transição *? AuthReply(AH)S/ ! Med_Req(AUTH_DATA)*, uma vez que com o disparo da transição *?Appl_Req(AH)S/ !AuthReq(AH)S* após o envio da primeira mensagem autenticada, uma ficha é colocada no lugar *WFauth SR* do iniciador.

A submissão da Rede de Petri do módulo MS ao software ARP resultou em uma rede com 510 estados possíveis, viva, estritamente conservativa, livre de bloqueios (*deadlocks ou livelocks*), propriedades buscadas para as redes que representam protocolos de comunicação. Foram também testados invariantes de lugar e transição. Um invariante de lugar de interesse é o que apresenta os lugares *MV* e *AUTH_DATA* associados, significando que há uma relação linear entre este subconjunto de lugares, ou seja, apresenta a propriedade "conservativo para um vetor de pesos *w*", no caso específico igual a um. Em termos práticos, se demonstra a exclusão mútua entre estes lugares. Os vários invariantes de transição encontrados também espelham os vários cenários possíveis, sem ocorrência de bloqueio na rede. Cada invariante de transição representa uma seqüência cíclica. Um exemplo interessante é a seqüência de disparos que define a situação em que um nó móvel alcança uma rede estrangeira, é por ela suportado, recebendo um endereço temporário, efetua suas autenticações com sucesso para o registro com o Agente em sua rede de origem, entra no estado de ativo, se movimenta novamente e sai do alcance da rede visitada, voltando ao estado original (*INACTIVE*).

Todos os demais módulos foram validados através desta metodologia, apresentando as características buscadas durante o projeto de protocolos de comunicação. Após esta validação intermediária, partiu-se para a transformação das MEF numa especificação em ESTELLE, para obter-se a validação completa da arquitetura proposta neste trabalho através de ferramentas de simulação. A próxima seção descreve os passos relativos a esta fase.

5 Especificação em Estelle e Simulação da Arquitetura - Resultados Obtidos

Em 1989, ESTELLE foi aprovada como uma das técnicas internacionais de descrição formal (TDF) padrão para a especificação protocolos de comunicação [8]. Baseada em máquinas de estado finitas estendidas, ESTELLE possui uma semântica formal independente de implementação. É uma linguagem expressiva, bem definida e bem estruturada que é capaz de permitir a especificação de sistemas de processamento de informação concorrente de forma

consistente, concisa e bem documentada. Em uma especificação feita em ESTELLE busca-se a descoberta e a resolução de eventuais ambigüidades na especificação inicial de protocolos, feita normalmente em através de um texto informal, tabelas e gráficos sem vínculo a nenhum padrão estabelecido. Uma especificação ESTELLE representando um modelo de um protocolo de comunicação pode, através de técnicas adequadas, ser submetida à testes de conformidade, alcançando assim alto nível de cobertura de falhas.

O objetivo do protótipo desenvolvido em ESTELLE foi o de cobrir as transações entre nós móveis e agentes de mobilidade, com a finalidade de permitir as seguintes tarefas:

- obtenção de endereços temporários (COA) por nós móveis em redes estrangeiras
- registro de um nó móvel suportado por uma rede estrangeira;
- obtenção de certificados e geração de dados de autenticação para as mensagens;
- utilização de Associações de Segurança entre nós móveis; e
- envio de mensagens autenticadas entre nós móveis fora de suas respectivas redes de origem.

Para permitir a simulação das transações citadas acima, foi idealizado o protótipo ilustrado na figura 6.

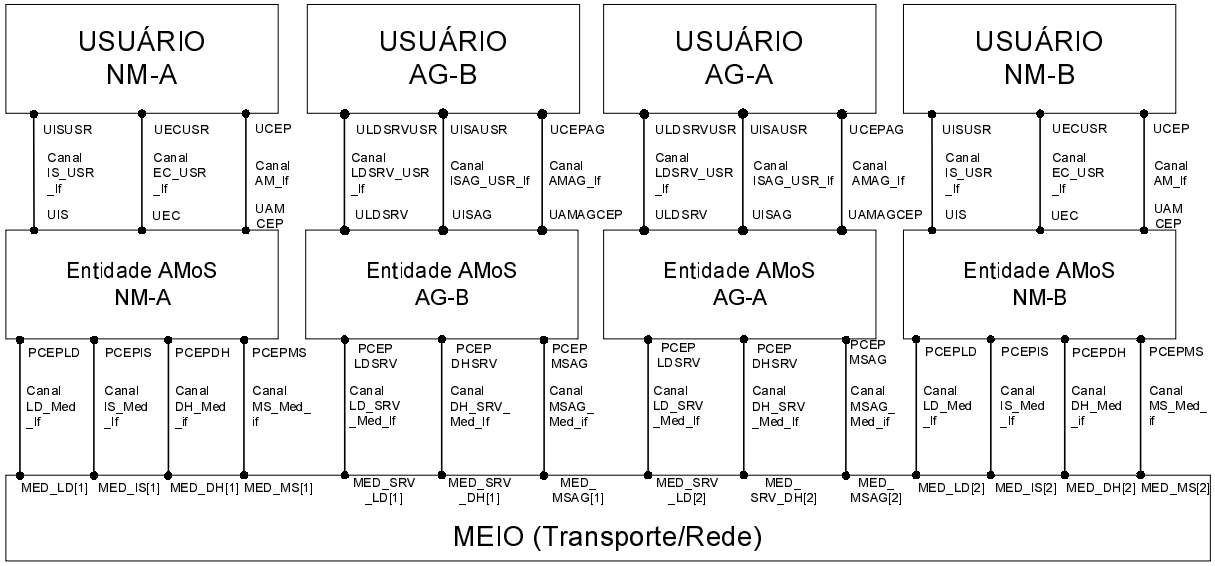

Figura 6: Protótipo desenvolvido em ESTELLE.

Na figura 6, pode ser observada a aplicação da estratégia escolhida para abordar o problema de se suportar a segurança em um ambiente com mobilidade. As funções relativas à este suporte estão compartimentadas em módulos específicos, aqui denominados AMoS NM (arquitetura para suporte a mobilidade e segurança – nós móveis) e AMoS AG (idem, agentes). Segundo a orientação do IETF [11], este suporte deve transparecer ao usuário (incluindo-se TCP/UDP) e ao enlace, onde questões de mobilidade estão sendo de forma adequada. Optou-se então por deter a atenção apenas nas questões ainda não resolvidas, com a criação destas entidades. Os módulos de usuário prestam-se apenas à simulação, sendo estes mais simples quanto possível, para permitir apenas a introdução de primitivas. As questões mais intrínsecas à camada IP (roteamento, fragmentação, etc.) não foram tratadas, pois a intenção do protótipo é mapear alterações num código já existente. Foi isolado apenas o que é introduzido pela arquitetura proposta e algumas funções de suporte à mobilidade, necessárias à cooperação entre os protocolos por ela introduzidos.

Por realizarem funções distintas, entidades do tipo nós móveis e agentes possuem algumas diferenças em suas respectivas especificações.

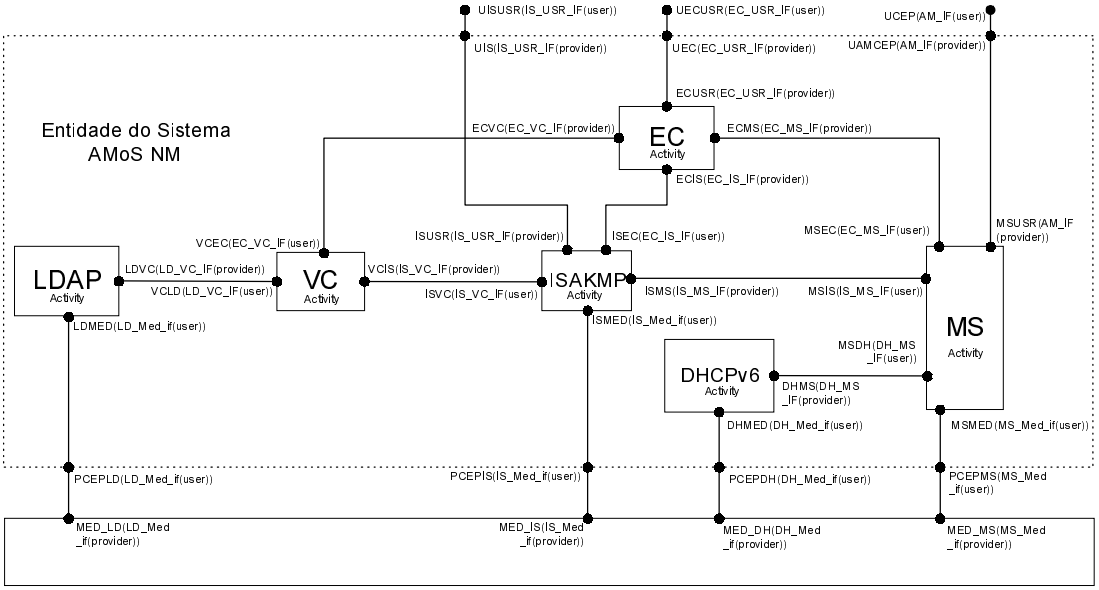

Figura 7: Arquitetura interna do módulo AMoS de nós móveis.

Na figura 7 encontram-se destacados os módulos que representam os protocolos da arquitetura típicos aos nós móveis, seus pontos de interação e canais de ligação. Em cada um dos módulos definidos, são descritos através de código ESTELLE os procedimentos definidos nas respectivas MEF. Além destes procedimentos, as interfaces são descritas detalhadamente, de forma que o produto final desta fase da metodologia de desenvolvimento de protocolos de comunicação, a especificação, é um valioso instrumento para a realização de implementações.

Para exemplificar, pode-se observar a seguir um detalhe da especificação do módulo MS, contido no módulo AMoS de nós móveis, em ESTELLE. Este detalhe captura os trechos referentes à transmissão de uma mensagem autenticada, traduzido em Rede de Petri na figura 5.

```
body AMOS_NM_body for AMOS_NM_type;
...
type

EC_MS_code_pdu_type = (AURQRG, AURQH, AURQRO, AURQSR, AURPLRG, AURPLH,
                       AURPLRO, AURPLS, AURPLSR, AURPLARO, AURQS,
                       AURQBUH, AURQBUAML, AURPLBUH, AURPLBUAML);

EC_MS_pdu_type = record
          sendercn: targetcn_type; *)
          senderpk: stringcn;
          targetcn: targetcn_type; *)
          targetpk: stringcn;
          auth    : auth_type;
          code    : EC_MS_code_pdu_type;
          sdu_conc: string;
          end;

IS_MS_code_pdu_type = (ISRQAML, ISRQH, ISRQAP, ISRQSR, ISRQRO, ISRPAPP, ISRPAPN, ISRPH, ISRPAML, ISRPHN, ISRPAMLN, ISRPSRP,
ISRPSRN, ISRPROP, ISRPRON, ISRQAGNMH, ISRQAGNMRG, ISRPLAGNMH, ISRPLAGNMRG, ISRPLAGNMHN, ISRPLAGNMRGN );

IS_MS_pdu_type = record
          sender  : target_addr_type;
          target  : target_addr_type;
          sendercn: sendercn_type;
          targetcn: targetcn_type;
          coa     : integer;
          senderpk: stringcn;
          targetpk: stringcn;
          serverId: target_addr_type;
          spi     : spi_type;
          code    : IS_MS_code_pdu_type;
          end;
```

```
...
channel IS_MS_if (user, provider);
    by user:
       IS_MS_req (IS_MS_PDU : IS_MS_PDU_type);
    by provider:
       IS_MS_ind (IS_MS_PDU : IS_MS_PDU_type);

channel EC_MS_if (user, provider);
    by user:
       EC_MS_req (EC_MS_PDU : EC_MS_PDU_type);
    by provider:
       EC_MS_ind (EC_MS_PDU : EC_MS_PDU_type);


...
module MS_type activity;
    ip
          MSUSR :   AM_if (provider);
          MSEC  :   EC_MS_if (user);
          MSIS  :   IS_MS_if (user);
          MSDH  :   DH_MS_if (user);
          MSMED :   MS_Med_if (user);
    end;
...
body MS_body for MS_type;
...
trans
         (* comportamento do iniciador *)
...
from I_WFAUTH_SR
                    when MSEC.EC_MS_ind
                              provided EC_MS_PDU.code = AURPLS
                              to I_SACT_SR
                              name msacrescauth:
                              begin
                                        WriteString ('Mensagem segue com Autentic.');
                                        WriteLn;
                                        IsAppl    := true;
                                        Isping    := false;
                                        MSAGCode  := MDRQ;
                                        auth_aux  := EC_MS_PDU.auth;
                                        BuildMSMEDpdu;
                                        output MSMED.MS_Med_req (PDUMSMED);
                              end;

...
(* comportamento de respondedor *)

          from I_ACTIVE
                    when MSMED.MS_Med_ind
                              provided MS_E_PDU.code = MDRQ
                              to I_WFIS
                              name chegoumsgauth:
                              begin
                                        WriteString ('Chegou mensagem autenticada.');
                                        WriteLn;
                                        MSEpdu_aux      := MS_E_PDU;
                                        sdu_aux         := MS_E_PDU.sdu;
                                        PDUMSIS.target  := my_addr_aux;
                                        PDUMSIS.spi     := MS_E_PDU.spi;
                                        PDUMSIS.sender  := MS_E_PDU.sender;
                                        PDUMSIS.targetcn:= MS_E_PDU.replierсn;
                                        PDUMSIS.sendercn:= MS_E_PDU.sendercn;
                                        PDUMSIS.code    := ISRQSR;
                                        output MSIS.IS_MS_req (PDUMSIS);
                              end;

...
end; (* MS_body *)
```

Neste detalhe, trechos foram suprimidos nas posições indicadas por reticências (...). Salienta-se a descrição do trecho da MEF onde o nó móvel iniciador, em estado de *WF Auth SR* (vide figuras 4 e 5) recebe do EC, através do ponto de interação *MSEC* dados de autenticação para inclusão na mensagem a ser enviada, identificado no trecho em ESTELLE por *AURPLS*. A mensagem é então enviada ao nó respondedor, que ao recebê-la, em estado de *ACTIVE*, envia uma mensagem através do ponto de interação *MSIS* ao módulo *ISAKMP*, visando obter a Associação de Segurança com o nó iniciador.

A especificação, apesar das simplificações permitidas aos vários módulos em função do alto nível pretendido, atingiu em torno de 5100 linhas.

Para validação da especificação obtida, usou-se inicialmente um compilador para a linguagem ESTELLE [30]. Através deste compilador, foram descobertos e eliminados erros através da análise léxica, sintática e de contexto do código da especificação. Ao término da

compilação, obteve-se uma forma intermediária (FI) em Módula-2. Esta FI é usada como entrada para o simulador de protocolos de comunicação utilizado [31], através do qual foram realizados testes exaustivos, incluindo situações de erro, para depurar o código obtido, tais como:

- Inserção de Associações de Segurança, certificados e chaves manualmente, para permitir a simulação no ambiente local;
- Registro dos nós móveis com seus respectivos agentes nas redes de origem;
- Inicialização de uma aplicação genérica;
- Estabelecimento de uma Associação de Segurança entre os nós móveis; e
- Envio de uma mensagem autenticada.

Muitas são as condições de erro nesta arquitetura. Vários testes foram realizados, com inexistência de chaves, dados de autenticação que não "conferem", Associações de Segurança negadas, etc. No entanto, devido ao grande número de situações que podem "mascarar" omissões de tratamento de erros na especificação, optou-se pela utilização de seqüências de testes obtidas pelo *software* GASTPC [9]. Estas seqüências representam uma técnica adequada à validação da arquitetura, por serem obtidas com um algoritmo que abrange inúmeras possibilidades, gerando um conjunto de interações com uma dada máquina de estados.

O GASTPC utiliza o algoritmo de geração correspondente ao método U, método das seqüências únicas, onde são percorridas todas as transições de estados e derivada uma marca única para cada estado (uma entrada e sua respectiva saída), denominada seqüência única de entrada e saída (seqüência UIO). A seqüência UIO para um estado corresponde a um comportamento que não é exibido por nenhum outro estado. A partir desta seqüência única, é gerada a seqüência completa que percorrerá todos os estados e transições da máquina de estados do protocolo, apresentando assim uma boa cobertura de falhas. Este método possui a vantagem de originar seqüências mais curtas do que os demais métodos existentes, para uma mesma capacidade de detecção de falhas. Uma limitação deste método é a de exigir a caracterização da MEF como uma máquina do tipo *Mealy*, onde há uma única saída possível em função do estado inicial da máquina e da entrada a ser submetida.

Para obtenção das seqüências, optou-se por usar o modelo do serviço oferecido pela arquitetura AMoS, ilustrado na figura 8.

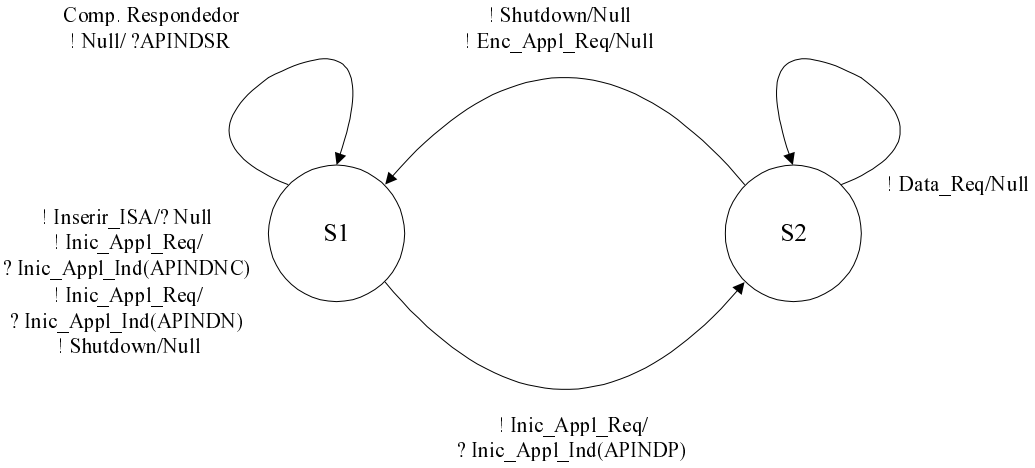

Figura 8: Modelo do serviço oferecido pela Arquitetura AMoS.

Salienta-se que, apesar do modelo da figura 8 ser aparentemente simples, a correta recepção de primitivas e mudanças de estados dependerá da perfeita interação entre todos os

componentes internos da arquitetura entre agentes de mobilidade e nós móveis, tornando este modelo o mais abrangente para o teste de conformidade.

Para diferenciar a primitiva de serviço que resultará numa tentativa frustrada de inicialização da aplicação da tentativa bem sucedida, num ambiente de mobilidade com segurança, as primitivas foram rotuladas então como *Inic_Appl_N_Req* e *Inic_Appl_Req*, respectivamente. Tal adaptação não invalida a abrangência do teste, pois assim é possível garantir a verificação de todas as possibilidades dentro do cenário para o qual a arquitetura foi projetada.

Empregou-se para as simulações a seqüência de conformidade forte, que produz não apenas um acompanhamento exaustivo da MEF, bem como introduz a ocorrência de primitivas não esperadas para um determinado estado, como no caso da subseqüência número 7, com a ocorrência de um *Data_Req* logo após um *reset* (*r/N*) na máquina, levando-a ao estado S1. Como esta primitiva só deve ocorrer após a passagem da MEF para o estado S2, o protocolo deve responder adequadamente, rejeitando a primitiva recebida e mantendo-se no estado de origem (S1). Foram obtidas e submetidas vinte subseqüências de testes, listadas a seguir.

```
***   SEQUENCIA FORTE DE TESTE GERADA PARA A MEF  ***

SUBSEQ. NUM. (1)  = r/N, insere_isa/N, insere_isa/N
SUBSEQ. NUM. (2)  = r/N, inic_appl_n_req/inic_appl_n_ind, insere_isa/N
SUBSEQ. NUM. (3)  = r/N, shutdw/N, insere_isa/N
SUBSEQ. NUM. (4)  = r/N, null/data_ind, insere_isa/N
SUBSEQ. NUM. (5)  = r/N, inic_appl_req/N, insere_isa/N
SUBSEQ. NUM. (6)  = r/N, enc_appl_req/N, insere_isa/N
SUBSEQ. NUM. (7)  = r/N, data_req/N, insere_isa/N
SUBSEQ. NUM. (8)  = r/N, inic_appl_n_req/N, insere_isa/N
SUBSEQ. NUM. (9)  = r/N, null/N, insere_isa/N
SUBSEQ. NUM. (10)  = r/N, inic_appl_req/inic_appl_ind, data_req/N, data_req/N
SUBSEQ. NUM. (11)  = r/N, inic_appl_req/inic_appl_ind, shutdw/N, insere_isa/N
SUBSEQ. NUM. (12)  = r/N, inic_appl_req/inic_appl_ind, enc_appl_req/N, insere_isa/N
SUBSEQ. NUM. (13)  = r/N, inic_appl_req/inic_appl_ind, insere_isa/N, data_req/N
SUBSEQ. NUM. (14)  = r/N, inic_appl_req/inic_appl_ind, inic_appl_req/N, data_req/N
SUBSEQ. NUM. (15)  = r/N, inic_appl_req/inic_appl_ind, shutdw/N, data_req/N
SUBSEQ. NUM. (16)  = r/N, inic_appl_req/inic_appl_ind, enc_appl_req/N, data_req/N
SUBSEQ. NUM. (17)  = r/N, inic_appl_req/inic_appl_ind, inic_appl_n_req/N, data_req/N
SUBSEQ. NUM. (18)  = r/N, inic_appl_req/inic_appl_ind, null/N, data_req/N
SUBSEQ. NUM. (19)  = r/N, r/N, insere_isa/N
SUBSEQ. NUM. (20)  = r/N, inic_appl_req/inic_appl_ind, r/N, insere_isa/N
```

6 Conclusão

Este trabalho apresentou uma proposta de arquitetura que visa o provimento do suporte à segurança e mobilidade no ambiente Internet, utilizando como base o serviço IPv6, com a implementação de um suporte à mobilidade específico para esta camada de *software* (camada Internet). 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 segurança com um alto nível de escalabilidade no modelo.

Podem ser citadas como vantagens nesta arquitetura: as únicas modificações a serem feitas no IPv6 são o reconhecimento de novas opções de destino e as interfaces com os módulos auxiliares. A capacidade de armazenar e consultar os *cache bindings*, bem como a inclusão de dados de autenticação em datagramas já está prevista no âmbito do IETF, com a utilização de cabeçalhos e opções especiais. 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, de forma que as consultas à certificados podem ser feitas mais "amigavelmente".

A confecção de um cuidadoso projeto conceitual, a partir de máquinas de estados finitas de protocolos, e em Redes de Petri, permitiu uma depuração prévia de incompatibilidades na arquitetura através de um analisador para Redes de Petri, reduzindo bastante a chance de se conduzir problemas para fases posteriores.

A estratégia de implementação, definida em função da exaustiva validação passo-a-passo dos módulos da arquitetura proposta, demonstrou resultados bastante satisfatórios. A simulação da interoperação entre os protocolos componentes, com o uso de ferramentas disponíveis, privilegiou a construção de um modelo global da arquitetura com uma especificação legível e correta em ESTELLE, capaz de ser implementada em qualquer linguagem de programação. O uso de ferramentas disponíveis, como o compilador para a linguagem ESTELLE e o simulador de protocolos, permitiu uma visão dinâmica da arquitetura proposta, através do acompanhamento da execução de cenários de funcionamento. Visando ainda reduzir ao máximo a possibilidade de erros residuais, foi utilizado ainda um gerador de seqüências de testes, que permitiu a submissão do protótipo à uma seqüência de testes para conformidade forte, quando pequenos detalhes finais foram alterados na especificação.

Num ambiente onde se suporta mobilidade de nós, muitas vezes através de enlaces "sem-fio", a segurança é fator de extrema importância. É neste contexto que este trabalho se insere, apresentando uma arquitetura escalável e bem definida para prover segurança sobre ambientes que suportam mobilidade sobre IPv6.

Referências Bibliográficas

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

[2] Cheshire, S., Baker, M.,"Internet Mobility 4 x 4". In: *Proceedings of the SIGCOMM'96*, pp. 318-329, Stanford University, CA, August 1996.

[3] Jonhson, D. B., Myles, A., Perkins, C. E., "A Mobile Host Protocol supporting Route Optimization and Autentication.", *IEEE Journal of Selected Areas in Communications*, v. 13(5), pp. 839-849, June 1995.

[4] Binkley, J. R., Mc. Hugh, J., *Secure Mobile Networking - Winter 1997*. Technical Report, Portland State University, April 1997.

[5] Souza, A. A., *Uma Extensão da Plataforma de Distribuição ANSAware para Suportar a Computação Móvel*. Dissertação de Mestrado, UFPE, Recife, PE, 1996.

[6] Oliveira, F. S. G., Pedroza, A. C. P., Duarte, O. C. M. B., "Suporte para Segurança e Mobilidade no IPv6". *In: Anais do 2º Seminário Franco-Brasileiro de Sistemas Informáticos Distribuídos*, pp. 233-244, Fortaleza, Ceará, novembro de 1997.

[7] Oliveira, F. S. G., Pedroza, A. C. P., "Uma Arquitetura para Suporte a Segurança e Mobilidade sobre IPv6". *In: Anais do XVI Simpósio Brasileiro de Redes de Computadores*, pp. 596-612, Rio de Janeiro, RJ, maio de 1998.

[8] Budkowski, S., Dembinski, P., "An Introduction to Estelle: A Specification Language for Distributed Systems", *Computer Networks and ISDN Systems*, v.14(1) pp.3-23, January 1987.

[9] Silva, G. S., Pedroza, A. C. P., "Um Sistema de Geração Automática de Sequências de Testes para Protocolos de Comunicação", *Revista Brasileira de Computação*, v.5, n.1. pp. 33-44, 1989.

[10] Perkins, C. E., Johnson, D. B., "Mobility Support in IPv6". *In: Proceedings of the Second Annual International Conference on Mobile Computing and Networking - MOBICOM 96*, pp. 27-37, November 1996.

[11] Perkins, C. E., "Mobile IP", *IEEE Communications Magazine*, pp.84-99, May 1997.

[12] Teraoka, F., Uehara, K., Sunahara, H., et al., "VIP: A Protocol Providing Host Mobility", *Communications of the ACM*, v.37(8), pp. 67-113, August 1994.
[13] Narten, T., Nordmark, E., Simpsom, W., "RFC-1970 – Neighbor Discovery for IP Version 6 (IPv6)". *Internet RFC*, August 1996.
[14] Jacobs, S., Cirincione, G., "Security of Current Mobile IP Solutions and Proposed Secure Enhanced Mobile IP (SEMIP)". *In: Proceedings of Advanced Telecommunications Information Distribution Research Program (ATIRP) Conference.* pp. 7-15, University of Maryland, January 1997.
[15] Chadwick, D. W., Young, A. J., Cicovic, N. K., "Merging and Extending the PGP and PEM Trust Models – The ICE-TEL Trust Model". *IEEE Network*, v.11(3), pp. 16-24, May/June 1997.
[16] Gehrke, M., Hetschold, T., "Management of a Public Key Certification Infraestructure - Experiences from the DeTeBerkom project BMSec". *Computer Networks and ISDN Systems*, v.28, pp. 1901-1914, November 1996.
[17] Stallings, W., "IPv6: The New Internet Protocol", *IEEE Comunications Magazine*, v. 34(7), pp. 96-108, July 1996.
[18] Metzer, P., Simpson, W., "RFC-1828 - IP Authentication using *Keyed* MD5". *Internet RFC*, August 1995.
[19] Perkins, C. E., Bound, J., "DHCP for IPv6". *In: Proceedings of the Third IEEE Symposium on Computers and Communications (ISCC'98)*, Athens, Greece, July 1998.
[20] Yeong, W., Howes, T., Kille, S., "RFC-1777 – Lightweight Directory Access Protocol". *Internet RFC*, March 1995.
[21] Maughan, D., Schertler, M., Schneider, M., et al., "Internet Security Association and Key Management Protocol", *IETF IPSEC Working draft (work in progress)*, July 1998.
[22] Conta, A., Deering, S., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification". *Internet RFC*, December 1995.
[23] Huitema, C., *Routing in the Internet*. 1st ed., Upper Saddle River, NJ, Prentice-Hall, 1995.
[24] Kille, S., "RFC-1779 - A String Representation of distinguished Names". *Internet RFC*, March 1995.
[25] Needham, R. M., "The Changing Environment for Security Protocols", *IEEE Network*, v. 11(3), pp. 12-15, May/June 1997.
[26] Salomão, S. L. C., *Uma Proposta em Hardware para o Algoritmo Criptográfico IDEA*. Tese de Mestrado – PEE/COPPE/UFRJ, Rio de Janeiro, RJ, 1997.
[27] Holzmann, G. J.,. *Design and Validation of Computer Protocols.* 1st ed., Murray Hill, NJ, Prentice-Hall, 1991.
[28] Pedroza, A. C. P., *Contribuition a la definition d'un environnement pour la conception de protocoles*. Docteur These, L'Universite Paul Sabatier, Toulouse, France, 1985.
[29] *ARP - Analisador de Redes de Petri.* Laboratório de Controle e Microinformática do Departamento de Engenharia Elétrica da Universidade Federal de Santa Catarina, 1995.
[30] Oliveira.Jr., R. C., *Um Compilador para Linguagem ESTELLE*. Tese de Mestrado, PEE/COPPE/UFRJ, Rio de Janeiro, RJ, 1991.
[31] Loureiro, F. E. R., *Um Simulador para a Linguagem ESTELLE e ESTELLE**. Tese de Mestrado, PEE/COPPE/UFRJ, Rio de janeiro, RJ, 1995.