

SiGMA: Uma entidade para localização e autenticação de dispositivos móveis entre áreas de micromobilidade

Wellington Albano¹, William de Araújo², Francisco R. Cavalcanti¹,
José Neuman de Souza² e Rossana Andrade²

¹Universidade Federal do Ceará, Pós-Graduação em Engenharia Elétrica
Campus do Pici, Bloco 716, Fortaleza, Ceará, Brasil

²Universidade Federal do Ceará, Departamento de Computação
Campus do Pici, Bloco 910, Fortaleza, Ceará, Brasil

{wellington, rod}@ufc.br, {william, neuman, rossana}@lia.ufc.br

Abstract. *Mobile IP presents difficulties such as the need for registration and authentication of the mobile device with its Home Agent every time it migrates to a new network. Proposals have been developed to minimize the number of registrations when the mobile device is within a limited area (called micromobility area) reducing the number of accesses to the Home Agent. In this paper, a network entity to locate and authenticate mobile devices between micromobility areas is proposed. Use Case Maps, Sequence Diagrams and the Network Simulator are applied to modelling and simulation of the proposal.*

Resumo. *O Mobile IP apresenta dificuldades como a necessidade de registro e de autenticação de um dispositivo móvel com o seu Home Agent cada vez que se movimenta para uma nova rede. Para resolver esse problema, algumas propostas surgiram para gerenciar o deslocamento dentro de uma área limitada (denominada de área de micromobilidade), reduzindo o número de acessos ao Home Agent. Neste artigo é proposta uma nova entidade de rede para localização e autenticação de dispositivos móveis entre áreas de micromobilidade. Use Case Maps, Diagramas de Seqüência e o Network Simulator são utilizados para a modelagem e a simulação da proposta.*

1. Introdução

Um dos motivos que dificulta a adoção das funções de mobilidade em redes tradicionais está no fato de que os protocolos de endereçamento foram projetados levando em consideração que os terminais estariam sempre fixos na sua rede de origem.

Mobile IP é uma proposta para o gerenciamento de mobilidade apresentada pela IETF [11]. Essa proposta é uma extensão do IP que permite que um terminal móvel possa ser localizado mesmo que esteja visitando uma outra rede, mantendo o seu endereço IP de origem. Há dificuldades relacionadas à utilização do *Mobile IP*, como por exemplo, o fato do móvel, sempre que quiser estar disponível para a rede, precisar fazer um registro na sua rede de origem, o que certamente consome recursos de processamento e largura de banda.

Para minimizar o problema quando o terminal móvel se desloca dentro de uma determinada área de abrangência, denominada de área de micromobilidade (e.g., um domínio administrativo), surgiram propostas tais como *Cellular IP* [6] e *HAWAII* [12]. No entanto, no deslocamento entre essas áreas, o procedimento do *Mobile IP* volta a ser

utilizado. Isso pode ser inconveniente se a rede de origem do terminal móvel estiver muito distante.

Neste artigo é apresentada uma proposta para minimizar o número de registros necessários para localizar o terminal móvel no deslocamento entre áreas de micromobilidade. Esta proposta aplica os princípios de mobilidade utilizados pelo *Cellular IP* em uma área de abrangência maior. Além disso, a proposta trata da necessidade de garantir a segurança de comunicação entre os elementos de rede envolvidos durante o registro de localização do terminal móvel ao passar de uma área de micromobilidade para outra.

Na próxima seção, conceitos de mobilidade em redes IP e o modo de operação do *Mobile IP* e do *Cellular IP* são descritos de forma sucinta. A proposta para localização de terminais móveis entre áreas de micromobilidade é detalhada na Seção 3. Os aspectos de segurança também são discutidos nessa seção utilizando diagramas de seqüência. A Seção 4 apresenta a modelagem da proposta utilizando uma técnica semi-formal denominada *Use Case Maps* e a simulação utilizando o *Network Simulator*. Finalmente, as principais contribuições deste artigo e os trabalhos futuros são resumidos na Seção 5.

2. Mobilidade em Redes IP

A mobilidade de dispositivos em redes de computadores pode ser dividida em três tipos. O primeiro tipo é conhecido como mobilidade de acesso e trata da mobilidade relacionada à rede local onde os terminais estão conectados (e.g., redes locais IP sobre IEEE 802.11b). Conforme mencionado na Seção 1, uma outra forma, a micromobilidade, acontece no deslocamento dentro de uma área limitada, por exemplo, um domínio administrativo. O deslocamento dos dispositivos entre regiões de abrangência maiores do que áreas de micromobilidade é chamado de macromobilidade.

A mobilidade de acesso está fora do escopo deste trabalho. Protocolos como o *Mobile IP* e o *Cellular IP*, detalhados a seguir, são mais adequados, respectivamente, para macromobilidade e micromobilidade.

A RFC 3344 descreve o *Mobile IP* (MIP) [11], que adiciona novos elementos de rede. Por exemplo, um roteador na rede de origem do terminal móvel, chamado de agente de origem (*Home Agent* - HA), tem como função principal manter o registro de localização do terminal móvel quando este estiver fora da sua área de origem, além de fazer a interceptação e o tunelamento dos dados que forem enviados ao terminal móvel. Na rede visitada, encontra-se o agente estrangeiro (*Foreign Agent* - FA), que tem por função atribuir um endereço de rede ao nó móvel e fazer o desencapsulamento dos dados que forem enviados pelo *Home Agent*. Os outros elementos são o próprio terminal móvel (*Mobile Host* - MH) e a máquina que está se comunicando com este terminal em um determinado momento, denominada de nó correspondente (*Correspondent Node* - CN).

O funcionamento do *Mobile IP* consiste das seguintes atividades principais: descoberta de agentes, registro e tunelamento. A descoberta de agentes inicia quando o nó móvel (MH) chega em uma rede estrangeira (ou rede visitada). O MH capta anúncios dos agentes que podem servi-lo como *Foreign Agent*. O MH pode enviar uma requisição de registro na tentativa de encontrar um agente disponível se assim for necessário. Uma vez obtido o endereço IP que será utilizado naquela rede, chamado de *Care-of Address*, o MH tenta fazer o registro com o seu HA. O registro pode ser feito

diretamente ou através do FA. Os dados para o terminal móvel são interceptados pelo HA e enviados através de um túnel mantido entre o HA e o detentor do *Care-of Address* (que pode ser o FA ou o próprio MH), sendo encapsulados, por exemplo, dentro de outro pacote IP destinado ao *Care-of Address*. Assim, eles são roteados através da rede até o final do túnel. Para o envio dos dados que partem do MH, é utilizado o roteamento clássico, através do *gateway* da rede visitada.

As dificuldades relativas à utilização do *Mobile IP*, mencionadas na Seção 1, estão relacionadas ao consumo de recursos de processamento e largura de banda devido ao fato do MH, sempre que quiser estar disponível para a rede, precisar fazer um registro na sua rede de origem.

Conforme mencionado anteriormente, o *Cellular IP* (CIP) é uma proposta para minimizar o problema de registro de localização quando o MH se desloca dentro de áreas de micromobilidade, apesar de poder ser estendido até redes metropolitanas com o mesmo princípio. Na transição entre áreas de micromobilidade, o *Mobile IP* é utilizado. Na arquitetura do *Cellular IP*, as estações-base (*Cellular IP Base Station - CIPBS*) periodicamente emitem sinais que permitem aos terminais móveis identificarem a rede mais próxima deles. Os pacotes são transmitidos para a estação-base e daí até o *gateway* comum. Cada nó (*CIP node*) mantém uma tabela de rotas e os pacotes transmitidos atualizam uma entrada da tabela da seguinte forma: ao passar por um nó, a tabela é atualizada indicando de que vizinho o pacote veio e qual a sua origem. Isso forma uma cadeia que é utilizada quando os pacotes vêm em sentido contrário (*downlink*). Os pacotes são roteados de acordo com as tabelas mantidas em cada nó até o terminal móvel.

Pacotes de controle são enviados periodicamente pelo MH para evitar que o mapeamento seja removido por expiração do tempo das entradas na tabela. Se não tiverem pacotes para transmitir, os terminais móveis enviam apenas pacotes de *route-update*, para manter as suas entradas nas tabelas.

Da mesma forma que em sistemas celulares, os terminais móveis de uma rede *Cellular IP* não estão sempre conectados à rede, diminuindo o consumo de recursos, porém precisam enviar periodicamente pacotes de *paging-update*, para que seja mantida a tabela com as informações sobre sua localização.

3. Uma Entidade para Localização e Autenticação entre Áreas de Micromobilidade

Este trabalho propõe a adição de uma entidade de rede denominada de Sistema Gerenciador de Macromobilidade e Autenticação (SiGMA) em uma rede composta de várias áreas de micromobilidade, conforme ilustra a Figura 1. A função principal do SiGMA é minimizar o número de registros necessários para localizar o MH no deslocamento entre áreas de micromobilidade, além de autenticar MHs visitantes com um reduzido número de acessos ao HA. As idéias iniciais relacionadas às dificuldades e estratégias de solução para o registro de localização e segurança em áreas de macromobilidade são introduzidas em [1] e [2].

Nas próximas subseções, o comportamento funcional desta entidade de rede em relação aos aspectos de registro de localização e autenticação é apresentado em detalhes.

3.1. Aspectos de Localização

O SiGMA mantém atualizada uma tabela com a localização de um determinado número de terminais móveis, estando ligado à rede fixa e podendo ser consultado pelos *gateways* das redes de origem (e.g., o *gateway* comum no caso de redes *Cellular IP*) e por outros sistemas semelhantes na busca da localização de um terminal que esteja em trânsito. Neste caso, o SiGMA utiliza uma parte do comportamento funcional da entidade de rede MSC (*Mobile Switching Center*) dos sistemas celulares funcionando como entidade âncora na movimentação (*roaming*) dos dispositivos [3].

Se não estiver transmitindo dados, o MH não precisa fazer registro com nenhum agente, e também não precisa estar alcançável pelo *Home Agent*. Quando dados para o nó móvel chegam ao *Home Agent*, é necessário acionar um mecanismo de *paging* para que a localização atual do MH seja conhecida. Para que permaneça conectado passivamente à rede, é necessário, no entanto, que pacotes com atualização da localização sejam periodicamente enviados.

Enquanto estiver em uma área de micromobilidade, o terminal móvel está sempre atualizando a sua localização de acordo com a tecnologia que estiver sendo empregada, como o *Cellular IP*. Ao chegar em uma nova área, logo que detectar os anúncios dos agentes presentes na nova rede, o terminal tentará se autenticar e realizar um registro através do SiGMA, como é descrito na Seção 3.2.

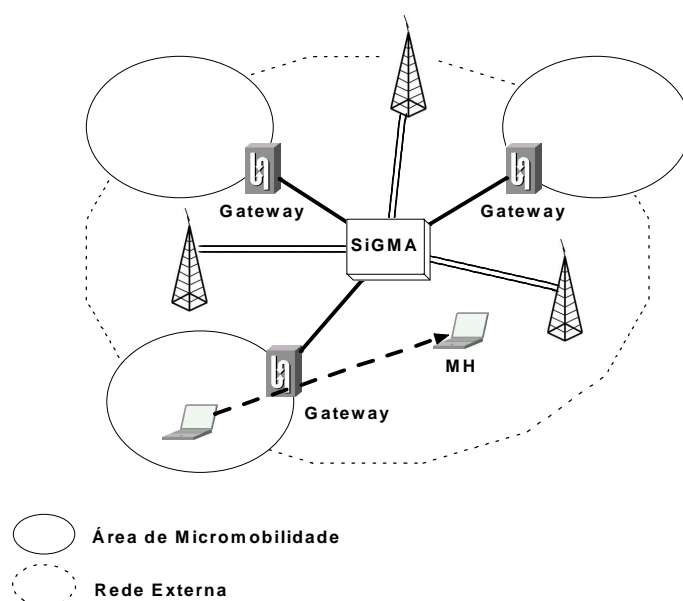


Figura 1. Localização entre Áreas de Micromobilidade

Uma vez fora da área de micromobilidade, é necessário que o MH envie pacotes de atualização de localização. Esses pacotes chegam ao SiGMA, que atualiza as tabelas. Quando o *Home Agent* precisa enviar dados ao nó móvel e não tem entrada para a nova rede do terminal em suas tabelas, ele faz uma consulta ao SiGMA, que lhe fornece a localização atual do MH. Estando o MH ainda em trânsito entre duas redes, o SiGMA pode atuar como *gateway* da área e o pedido de registro é feito. O terminal móvel registra-se com seu HA, utilizando o número IP do SiGMA como *Care-of Address*. Neste caso, o SiGMA é o final do túnel para os dados que vêm do *Home Agent*.

Quanto ao processo de mudança de estação-base ou ponto de acesso (i.e., *handoff*), ele é gerenciado pelo próprio terminal, ao notar que se aproxima de uma

estação-base ou de uma nova rede que possa lhe oferecer melhores recursos (e.g., maior largura de banda ou sinal de transmissão mais forte). O pedido é enviado diretamente do terminal ao SiGMA através da nova estação-base. O processo de autenticação e registro é, então, realizado diretamente com o SiGMA, através da nova estação-base.

3.2. Aspectos de Segurança

Nesta seção é apresentada uma solução para otimizar a autenticação [7][13][10] de MHs que se movimentam entre domínios de micromobilidade.

O conceito de domínio de segurança é introduzido neste trabalho para denominar uma área constituída por um conjunto de domínios administrativos próximos e que tenham uma relação de confiança com o SiGMA responsável por essa área. O SiGMA é o responsável pela autenticação dos MHs que estejam dentro de um domínio de segurança. Toda requisição de autenticação de MHs visitantes deve obrigatoriamente passar pelo SiGMA.

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

Após conhecer o domínio em que se encontra, o MH visitante transmite uma solicitação de autenticação ao SiGMA, através do *gateway* do domínio administrativo. Essa solicitação deve possuir um identificador do tipo de mobilidade que o MH executou, de tal forma que o SiGMA possa receber e distinguir a mobilidade realizada pelo MH: mobilidade interna ao domínio de segurança ou mobilidade entre domínios de segurança. Se o domínio administrativo em que o MH solicitou a autenticação pertencer a um domínio de segurança diferente do domínio onde o terminal estava anteriormente, a solicitação deve ser transmitida e tratada pelo seu *Home Agent*. Entretanto, se o MH entrar em um domínio administrativo que pertença a um domínio de segurança igual ao anterior, o SiGMA já deve possuir informações de autenticação.

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

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

Para que não seja possível um ataque por *replay* [7], um campo contendo o instante atual do sistema (*timestamp*) deve ser adicionado. Assim, ao receber o Autenticador, o destinatário deve comparar o *timestamp* com o tempo atual do sistema,

aceitando a mensagem caso forem aproximados e rejeitando caso contrário. Dessa forma, o Autenticador pode ser usado apenas uma vez. É necessário, então, que haja constante sincronização entre as partes comunicantes. Outra maneira de combater ataques por *replay* é através de identificadores que são valores randômicos gerados e enviados pelo emissor e que devem ser retornados pelo receptor ao emissor.

Os conceitos de *nonce*, tempestividade e criptografia de chave pública ou assimétrica são também utilizados para garantir a autenticação. *Nonce* é um valor randômico gerado pelo emissor e que deve estar contido na mensagem de resposta do receptor e é usado para proteger as partes integrantes do ataque por *replay*. Tempestividade é a característica de uma mensagem ter sido gerada recentemente e é utilizada para evitar que mensagens antigas sejam reutilizadas. A forma de verificar a tempestividade é através de *timestamps*. Os conceitos de *nonces* e *timestamps* estão presentes na especificação do MIP.

A modelagem dos aspectos de autenticação é apresentada a seguir utilizando diagramas de seqüência para representar dois cenários diferentes quando um móvel se movimenta: o primeiro retrata a mudança de domínio de segurança e, no segundo, o MH permanece no mesmo domínio de segurança.

3.2.1. Visitando um novo domínio de segurança

A Figura 2 ilustra o diagrama de seqüência do processo de autenticação de um móvel ao entrar em um domínio administrativo pertencente a um domínio de segurança diferente daquele que servia o domínio administrativo visitado anteriormente. O processo envolve o HA, visto que o SiGMA do domínio visitante inicialmente não possui informações necessárias para validar a identidade do usuário.

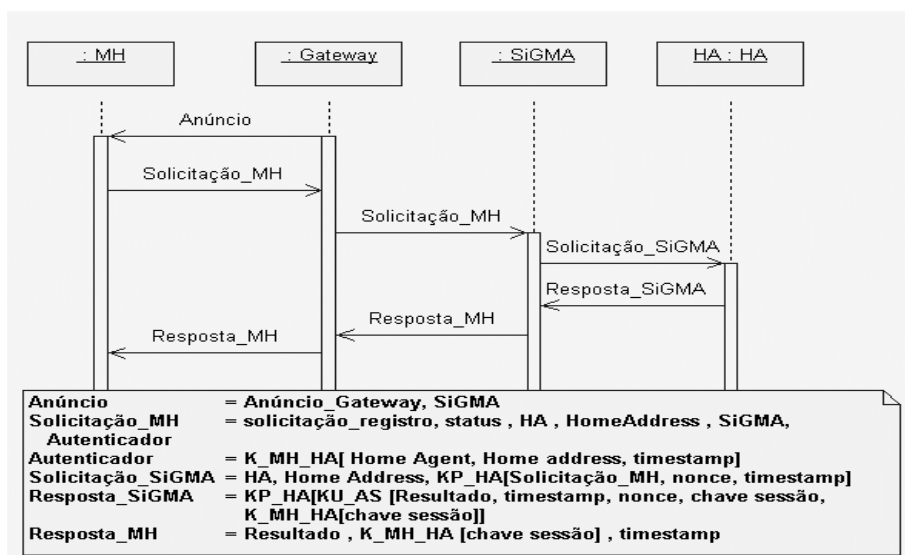


Figura 2. Solicitação de Autenticação com Acesso ao HA

Para que o MH possa detectar em qual domínio de segurança ele se encontra no momento, adicionamos o identificador do SiGMA nas mensagens de anúncio emitidas pelos gateways dos domínios administrativos (Anúncio_Gateway). Esse identificador deve ser armazenado no MH ao finalizar uma autenticação realizada com sucesso. Dessa forma, ao entrar em um novo domínio administrativo e receber os anúncios emitidos, o MH é capaz de concluir se houve uma mudança ou não de domínio de

segurança, comparando o identificador recebido e o armazenado. A estrutura da mensagem de anúncio está definida como segue:

Anúncio = Anúncio_Gateway, SiGMA

Ao entrar em um novo domínio administrativo e constatar a mudança de domínio de segurança, o MH envia ao *gateway* do domínio administrativo visitado uma mensagem de solicitação de autenticação/atualização de registro (Solicitação_MH). Caso o MH não tenha mudado de domínio de segurança, o processo de autenticação ocorrerá da forma como é abordado na próxima subseção.

A mensagem de solicitação contém um campo, denominado *status*, que indica se o MH é recém-chegado ao domínio de segurança (*status*=recente), representado na Figura 2, ou já foi autenticado anteriormente (*status*=não recente). Também contém os campos identificador do *Home Agent*, o *Home Address* do MH, o identificador do SiGMA que está sendo visitado e um autenticador para garantir ao HA a identidade do usuário. O autenticador, por sua vez, é constituído pelos campos identificador do *Home Agent*, o *Home Address* e *timestamp*, que são cifrados com a chave compartilhada entre o MH e o seu *Home Agent* (K_MH_HA). A solicitação de atualização de registro do MH é também adicionada à mensagem (solicitação_registro). A estrutura da mensagem de solicitação e do autenticador está definida como segue:

Solicitação_MH = solicitação_registro, *status*, HA, *Home Address*, SiGMA, Autenticador

Autenticador = K_MH_HA[*Home Agent* | *Home address* | *timestamp*]

O *gateway*, por sua vez, encaminha a solicitação ao SiGMA responsável pela gerência de localização. Antes de atualizar a localização de registro do MH, o SiGMA verifica se a solicitação de atualização de registro/autenticação foi realmente destinada a ele através do campo SiGMA. Após esta verificação, o SiGMA encaminha ao *Home Agent* do MH a mensagem recebida acrescida de um *nonce* e *timestamp*. Esta mensagem deve ser cifrada com a chave pública do HA (KP_HA). Além dessas informações, são acrescentados o *Home Agent* e o *Home Address* como mostramos a seguir:

Solicitação_SiGMA= HA | *Home Address* | KP_HA[Solicitação_MH | *nonce* | *timestamp*]

Em seguida, o *Home Agent* obtém as informações contidas no autenticador utilizando a chave simétrica compartilhada com o MH. Com essas informações, o HA será capaz de certificar que aquela solicitação é destinada a ele, bem como verificar a identidade do MH que está fora de sua rede. O HA verifica, também, a tempestividade da solicitação através da comparação do seu *timestamp* com os *timestamps* enviados pelos MH e o SiGMA. Esta verificação é necessária para proteger o domínio administrativo contra ataques do tipo *replay*.

Após se certificar da identidade do MH, o HA envia ao SiGMA uma mensagem de resposta à solicitação de autenticação. A mensagem de resposta contém o resultado da solicitação, o *timestamp*, o *nonce* recebido na solicitação e uma chave de sessão simétrica gerada aleatoriamente pelo HA, todos cifrados com a chave pública do SiGMA (KU_SiGMA). Contém também a mesma chave de sessão criada pelo HA cifrada com a chave compartilhada entre o HA e o MH. Para garantir a identidade do emissor, a mensagem será cifrada com a chave privada do HA (KP_HA).

A chave de sessão recebida pelo SiGMA também será recebida pelo MH, como será visto adiante nesta seção, servindo para autenticá-lo em futuras solicitações dentro do domínio de segurança. Apresentamos, a seguir, a estrutura da mensagem de resposta:

Resposta_SiGMA = KP_HA[KU_SiGMA [Resultado, *timestamp*, *nonce*, chave sessão] K_MH_HA[chave sessão]]

O SiGMA, ao receber a resposta da solicitação, verifica a assinatura da mensagem utilizando a chave pública do HA. Se a assinatura não estiver correta, a mensagem de resposta será descartada, pois não pertence ao HA original. Após a verificação da assinatura, o SiGMA decifra a mensagem com sua chave privada, recuperando o resultado da solicitação, o *timestamp*, o *nonce* e a chave de sessão. Através do resultado da solicitação, o SiGMA verifica se a autenticação do usuário ocorreu corretamente. Também é comparado o *nonce* recebido com o que foi enviado ao HA. A tempestividade da solicitação é verificada através do *timestamp*. Além disso, o SiGMA obtém a chave de sessão que será compartilhada com o MH.

Após se certificar da identidade do MH, o HA envia ao SiGMA uma mensagem de resposta à solicitação de autenticação. A mensagem de resposta contém o resultado da solicitação, o *timestamp*, o *nonce* recebido na solicitação e uma chave de sessão simétrica gerada aleatoriamente pelo HA, todos cifrados com a chave pública do SiGMA (KU_SiGMA). Contém também a mesma chave de sessão criada pelo HA cifrada com a chave compartilhada entre o HA e o MH. Essa chave de sessão recebida pelo SiGMA também será recebida pelo MH, como será visto adiante nesta seção, e servirá para autenticar o MH em futuras solicitações de registro dentro do domínio de segurança. Para garantir a identidade do emissor, a mensagem será cifrada com a chave privada do HA (KP_HA). A estrutura da mensagem é mostrada a seguir:

Resposta_MH = Resultado, K_MH_HA [chave sessão], *timestamp*

É importante perceber que toda a comunicação que utiliza criptografia de chave pública, que exige um alto poder de processamento, é realizada entre o HA e o SiGMA, ao passo que a comunicação envolvendo o MH é realizada usando chave simétrica, respeitando a baixa capacidade de processamento desse MH.

3.2.2. Autenticando em um mesmo domínio de segurança

A Figura 3 ilustra o processo de autenticação de um móvel ao entrar em um domínio administrativo que pertence ao mesmo domínio de segurança do domínio administrativo anterior.

Neste cenário, inicialmente, o MH envia uma mensagem de solicitação de autenticação/atualização de registro (Solicitação_MH) ao *gateway* do domínio administrativo visitado, informando que o pedido de autenticação deve ser tratado localmente, ou seja, realizado dentro do domínio de segurança, evitando o envio da solicitação ao HA. O campo *status* é o responsável por trazer essa informação como discutido anteriormente. Esta mensagem é idêntica à mensagem de solicitação de um MH recém-chegado, diferindo apenas na chave usada para criar o Autenticador, que é a chave obtida no primeiro pedido de autenticação (K_MH_SiGMA0). A estrutura da mensagem é apresentada a seguir:

Solicitação_MH = solicitação_registro, *status*, HA, Home Address, SiGMA, Autenticador

Autenticador = $K_{MH_SiGMA}[Home\ Agent, Home\ address, timestamp]$

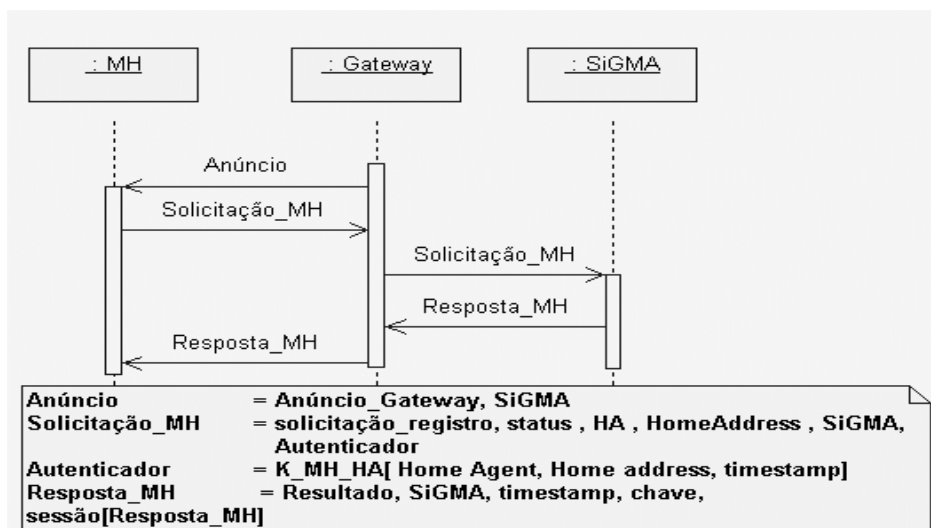


Figura 3. Solicitação de Autenticação dentro do Domínio de Segurança

O *gateway* envia a mensagem ao SiGMA, que reconhece através do *status* que se trata de uma solicitação de autenticação a ser atendida dentro do domínio de segurança. Logo em seguida, o usuário é validado através do Autenticador. Se a verificação for realizada com sucesso, o MH terá permissão para utilizar o recurso da rede, caso contrário, terá o acesso negado.

Depois de confirmar a identidade do usuário, o SiGMA realiza a atualização de registro do MH e envia ao terminal móvel (através do *gateway*) a resposta de confirmação (Resposta_MH), a identificação do SiGMA e o *timestamp*. Além disso, também é enviada a mensagem de resposta cifrada com a chave de sessão, para garantir ao terminal móvel a identidade do SiGMA. O *gateway*, por sua vez, libera ao MH os recursos disponíveis na rede.

4. Especificação e Simulação entre áreas de Micromobilidade Cellular IP

Para validar o comportamento da entidade de rede SiGMA, o protocolo *Cellular IP* é utilizado nas áreas de micromobilidade (veja Figura 4, Figura 5 e Figura 6).

Para as etapas iniciais de modelagem do protótipo para validação, utiliza-se uma técnica semi-formal baseada em cenários denominada *Use Case Maps* (UCM) [4], conforme é ilustrado na Figura 4. UCMs mostram graficamente responsabilidades e fluxos de controle entre as responsabilidades que ocorrem em diferentes cenários. Esta notação é necessária para especificar a integração de protocolos existentes (e.g., MIP e CIP) com novas propostas antes da fase de projeto e implementação. Além disso, UCMs diminuem o intervalo entre a especificação dos requisitos e a implementação no simulador e adequam-se aos propósitos do trabalho pela sua flexibilidade em mapear tanto a descrição informal utilizando texto dos aspectos de localização quanto a descrição formal aplicando diagramas de seqüência dos aspectos de segurança, apresentados na Seção 3. Com UCMs é possível ter uma visão geral do comportamento do SiGMA integrado aos protocolos CIP e MIP, além de possibilitar a detecção de omissões, ambigüidades e inconsistências nas etapas iniciais de desenvolvimento. Uma descrição detalhada da notação UCM pode ser encontrada em [4] e [3].

Na Figura 4, o início da comunicação acontece quando o Nó Correspondente (CN) precisa enviar dados ao Terminal Móvel (MH). Assim, ele envia os dados à rede de origem do MH, como supõe o roteamento tradicional. Esses dados são interceptados pelo *Home Agent* (HA). O HA consulta sua tabela de rotas para encontrar a localização do MH, que pode estar na rede local ou em uma rede estrangeira. Estando na rede local, o HA simplesmente repassa os dados adiante, que serão reconhecidos na interface de rede do terminal móvel (ainda em sua rede inicial). Se o MH estiver em uma rede estrangeira, os pacotes deverão ser enviados pela rota presente na tabela.

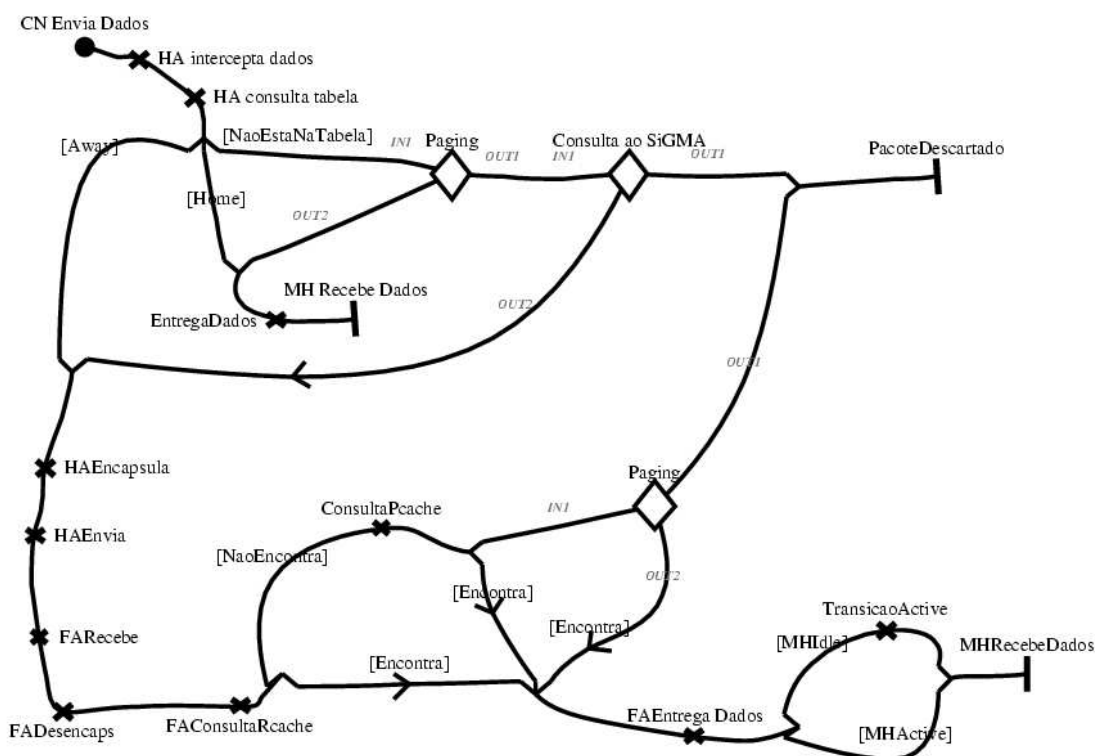


Figura 4. Modelagem com Use Case Maps

Caso não possua informação sobre o terminal, o HA realizará um *paging* na área de micromobilidade da rede de origem. Não encontrando o MH, fará uma consulta ao SiGMA. Essa consulta pode resultar na informação da rota para o MH ou no aviso de que a rota não pode ser encontrada. Neste último caso, os pacotes são descartados. No caso de haver a rota para uma rede estrangeira ou do HA obter essa rota pela consulta realizada, os dados serão encapsulados de acordo com o procedimento que estiver sendo utilizado (por exemplo, IP sobre IP) e enviados ao *Care-of-Address* (final do túnel).

Quando os dados chegarem à rede destino, serão tratados de acordo com o protocolo *Cellular IP*. Ao recebê-los e notar que estão utilizando um encapsulamento (isso é verificado nos campos do cabeçalho externo), o FA, que se trata de um *gateway* de uma rede CIP, irá desencapsulá-los, verificar o número do terminal destino e consultar a sua tabela de rotas (*Routing Cache*) para localizá-lo em sua área. Não encontrando a rota no *Routing Cache*, será consultada a tabela de *paging* (*Paging Cache*). Se ainda não for encontrada informação sobre a localização, o procedimento de *paging* do *Cellular IP* será realizado. Se ainda assim não for encontrado o terminal móvel, os pacotes serão descartados. Sendo encontrada a rota a partir do *Foreign Agent*,

nas três condições descritas acima (*Routing Cache*, *Paging Cache* ou através de *paging*), os pacotes são enviados ao destino. Ao recebê-los, se estiver no modo inativo, o MH fará a transição para o modo ativo e receberá os dados.

Para a etapa de simulação do comportamento do SiGMA, o *Network Simulator* (ns-2) [15], que é um simulador de eventos discreto, é utilizado. Um fator importante que nos levou a adotar o ns-2 como ferramenta de simulação foi a existência de simulações relacionadas com MIP e CIP [16][8] e que serviram como ponto de partida para a nossa simulação.

Para realizar a simulação do deslocamento entre redes CIP, utilizamos o pacote *Columbia IP Micro-mobility Suite* (CIMS) [6]. Neste pacote, a implementação do ns do *Cellular IP* suporta *hard* e *semi-soft handoff*, bem como *IP paging*. No entanto, a arquitetura *Cellular IP* implementada no pacote CIMS suporta apenas um único *gateway* e uma única rede CIP. Esse pacote inclui ainda a implementação do *Hawaii* e *Hierarchical Mobile IP*.

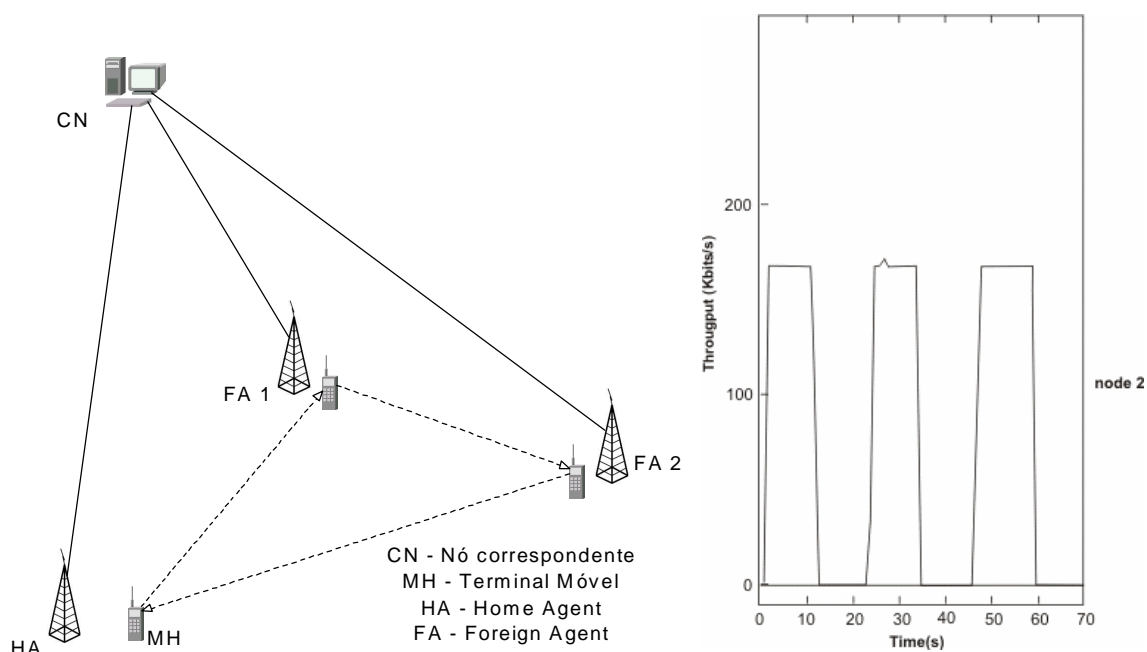


Figura 5. Simulação MIP : (a) Entidades de Rede e (b) Throughput no terminal móvel

A simulação foi realizada para observar o comportamento do terminal móvel durante a migração para uma rede externa, em que um outro agente precisaria servir de *gateway*. Para isso, utilizamos uma extensão do CIP [14], que permite múltiplos *gateways* funcionando simultaneamente em uma rede CIP. Modificações foram feitas nesta implementação do ns para adaptá-la à nossa proposta. Por exemplo, uma sinalização adicional foi criada para a que o terminal solicite o registro ao SiGMA. No entanto, a autenticação utilizando chaves não foi implementada.

Utilizamos, inicialmente, a simulação do deslocamento apenas com *Mobile IP* [16]. A Figura 5a ilustra as entidades de rede utilizadas nesta simulação. A largura de banda da rede sem fio simulada é de 2Mbps. O terminal móvel se desloca em uma área de 1000m x 1000m, passando de uma rede a outra e retornando ao ponto inicial. Ao começar a simulação, é iniciado um fluxo CBR a partir Nó Correspondente (CN) até o

terminal móvel (MH). Através dos arquivos de rastreamento (*trace files*), utilizamos um *script* em *perl* para traçar o gráfico do *throughput* dos dados relativos ao terminal móvel, que pode ser observado na Figura 5b. Observa-se que, enquanto o terminal está fora do alcance de uma nova rede, passa por períodos em que não é possível se comunicar.

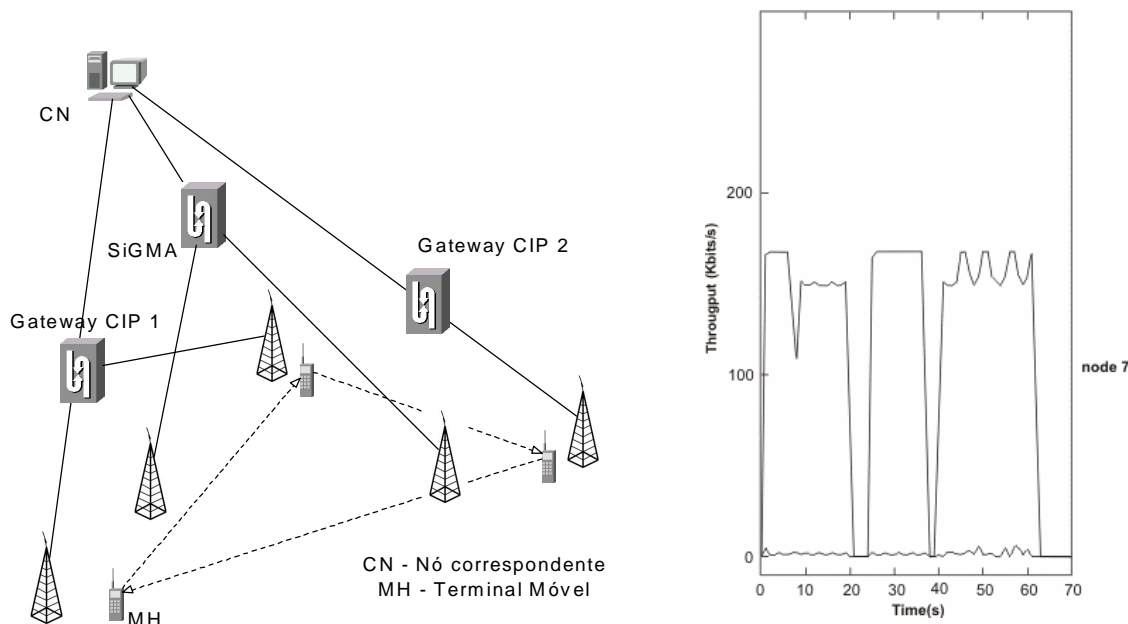


Figura 6. Simulação com CIP e SiGMA: (a) Entidades de Redes e (b) Throughput relativo ao terminal móvel

Em seguida, utilizamos a simulação do ns-2 para CIP com múltiplos *gateways*, porém adaptada à nossa proposta. O cenário e o *throughput* para a simulação podem ser vistos na Figura 6. Os parâmetros utilizados são os mesmos, à exceção da banda da região de macromobilidade, considerada como sendo igual a 150kbps. Ou seja, simulamos a região de macromobilidade com maior alcance, porém com largura de banda menor. Observa-se que, apesar de haver ainda alguma perda, devida à sinalização extra que é adicionada, a comunicação é mantida enquanto o terminal móvel passa de uma rede para outra.

Através do *throughput* observado, vemos que, devido à presença de uma outra rede para atender o MH, a perda de dados que houve durante a migração entre as regiões de micromobilidade foi menor do que no caso anterior. Ou seja, utilizando apenas MIP, na migração entre domínios administrativos diferentes, haverá perdas se esse deslocamento não for gerenciado. Segundo nossa proposta, a entidade SiGMA pertence a um domínio de localização que abrange algumas regiões de micromobilidade e é responsável também pela autenticação dos terminais que desejem ingressar em qualquer dessas regiões. Além disso, enquanto se deslocar no mesmo domínio de segurança, não será necessário efetuar novos registros com o *Home Agent*, diminuindo o número de acessos a ele.

5. Conclusões e Trabalhos Futuros

Este artigo apresenta uma proposta para a localização e autenticação de dispositivos móveis entre áreas de micromobilidade (e.g., domínios administrativos) com a adição

de uma nova entidade funcional, denominada Sistema Gerenciador de Macromobilidade e Autenticação (SiGMA). As principais funções do SiGMA são mapear a localização de um dispositivo móvel quando este não estiver em uma área de micromobilidade e realizar a autenticação de MHs visitantes.

A forma de transmissão de dados proposta é a mesma sugerida pelo *Mobile IP*, apenas supondo que as redes visitadas operam com um protocolo para micromobilidade (e.g., *Cellular IP*) e que uma rede com uma cobertura maior é utilizada para a localização dos terminais móveis no deslocamento entre as redes visitadas. Os princípios de conectividade passiva e *paging* são aplicados durante a transmissão. A autenticação de um móvel entre domínios administrativos pertencentes a um mesmo domínio de segurança é também responsabilidade do SiGMA.

A adição de *gateways* em determinados pontos da Internet responsáveis pelos aspectos de localização e autenticação entre áreas de micromobilidade traz economia de processamento e largura de banda para o sistema.

Para que se possa efetivamente desfrutar do benefício de ter uma rede gerenciando várias regiões, é necessário que a abrangência dessa rede seja suficiente para encontrar o terminal móvel em qualquer situação no deslocamento entre domínios. Assim, a rede de telefonia celular poderia, por exemplo, ser uma rede desse tipo, mantendo a entidade SiGMA em seu núcleo de rede. Um outro cenário seria o campus de uma universidade, em que os vários departamentos seriam áreas de micromobilidade e haveria um elemento de rede com alcance suficiente para atender os terminais no deslocamento entre essas áreas.

Algumas dificuldades encontradas durante o desenvolvimento deste trabalho são deixadas como desafios para trabalhos futuros. Uma delas diz respeito à escalabilidade da rede, que pode ser resolvida com o armazenamento temporário de novos dados relativos aos usuários no próprio SiGMA ou em uma nova entidade (e.g., semelhante ao *Visitor Locator Register* - VLR dos sistemas celulares).

Uma melhor distribuição de informações de autenticação entre os SiGMAs que o MH pode visitar também é tema de pesquisa futura, de tal forma a minimizar mais ainda o acesso ao HA para obter estas informações. Uma solução a ser analisada é através de predição de prováveis localizações dos móveis.

Vale ressaltar ainda a importância de realizar a validação do protocolo de autenticação utilizando técnicas formais e a necessidade de novas simulações que implementem os aspectos de segurança previstos e uma maior variedade de cenários envolvendo os MHs e o SiGMA.

6. Referências Bibliográficas

- [1] Albano, W.; Andrade, R. M. C.; Cavalcanti, F. R.; Rodrigues, E. B. *Roaming of Mobile Devices Between Cellular IP Networks* In: World Wireless Congress, 3., 2003, São Francisco, Califórnia, EUA. Anais... São Francisco, 2003.
- [2] Albano, W.; Andrade, R. M. C.; Cavalcanti, F. R.; Allen, R. *Localização e segurança de dispositivos móveis entre Redes Cellular IP*. Newsgeneration, Rio de Janeiro, v. 7, edição especial números 2 e 3, jul. 2003. Disponível em: <<http://www.rnp.br/newsgen>>.

- [3] Andrade, R. M. C., *Capture, Reuse, and Validation of Requirements and Analysis Patterns for Mobile Systems*. Ph.D Thesis. School of Information Technology Engineering. University of Ottawa. Maio, 2001.
- [4] Buhr, R. J. A., *Use Case Maps as Architectural Entities for Complex Systems*, In: IEEE Transactions on Software Engineering, Special Issue on Scenario Management, Vol. 24, No. 12, Dezembro, 1998.
- [5] Campbell, A. et al., *Design, Implementation, and Evaluation of Cellular IP*, IEEE Personal Communications, p. 42-49, Agosto, 2000.
- [6] Campbell, A. et al., *Cellular IP*, Internet draft, draf-ietf-mobileip-cellularip-00.txt, Dezembro, 1999.
- [7] Inoue, A.; Ishiyama, M.; Fukumoto, A.; Okamoto, T., *Secure mobile IP using IP security primitives*. Enabling Technologies: Infrastructure for Collaborative Enterprises, 1997, Proceedings Sixth IEEE workshops on , pp. 235 –241, Junho, 1997.
- [8] *Micromobility Software Web Site*: <http://www.comet.columbia.edu/micromobility/>. Acesso em Abril, 2002.
- [9] Panda, Manas R., *Multiple Gateway Cellular IP Network*. Disponível em <http://www.columbia.edu/itc/ee/e6951/2002spring/Projects/LOCAL/cipcvn/cip-mgw.pdf>. Acesso em Outubro, 2002.
- [10] Perkins, C., *Mobile IP and security issue: an overview*. Internet Technologies and Services, 1999. Proceedings. First IEEE/Popov Workshop on , pp.131 –148, Outubro, 1999.
- [11] Perkins, C. *IP Mobility Support for IPv4*, IETF RFC 3344, Agosto, 2002.
- [12] Ramjee, R. et al., *IP micro-mobility support using HAWAII*, Internet draft, draft-ietf-mobileip-hawaii-00.txt, Dezembro 1999.
- [13] Ringapin, A.; Ben-Othman, J.; Urien, P., *Mobility and security in IP network*. Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on, v.1, pp.280-284, 2002.
- [14] *Use Case Maps Web Site*: <http://www.UseCaseMaps.org>. Acesso em Abril, 2002.
- [15] VINT *Virtual InterNetwork Testbed Web Site*. Disponível em <http://www.isi.edu/nsnam/vint/>>. Acesso em Julho, 2003.
- [16] Widmer, J., *Network Simulations for a Mobile Network Architecture for Vehicles*. International Computer Science Institute, Califórnia, Maio, 2000.