Domínios Virtuais para Redes Móveis Ad Hoc

Leonardo A. Martucci[1], Tereza C. M. B. Carvalho[1], Wilson V. Ruggiero[1]

[1]Laboratório de Arquitetura e Redes de Computadores (LARC)
Departamento de Computação e Sistemas Digitais (PCS)
Escola Politécnica – Universidade de São Paulo (USP)
Av. Prof. Luciano Gualberto, trav.3 – 158, sala C1-46
Cidade Universitária – CEP:05508-900 – São Paulo –SP – Brasil
{lmartucc, carvalho, wilson}@larc.usp.br

Abstract. *This paper describes a security mechanism that assures privacy aspects on wireless ad hoc networks. Trusted devices initially compose these networks and information regarding to their composition or even their location, cannot be obtained from non-authorized parties. Security is achieved splitting the ad hoc network into groups of trusted devices, called virtual domains. Only devices that belong to a virtual domain can find or identify other devices from the same virtual domain. Furthermore, each virtual domain is defined by a sequence given by a time-correlated pseudo-random number generator. The security mechanism described in this paper is not exclusive to ad hoc networks and could be applied on several other network environments.*

Resumo. *Este artigo descreve um mecanismo de segurança que garante a privacidade em uma rede móvel sem fio ad hoc. Dispositivos confiáveis compõem estas redes. As informações relativas à sua composição, ou mesmo sua localização são protegidas pelo mecanismo contra o acesso por partes não autorizadas. A segurança da rede é obtida separando estes dispositivos em domínios virtuais, sendo que um dispositivo pode apenas identificar outros que pertençam ao mesmo domínio virtual reconhecido. Um domínio virtual é definido através de uma seqüência pseudo-randômica associada ao tempo corrente. A aplicação do mecanismo proposto não está restrita apenas às redes móveis ad hoc, podendo ser aplicada em diversos contextos ambientais.*

1. Introdução

Redes móveis sem-fio ad hoc são compostas por dispositivos, ou nós, que podem se movimentar livremente pelo meio, em qualquer direção e a qualquer instante. Além disso, os enlaces de comunicação são estabelecidos automaticamente enquanto os dispositivos se movimentam, construindo uma rede efêmera sem que exista suporte ou intermediação de uma entidade central, como um ponto de acesso, por exemplo.

Esta tecnologia de redes de computadores torna possível a existência de ambientes de computação ubíqua, já que os enlaces de comunicação passam a existir naturalmente, sem que exista qualquer espécie de interferência humana ou de um dispositivo central.

As redes móveis sem-fio ad hoc, denominadas de redes ad hoc neste artigo por motivos de simplificação, trazem um novo paradigma para as redes de computadores e, também, desafios completamente novos e sem paralelo com as tradicionais soluções das redes de computadores estruturadas. Protocolos de roteamento para as redes ad hoc são estudados desde 1997 e ainda hoje permanecem sendo avaliados, sem que um padrão possa ser definido, principalmente devido à existência de diferentes contextos ambientais a serem discutidos [Corson e Macker 1999]. A segurança em ambientes móveis ad hoc começou a receber uma maior atenção da comunidade científica recentemente e, assim como os aspectos relativos ao roteamento nestas redes, esta questão pode ser abordada sob a luz de diferentes pontos de vista, de modo que possam ser alcançadas diferentes propostas de soluções, dependendo do enfoque utilizado.

Deste modo, este artigo apresenta uma visão para o problema da segurança das redes de computadores e oferece uma solução que seja capaz de lidar com as propriedades de uma rede ad hoc sem tolher suas características. A solução proposta neste artigo assume que seja possível definir inicialmente quais dispositivos são confiáveis em uma rede ad hoc através de alguma característica comum, como pertencerem a um mesmo usuário ou a uma empresa. Estes dispositivos, uma vez separados nestes grupos, os quais são denominados de domínios virtuais, passam a ser capazes de reconhecer seus pares e estabelecer um canal seguro de comunicação.

A especificação do mecanismo de domínios virtuais para redes ad hoc e dos principais componentes de sua arquitetura, assim como a verificação da viabilidade de sua utilização, são os principais objetivos deste artigo. O artigo ainda compara o mecanismo de segurança proposto com outras soluções para o problema da segurança em redes ad hoc.

Este artigo está organizado em cinco seções. Esta seção continua com a apresentação dos objetivos a serem cumpridos pelo mecanismo proposto e dos desafios para o desenvolvimento e implementação do mesmo. Tais desafios decorrem dos novos paradigmas criados pelas redes ad hoc. A próxima seção apresenta os conceitos principais e o funcionamento do mecanismo de domínios virtuais. A arquitetura do mecanismo proposto e seus principais blocos funcionais são identificados e descritos na terceira seção. Aspectos da implementação são discutidos na quarta seção. Trabalhos relacionados e as conclusões finais sobre o mecanismo de domínios virtuais são apresentados nas duas últimas seções deste artigo.

1.1. Objetivos do Mecanismo de Domínios Virtuais

O objetivo do mecanismo de domínios virtuais é criar condições para garantir que as informações relativas a um grupo de dispositivos confiáveis, como os serviços presentes ou sua localização, não possam ser obtidas por uma terceira parte. De modo a esclarecer o posicionamento do mecanismo proposto faz-se necessária a apresentação de uma classificação dos diversos aspectos relativos à segurança em redes ad hoc.

Os aspectos de segurança em redes ad hoc podem ser classificados de acordo com a taxonomia proposta por [Zhou e Hass 1999]. Esta taxonomia define como atributos de segurança para redes ad hoc os seguintes aspectos: não-repúdio, disponibilidade, autenticação, integridade, confiabilidade e controle de acesso. No

entanto, sabe-se que não existe um único mecanismo de segurança que possa fornecer todos estes atributos [Stallings 1998].

O mecanismo de domínios virtuais segue esta definição e, portanto, não é seu objetivo conseguir garantir todos os atributos de segurança presentes na taxonomia apresentada. De fato, o mecanismo proposto foi desenvolvido como uma barreira inicial para proteger um grupo de dispositivos de um atacante externo, de modo que diversos atributos de segurança podem ser parcialmente atribuídos ao mecanismo proposto como privacidade, autenticação, integridade e controle de acesso. A utilização do termo parcialmente deve-se ao fato de não ser possível classificar com precisão as funcionalidades do mecanismo proposto dentro da taxonomia descrita, como será visto após a apresentação do mecanismo nas seções a seguir.

O mecanismo de domínios virtuais também deve ser expansível de modo que seja possível associá-lo a outros mecanismos de segurança, como criptografia de chaves públicas ou um processo de distribuição de chaves adequado às redes ad hoc, por exemplo, de modo que essas associações possam assegurar que todos os atributos de segurança da taxonomia apresentada sejam atendidos.

1.2. Desafios de um Ambiente Ad Hoc

Qualquer solução de segurança projetada para uma rede ad hoc é obrigada a lidar com alguns desafios impostos pelas características particulares destes ambientes de redes de computadores.

Em seu artigo, [Feeney, Ahlgren e Westerlund 2001] descrevem cinco desafios que, agregados aos quatro escolhidos por [Zhou e Haas 1999], estabelecem um caminho a ser seguido por qualquer mecanismo proposto cujo objetivo seja garantir a segurança em redes ad hoc. É importante ressaltar que estes desafios não estão limitados apenas aos aspectos de segurança, refletindo os principais pontos que devem ser atendidos para o desenvolvimento de quaisquer aplicações para ambientes ubíquos. A seleção abaixo apresenta resumidamente as visões de [Feeney, Ahlgren e Westerlund 2001] e de [Zhou e Haas 1999], adicionando a estas algumas considerações sobre segurança.

- A ausência de uma fronteira definida em uma rede ad hoc. Uma rede ad hoc possui natureza volátil por definição e, portanto, pode se dividir em um instante e depois se agrupar novamente de modo não previsível. A implicação deste fato é que não é possível definir as fronteiras geográficas destas redes, ou seja, estas não possuem elementos específicos de entrada e saída de informação, de modo que ataques podem ser originados de qualquer ponto da rede.
- A própria natureza dos enlaces sem fio torna a rede ad hoc susceptível a ataques passivos, como *eavesdropping*, e também ativos, como ataques de personificação ou de repetição.
- A ausência de entidades centrais, não permitidas em redes ad hoc por definição já que estes podem não estar ao alcance do de todos os dispositivos a todo o tempo. Esta limitação impõe que qualquer solução de segurança para redes ad hoc deve ser uma solução distribuída, sem a utilização de servidores centrais.

- Não existe garantia que os nós pertencentes a uma rede ad hoc tenham sido pré-configurados. Quaisquer processos que lidem com procedimentos de configuração e que exijam a intervenção humana devem ser intuitivos o bastante para que possam ser manipulados por qualquer usuário. Esta exigência deve-se ao fato de que não se pode considerar que todos os usuários sejam especialistas em configurações de dispositivos, ainda mais quando estão envolvidas questões relativas à segurança.
- Não é possível prever o tamanho de uma rede móvel ad hoc, de modo que qualquer mecanismo de segurança proposto para uma rede ad hoc deve ser aplicável a qualquer tamanho de rede.

A observação a estas considerações deve guiar quaisquer soluções e aplicações propostas para uma rede ad hoc e não deve ser vista apenas como desafios, mas sim como oportunidades para o desenvolvimento de novas soluções que possam ser aplicadas a qualquer ambiente de redes de computadores, ad hoc ou não.

Além disso, os desafios acima citados são um guia útil para o processo de avaliação do mecanismo de domínios virtuais proposto neste artigo. Respeitar e atender estes desafios corresponde ao primeiro objetivo de qualquer mecanismo de segurança a ser proposto para redes ad hoc.

2. Mecanismo de Domínios Virtuais

Um domínio virtual é formado por um grupo de dispositivos móveis e/ou fixos que compartilham uma informação secreta. Além disso, os nós pertencentes a um mesmo domínio virtual confiam nos demais participantes de seu domínio virtual por definição.

Outra característica importante de um domínio virtual é que ele não é geograficamente definido, não existindo fronteiras estabelecidas, já que um domínio virtual existe dentro de cada dispositivo pertencente a ele. Assim, um domínio virtual composto por n diferentes dispositivos pode estar decomposto em m partes e, ainda assim ser, o mesmo domínio virtual.

Uma analogia pode ser feita comparando-se um determinado domínio virtual a uma pequena quantidade de óleo colocada dentro de um copo de água. Os líquidos são, imiscíveis, permanecendo separados um do outro devido às diferentes polaridades de ambos. Agitando o conteúdo do copo com uma colher, o óleo se dividirá em diversas partes menores, gotículas de óleo em meio à água. Deixando o conteúdo do copo em repouso, as gotículas de óleo começarão a se juntar, formando gotas maiores que, finalmente, irão se tornar um único corpo coeso. Deste mesmo modo é um domínio virtual: um conjunto de dispositivos que pode se separar e se juntar novamente de modo natural, como uma gota de óleo dentro de um copo, ligados por uma informação comum, como um segredo compartilhado ou uma propriedade físico-química.

O mecanismo de domínios virtuais foi projetado com o objetivo de garantir um nível mínimo de segurança para ambientes de computação ubíqua nos quais os serviços estão próximos do usuário, dentro de seu campo de visão preferencialmente, sempre possuindo uma característica comum, como pertencer a um usuário ou compartilhar um mesmo espaço, como uma casa ou um escritório.

O mecanismo de domínios virtuais é fundamentado em um processo de desafio/resposta utilizando uma chave secreta compartilhada. O mecanismo proposto procura garantir que estes desafios e respostas não podem ser preditos por uma terceira parte através da utilização de um gerador de números pseudo-aleatórios (PRNG), seguro do ponto de vista criptográfico, que utiliza o tempo corrente como parte de sua semente.

A Figura 1 apresenta a troca de mensagens entre dois dispositivos, **A** e **B**, assim como o conteúdo destas mensagens em um processo de três passos iniciado pelo dispositivo **A**.

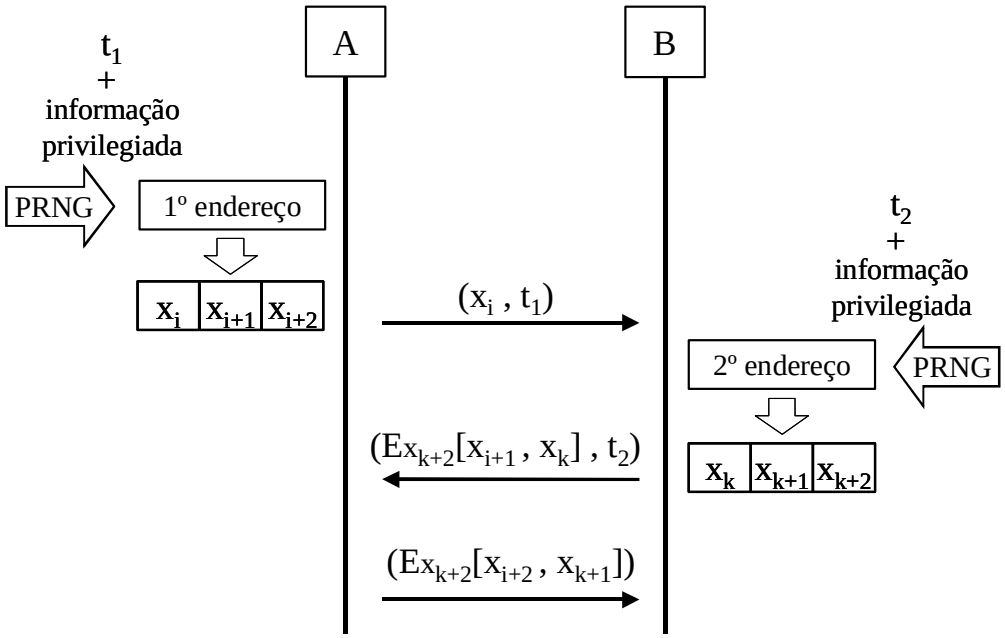

Figura 1: A troca de mensagens executada pelo mecanismo de domínios virtuais.

Sendo que t_1 e t_2 correspondem a índices de tempo, os valores x correspondem a uma parcela do valor pseudo-randômico gerado e o marcador **E***k*[**z**] indica que a informação **z** foi cifrada utilizando-se o algoritmo de criptografia simétrico **E** e a chave *k*.

A primeira mensagem, enviada por **A**, foi chamada de mensagem *desafio*. Uma mensagem desafio é enviada por um dispositivo sempre que este deseja verificar se o dispositivo ao qual irá se comunicar pertence a um domínio virtual reconhecido. Antes de enviar esta mensagem inicial, o dispositivo **A** deve, obviamente, produzir os valores que irão compor a mensagem a ser enviada. Deste modo, o dispositivo **A** verifica o valor de tempo corrente, t_1, e o compõe com o segredo que é compartilhado entre os participantes do domínio virtual **S**, ao qual o dispositivo **A** pertence. Esta composição entre as informações de tempo e o segredo do domínio virtual em questão é utilizada como semente de um gerador de valores pseudo-aleatórios que irá produzir uma seqüência denominada *1º endereço*. Este *1º endereço* é então dividido em três partes: x_i, x_{i+1} e x_{i+2}. A mensagem *desafio* pode agora ser enviada, tendo como campos os valores x_i e t_1.

Esta mensagem *desafio* é recebida e analisada pelo dispositivo **B**. Esta análise é realizada através da verificação do valor x_i da mensagem recebida. Caso **B** faça parte do domínio virtual **S**, verificará que a primeira parte da seqüência do valor, obtido do PRNG tendo como semente a composição do índice de tempo t_1 com o segredo

compartilhado do domínio virtual **S** é igual ao valor x_i da mensagem *desafio* recebida. É importante ressaltar que este valor gerado é, portanto, idêntico ao *1º endereço* produzido pelo dispositivo **A**.

O dispositivo **B**, possuindo então indícios de que **A** pertence a um domínio virtual reconhecido, produz o *2º endereço* através da utilização do mesmo segredo compartilhado e de um segundo índice de tempo, t_2. O *2º endereço* é também dividido em três partes: x_k, x_{k+1} e x_{k+2}. De posse destas informações, **B** é agora capaz de construir uma mensagem resposta a ser enviada para **A**.

A mensagem *resposta* é composta pelo índice de tempo t_2 e pela segunda parcela do *1º endereço*, x_{i+1}, e pela primeira parcela do *2º endereço*, x_k, sendo que estas duas últimas informações são cifradas utilizando-se a terceira parcela do *2º endereço*, x_{k+2}, como chave criptográfica do algoritmo de criptografia simétrico **E**.

Uma vez recebida a mensagem *resposta* enviada por **B**, **A** a verifica através da reprodução do *2º endereço* a partir da informação de tempo t_2 presente na mensagem recebida. De posse do *2º endereço*, **A** utiliza a terceira parcela deste, x_{k+2}, como chave do algoritmo de criptografia simétrico **E** para decifrar a parte protegida da mensagem e então verificar se as parcelas obtidas correspondem aos valores esperados x_{i+1}, e x_k. Caso os valores obtidos correspondam aos esperados, **A** envia uma mensagem de *confirmação* para **B**. Esta mensagem é composta pela terceira parcela do *1º endereço*, x_{i+2}, e pela segunda parcela do *2º endereço*, x_{k+1}, cifradas utilizando-se o algoritmo **E** e tendo como chave a terceira parcela do *2º endereço*, x_{k+2}.

Esta mensagem de *confirmação* é recebida por **B** que verifica seu conteúdo e, caso este corresponda ao valor esperado $\mathbf{E}x_{k+2}[x_{i+2}, x_{k+1}]$, o dispositivo B considera que a partir deste instante possui evidências suficientes que indiquem que **A** pertence a um domínio virtual reconhecido **S**. A chave utilizada até então, x_{k+2}, pelo algoritmo de criptografia **E**, pode ser mantida durante o restante da comunicação entre o par de dispositivos ou pode ser utilizada para uma eventual troca de certificados.

Este procedimento executado pelo mecanismo de domínios virtuais recebeu a denominação de *autenticação de rede*, já que se refere à verificação de que dois dispositivos móveis possuem uma característica comum, de modo que possam pertencer a um mesmo domínio virtual e compartilhar, portanto, um segredo. Este processo ocorre sem que exista a interferência humana, de forma natural e invisível.

O mecanismo proposto apresenta uma proteção intrínseca a ataques contra seu funcionamento, como de repetição intencional de mensagens (também conhecido como ataque *replay*) e o tradicional *man-in-the-middle*, no qual um dispositivo **M** recebe as informações de um dispositivo **A** e as repassa para outro dispositivo **B**, fora do alcance de **A**, fazendo-se passar por este [Stallings 1998]. No entanto, faz-se necessária a apresentação da arquitetura do mecanismo para que seja possível a explanação desta proteção natural do mecanismo a esses ataques de segurança.

3. Arquitetura do Mecanismo de Domínios Virtuais

A arquitetura do mecanismo de domínios virtuais está apresentada na Figura 2, abaixo

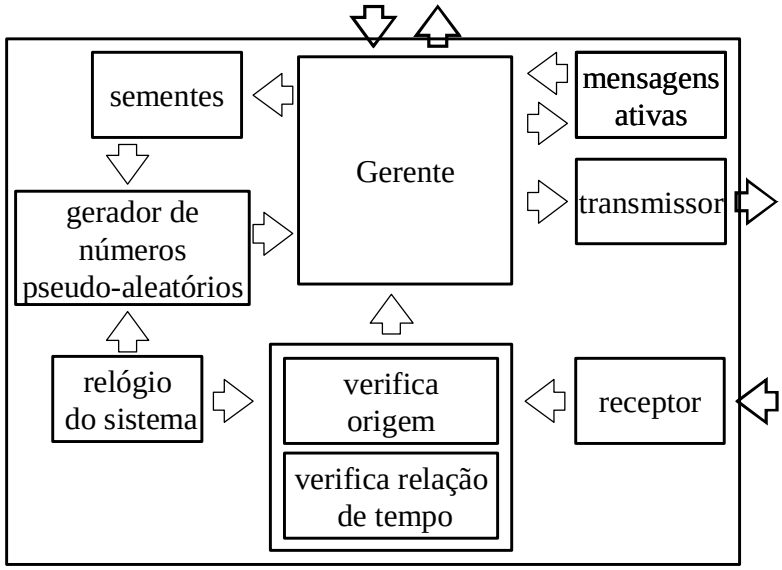

Figura 2: A arquitetura do mecanismo de domínios virtuais.

Assim, temos como blocos constituintes da arquitetura:

- Um gerador de números pseudo-aleatórios (PRNG).
- O relógio do sistema, de onde é retirada a informação temporal para a geração dos valores pseudo-aleatórios.
- Um banco de sementes que armazena o segredo compartilhado de cada um dos domínios virtuais ao qual um dispositivo pertence.
- Blocos de comunicação de dados (recepção/transmissão) para comunicação com o ambiente de rede móvel.
- Um banco de mensagens que armazena as mensagens enviadas que ainda esperam resposta e estejam válidas.
- Um bloco de verificação de mensagens recebidas, relacionadas ao endereço de origem destas mensagens e aos valores de tempo associados a cada uma das mesmas, de modo a se identificar ataques de força bruta e inviabilizar a utilização do mesmo índice de tempo em duas mensagens diferentes.
- Um gerente responsável pela comunicação do mecanismo com o sistema computacional, pela seleção da semente a ser utilizada na geração dos números pseudo-aleatórios, pela verificação dos valores pseudo-aleatórios recebidos e, também, pelo controle do estado de mensagens enviadas e recebidas pelo mecanismo.

A seguir, cada bloco da arquitetura é apresentado e detalhado individualmente.

3.1. O gerador de números pseudo-aleatórios

A função do PRNG é a construção das seqüências denominadas *1º* e *2º endereços* do qual são obtidas as parcelas a serem utilizadas pelo mecanismo de domínios virtuais durante o processo de autenticação de rede.

Um PRNG nada mais é que um algoritmo determinístico utilizado para produzir seqüências de valores aparentemente aleatórias. Todo PRNG necessita de um valor inicial de entrada, a chamada semente, que é utilizada como ponto de partida para a produção de seqüências. O PRNG necessário para o mecanismo de domínios virtuais deve possuir algumas características especiais em relação ao seu funcionamento. Estas características são:

- Deve ser seguro do ponto de vista criptográfico, ou seja, imprevisível.
- Deve ser capaz de aceitar um parâmetro de entrada arbitrário e público sem que exista prejuízo da primeira característica supracitada.

O processo de escolha do PRNG é apresentado na próxima seção, relativa aos aspectos de implementação do mecanismo.

3.2. O banco de sementes

Cada dispositivo pode ser membro de mais de um domínio virtual. Deste modo, se torna necessário armazenar uma semente, ou segredo, diferente para cada domínio conhecido, já que cada um possui uma semente única.

As sementes são, de fato, um segredo compartilhado entre os diversos dispositivos que compõem um domínio virtual. Um conjunto de dispositivos possui a mesma semente apenas se pertencerem ao mesmo domínio e, portanto, compartilharem de alguma característica comum, como pertencer ao mesmo dono ou família, ou fazer parte de um mesmo ambiente, como os dispositivos de um escritório, de uma casa, ou, até mesmo, equipamentos de um mesmo batalhão, por exemplo.

Uma semente é, como qualquer chave, uma seqüência longa de valores, que o usuário não necessita ter acesso ou conhecimento, já que se trata de uma informação a qual apenas o mecanismo proposto tem interesse e direito de acessar. No entanto, toda semente está associada a um nome que a identifica, de modo que, se necessário, seja permitido ao usuário poder escolher o domínio desejado de modo natural e intuitivo, relacionando-o a um nome comum, como "*casa*" ou "*escritório*", por exemplo.

Pode-se assumir tranqüilamente que o número de sementes armazenadas em um banco de sementes é, em média, pequeno, já que são poucos os dispositivos que se movimentam entre diversos domínios diferentes.

3.3. Blocos de verificação das relações temporais e de endereço origem

O objetivo dos blocos de verificação das relações temporais e do endereço origem é garantir a resistência do mecanismo de domínios virtuais a alguns ataques, como os de repetição e de força bruta.

O bloco de verificação das relações temporais define uma janela de tempo ao redor do tempo atual do dispositivo, aceitando apenas mensagens cujo valor de tempo

associado encontra-se dentro da janela definida. A verificação é feita através da comparação do limite superior e do inferior da janela de tempo com o índice de tempo (t_1 caso a mensagem recebida seja um *desafio* ou t_2 se for uma *resposta*). A Figura 3, abaixo, ilustra a janela de tempo de um dispositivo qualquer.

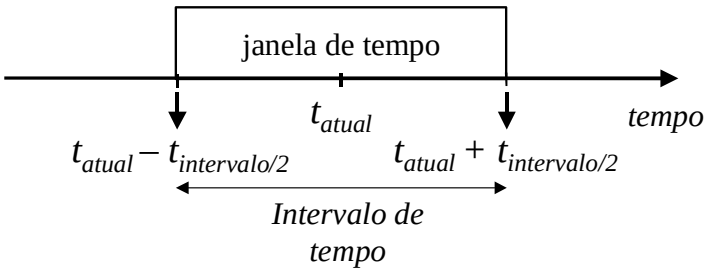

Figura 3: Janela de tempo.

Caso uma mensagem recebida apresente um índice de tempo que já tenha sido utilizado ou que esteja fora dos limites da janela de tempo, ela é descartada sem que seja executada qualquer outra verificação, o que significaria um gasto desnecessário de recursos de processamento e energia, geralmente escassos em dispositivos móveis. É importante ressaltar que esta medida pode, prematuramente, impedir a ocorrência de ataques de repetição, ao determinar que toda mensagem enviada durante o processo de autenticação de rede tenha um prazo de validade determinado.

É importante ressaltar que a utilização de janelas de tempo permite que os relógios de sistema dos dispositivos pertencentes a um domínio virtual não necessitam estar em perfeito sincronismo e possam ainda apresentar diferentes resoluções, o que é uma característica particularmente importante, já que um domínio virtual pode ser composto por dispositivos das mais diversas arquiteturas. Os valores de tempo trocados entre os dispositivos no processo de autenticação de rede devem ter sua resolução uniformizada e os índices de tempo convertidos para a referência UTC (*coordinated universal time*), de modo a padronizar o formato dos índices de tempo trocados entre os dispositivos de um domínio virtual.

A verificação de endereço origem das mensagens recebidas tem como objetivo detectar o comportamento anormal de um dispositivo, identificado através de seu endereço de origem. Como exemplo de comportamento anormal pode ser citada a ocorrência de diversas mensagens *resposta* em seqüência, relativas a uma única mensagem *desafio*, por exemplo, o que pode caracterizar um ataque de força bruta ou uma tentativa de ataque de exaustão de bateria, ou seja, uma tentativa de consumir os recursos do dispositivo alvo através de gasto desnecessário de processamento.

3.4. Bloco de mensagens ativas

O bloco de mensagens ativas armazena as mensagens enviadas e ainda determina um tempo de validade para as mesmas. As mensagens são identificadas através de um parâmetro que as identifica univocamente para o mecanismo. Este parâmetro é o *número de seqüência* da mensagem, que deve ser enviado juntamente com qualquer mensagem *desafio*. O bloco de mensagens ativas também armazena o *1º* e *2º endereços* associados a cada uma das mensagens enviadas, de modo a ser necessário calcular apenas uma vez cada um destes valores.

O *número de seqüência* de uma mensagem, além de ser utilizado como simples identificação de uma mensagem enviada, é utilizado também para relacionar uma mensagem *desafio* a uma mensagem *resposta* e esta a uma mensagem de *confirmação*. Sendo assim é possível identificar a relação entre as mensagens recebidas e as armazenadas pelo mecanismo e garantir que um dispositivo responderá apenas a mensagens *reposta* para a qual tenha enviado previamente uma mensagem *desafio*, protegendo o mecanismo de ataques de fabricação [Stallings 1998].

O tempo de validade de uma mensagem enviada é igual a, no mínimo, duas vezes o tempo de transmissão de uma mensagem para um dispositivo à máxima distância permitida pela tecnologia de rede utilizada, ou seja, 10 metros para equipamentos Bluetooth, por exemplo, adicionado ao tempo estimado de processamento da mensagem enviada. A Figura 4, abaixo, ilustra a janela de tempo correspondente ao tempo de validade mínimo de uma mensagem transmitida.

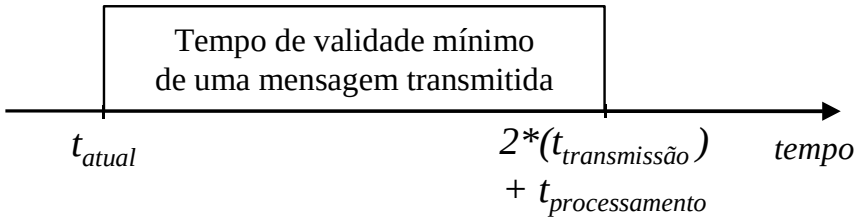

Figura 4: Tempo de validade mínimo de uma mensagem transmitida.

No entanto, deve-se ressaltar que o tempo de processamento de uma mensagem no dispositivo destino é difícil de ser estimado, já que depende de vários fatores, como o seu processador, a quantidade de sementes armazenadas no mesmo (quanto maior o número de sementes, maior é a quantidade de valores a serem calculados e verificados) e o PRNG utilizado.

3.5. Gerente e blocos de comunicação

O gerente é responsável pela comunicação interna entre os diversos blocos que compõem a arquitetura do mecanismo de domínios virtuais, controlando e direcionando o fluxo de informação do sistema. Ele também recebe as mensagens *desafio* que passam pelos blocos de verificação de relações temporais e de endereço origem e verifica, através de requisições ao banco de sementes e ao PRNG, a qual semente corresponde um *desafio* recebido.

O gerente também é responsável pela interface interna do mecanismo, seja com outro programa ou com o usuário final, recebendo requisições por procura de um determinado domínio virtual e determinando o envio de mensagens *desafio*.

Os blocos de comunicação correspondem à unidade de recepção e transmissão de dados do dispositivo, ou seja, sua interface de rede com o ambiente móvel ou fixo. É importante ressaltar que o mecanismo de domínios virtuais é independente da tecnologia de transmissão utilizada.

4. Implementação

Esta seção descreve os aspectos de implementação do protótipo do mecanismo proposto considerados de relevância, como a máquina de estados do mecanismo, a escolha do gerador de números pseudo-aleatórios e o comprimento em bits dos índices de tempo e das parcelas transmitidas.

4.1. Escopo e aspectos gerais da implementação

A implementação do protótipo do mecanismo de domínios virtuais é parte componente de um modelo de segurança para redes móveis ad hoc [Venturini et al.2002]. O papel do mecanismo proposto dentro deste modelo de segurança é atuar como uma barreira inicial de segurança de modo a evitar atacantes externos.

A linguagem de programação escolhida para o desenvolvimento do protótipo foi o Java devido, principalmente, à independência de arquitetura de sistema do código gerado, já que os *bytecodes* produzidos podem ser interpretados por qualquer máquina virtual Java. A versão da plataforma Java utilizada foi a J2SDK SE v.1.4.0. O acesso ao mecanismo era executado, originalmente, através de seus métodos públicos, mas uma interface texto simples foi adicionada para testes de demonstração fora do ambiente do modelo de segurança. O protótipo é, como esperado para uma aplicação de uma rede móvel ad hoc, *peer-to-peer*, ou seja, adequada para um ambiente ubíquo.

4.2. Máquina de estados finita

Seguindo a Figura 1, relativa à troca de mensagens executada pelo processo de autenticação de rede realizado entre dois dispositivos (**A** e **B**) pertencentes ao mesmo domínio virtual (**S**), podemos identificar oito estados distintos. A Tabela 1 apresenta estes estados, numerando-os e nomeando-os.

Tabela 1: Estados do mecanismo de domínios virtuais.

Estado	Nome do Estado
0	Inativo.
1	Esperando mensagem resposta.
2	Verificando mensagem desafio.
3	Esperando mensagem réplica.
4	Verificando mensagem resposta.
5	Esperando mensagem OK.
6	Verificando mensagem réplica.
7	Conectado.

A máquina de estados finita do mecanismo de domínios virtuais é apresentada a seguir, na Figura 5. A linhas cheias correspondem ao caminho percorrido pelo mecanismo quando este inicialmente envia uma mensagem *desafio* enquanto as linhas tracejadas correspondem ao caminho percorrido pelo mecanismo quando este recebe uma mensagem desafio.

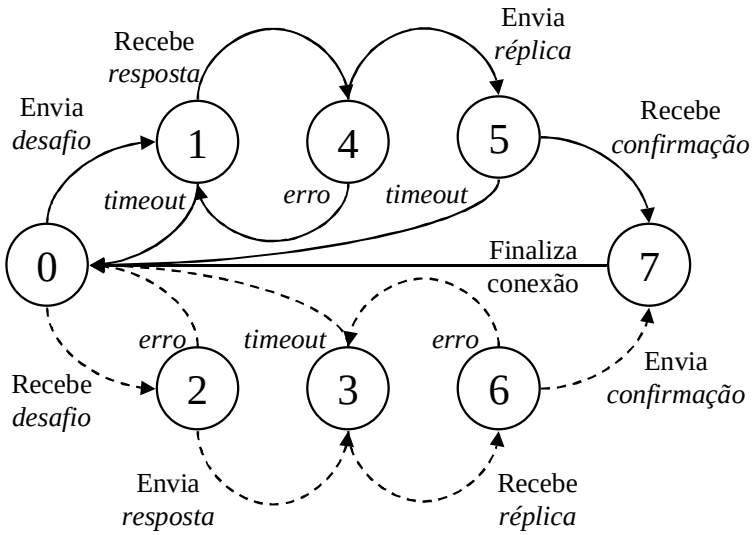

Figura 5: Máquina de estados finita do mecanismo de domínios virtuais.

Timeouts ocorrem toda vez que uma mensagem excede seu tempo de vida, que é definido pelo tempo de validade de uma mensagem enviada, enquanto que erros ocorrem toda vez que um mecanismo recebe uma mensagem de conteúdo inválido.

Erros e *timeouts* têm impactos diferentes sobre a máquina de estados finita do mecanismo de domínios virtuais. Erros sempre causam o retorno para o estado imediatamente anterior ao estado atual, enquanto *timeouts* sempre causam o retorno para o estado inicial 0 (inativo).

4.3. O PRNG

O PRNG a ser utilizado pelo mecanismo teve como critério inicial de seleção os requisitos apresentados previamente no item 3.1. Como critérios adicionais foram definidos: o desempenho do gerador em termos de quantidade de processamento exigido pelo seu algoritmo, o tamanho da seqüência produzida e o tamanho máximo da semente.

Foram selecionados para avaliação os PRNG analisados de acordo com seus aspectos de segurança em [Kelsey et al. 1998], o PRNG Blum Blum Shub [Blum, Blum e Shub 1986], e o Yarrow-160 [Kelsey, Schneier e Ferguson 1999].

Inicialmente foram descartados o Yarrow-160 e o RSAREF[1], já que ambos utilizam o valor previamente gerado como entrada para a geração da próxima seqüência, o que torna inviável a aplicação destes em um ambiente móvel ad hoc, pois não existe sincronização de geração de valores dentro de um domínio virtual e não é razoável supor que todos os dispositivos tenham conhecimento de quantos valores foram previamente produzidos pelos demais dispositivos.

O PRNG Blum Blum Shub atende a ambos os requisitos definidos no item 3.1. No entanto, este PRNG necessita de uma grande quantidade de processamento para que se possa obter uma seqüência de números de tamanho razoável, já que cada interação de

[1] Implementação de referência de criptografia proposta pelo RSA Laboratories, fundamentado em uma função de *hash* MD5 e adições módulo 2^{128} [RSA Laboratories 1994].

seu algoritmo é capaz de fornecer apenas um ou dois bits. Deste modo, pode-se descartar a utilização do PRNG Blum Blum Shub no mecanismo de domínios virtuais.

Os PRNG DSA[2] [NIST 2000] e ANSI X9.31[3] [ABA 1998] necessitam de uma pequena modificação em seus algoritmos para que possam se adequar aos requisitos definidos no item 3.1. Em ambos os casos trata-se da supressão do passo de atualização da semente. Dentre estes dois geradores, foi escolhido o PRNG DSA por ser capaz de produzir seqüências de 160bits e aceitar sementes de até 512bits, enquanto que o PRNG ANSI X9.31 consegue produzir apenas 64bits e possui chaves de 112bits (utilizando o 3DES com duas chaves). O algoritmo do gerador PRNG DSA com a supressão do passo de atualização da semente é apresentado abaixo:

$$saída = hash\left((timestamp + semente) \bmod 2^b\right), \text{ sendo } 160 \le b \le 512 \quad (1)$$

Uma vez definido o PRNG a ser utilizado pelo mecanismo de domínios virtuais, este foi devidamente avaliado e analisado, já que foram executadas alterações em seu funcionamento básico (no caso, a supressão do passo de atualização da semente), o que tornou necessária sua reavaliação, de modo a se verificar se as propriedades básicas do PRNG não foram afetadas. Este PRNG DSA modificado foi então submetido a uma série de testes que incluíram [Menezes, Oorschot e Vanstone 1996]:

- Testes de hipótese não-paramétrico de modo a verificar se as amostras produzidas pelo gerador aderem a uma distribuição χ^2.
- Quatro diferentes testes estatísticos: o teste de freqüência, o teste serial, o teste pôquer e o teste de comprimento de seqüência. Todos testes de hipótese que analisam se uma seqüência binária de comprimento arbitrário possui características de uma verdadeira seqüência aleatória.
- Uma bateria de testes padrão, a FIPS PUB 140-2 (NIST 2001).

Para o teste de hipótese χ^2 foram utilizados quatro amostras de 10 mil valores (sendo cada valor com 160 bits de comprimento) e outras quatro amostras de 100 mil valores. Para os demais testes foram utilizados quatro amostras com 20 mil bits de comprimento. O gerador passou com sucesso em todos os testes. Mais detalhes sobre estes testes, incluindo os gráficos de distribuição de valores das amostras (*scatter plots*) e os seus respectivos histogramas podem ser encontrados em [Martucci 2002].

4.4. As parcelas transmitidas e o índice de tempo utilizado.

Uma vez definido o PRNG a ser utilizado foi possível determinar o tamanho de cada parcela transmitida. Como cada valor produzido possui 160 bits de comprimento, este foi dividido em quatro parcelas de 40 bits, sendo a quarta parcela não inicialmente

---

[2] O PRNG DSA pertence ao padrão DSS (Digital Signature Standard) da NIST (National Institute of Standards Technology) que especifica um grupo de algoritmos a serem utilizados para produzir assinaturas digitais. Tem como bloco principal a função de *hash* SHA-1.

[3] O PRNG ANSI X9.31 é o gerador de números padrão utilizado pelo algoritmo de criptografia DES (Data Encryption Standard) para geração de chaves simétricas e tem, como bloco principal, um algoritmo de criptografia de blocos (sendo o 3DES comumente utilizado).

utilizada e podendo ser adicionada à terceira parcela do *2º endereço*, ou reservada para futura utilização. O índice de tempo é dado em milésimos de segundo e é definido através da utilização de um contador de 64 bits, de modo que o período da seqüência produzida por um gerador, sem que ocorra a alteração do segredo, é de 2^{64} milésimos de segundo, ou seja, aproximadamente 584 milhões de anos.

5. Trabalhos Relacionados

Um mecanismo semelhante ao descrito neste artigo é a solução de autenticação SecurID [RSA Security Inc 2002]. Essa solução utiliza pequenos dispositivos portáteis que, assim como o mecanismo de domínios virtuais, faz uso de um gerador de números pseudo-aleatórios, que possui como parâmetros de entrada uma semente compartilhada e uma informação de tempo. No entanto, a solução SecurID depende de um repositório central para o armazenamento de sementes, e exige o sincronismo entre os relógios dos dispositivos portáteis e do servidor, não sendo, assim, adequada para uma rede móvel ad hoc. O mecanismo de domínios virtuais, ao contrário, independe de entidades centrais, utilizando sementes distribuídas, não exige o sincronismo dos relógios dos dispositivos que compõem um determinado domínio de dispositivos e também não necessita, a princípio, de intervenção humana, já que se trata de um processo de autenticação entre dispositivos.

Comparando o mecanismo proposto com o mecanismo de autenticação *shared secret* previsto no padrão de redes móveis IEEE 802.11, que é fundamentado no WEP (*Wired Equivalent Privacy*), a única semelhança existente é o fato de que ambos utilizam chaves compartilhadas e tem como objetivo a autenticação de dispositivos. As mensagens trocadas pelo mecanismo de domínios virtuais não possuem desafios a serem cifrados e devolvidos, mas sim mensagens a serem completadas e geração dinâmica de chaves simétricas (índice *k+2* do 2º endereço produzido), enquanto que o WEP utiliza a mesma chave simétrica em todo o seu processo. Além disso, os índices de tempo do mecanismo proposto não possuem nenhuma semelhança com o *IV* do WEP, além do fato de serem transmitidos sem criptografia, já que o primeiro é utilizado na geração dos valores pseudo-randômicos e o segundo é parte da chave simétrica.

Um outro mecanismo para autenticação automática entre dispositivos em uma rede móvel ad hoc é o modelo de segurança Resurrecting Duckling [Stajano 2000]. A autenticação entre os dispositivos é executada através da utilização de chaves públicas e criptografia assimétrica e a distribuição de chaves é realizada por intermédio de um dispositivo central, denominado de *cyber-representative*. A utilização de criptografia assimétrica como única opção para autenticação de dispositivos em uma rede móvel ad hoc pode ser desgastante em termos de processamento e consumo de bateria para dispositivos mais limitados.

6. Conclusões Finais

Este artigo apresenta a especificação de um mecanismo, denominado mecanismo de domínios virtuais, a ser utilizado no processo autenticação entre dispositivos que compartilham alguma característica comum, como pertencerem a um mesmo usuário ou um mesmo ambiente, como uma casa ou um escritório. O mecanismo proposto é

fundamentado em um PRNG que tem como entradas um parâmetro público, um índice de tempo e um secreto, que é compartilhado entre os integrantes de um domínio virtual.

Este mecanismo é adequado às redes móveis ad hoc, respeitando as premissas básicas, descritas no item 1.2 deste artigo, já que um domínio virtual não possui e nem precisa possuir fronteiras definidas, de modo que a sua natureza volátil acompanha os movimentos da rede móvel ad hoc. Do mesmo modo, o mecanismo de domínios virtuais independe de entidades centrais e do tamanho e da quantidade de dispositivos presentes.

Nenhuma informação crítica é transmitida em aberto pelo mecanismo proposto, de modo que ataques passivos não são capazes de obter nenhuma informação útil das mensagens transmitidas. Algumas mensagens transmitidas (*resposta* e *confirmação*) possuem seu conteúdo cifrado por uma chave que não é transmitida em momento algum, tornando a atividade de criptoanálise de dados capturados praticamente infrutífera e protegendo os dispositivos da ação de ataques *man-in-the-middle*, pois a manutenção do uso da chave simétrica após a realização do processo de autenticação de rede impede a obtenção de qualquer informação útil por parte do atacante. A utilização do controle e verificação dos índices de tempo das mensagens recebidas e a utilização de um mecanismo de três passos impossibilitam a ação de ataques de repetição.

O mecanismo de domínios virtuais também não necessita de intervenção humana, pois o processo de autenticação de rede pode ocorrer de modo transparente ao usuário, que não precisa ter conhecimento do processo ocorrido, mas apenas ter ou não acesso aos serviços oferecidos por um segundo dispositivo.

Sendo assim, pode-se concluir que o mecanismo de domínios virtuais é completamente adequado a uma rede móvel ad hoc, respeitando suas premissas, além de necessitar de menos recursos que outras soluções apresentadas e fundamentadas apenas na utilização de criptografia assimétrica. De qualquer modo, caso se faça necessário um processo de autenticação individual, com o uso de certificados e chaves assimétricas, este deve ser precedido pelo mecanismo de domínios virtuais, de modo que os recursos do dispositivo sejam utilizados somente quando existe evidência suficiente de que estes não serão desperdiçados.

Assim sendo, a utilização do mecanismo de domínios virtuais é particularmente benéfica, trazendo apenas ganho para uma rede ad hoc.

References

AMERICAN BANKERS ASSOCIATION – ABA (1998). **Digital signatures using reversible public key cryptography for the financial services industry** (rDSA). ANSI X9.31. 1998. App.A.2.4.

BLUM, L.; BLUM, M. SCHUB, M. (Blum Blum Shub 1986) A simple unpredictable pseudo-random number generator. **SIAM Journal of Computing**, v.15, n.2, p.364-383, May 1986.

CORSON, S.; MACKER, J. (1999). Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. **IETF Network Working Group Request for Comments**. Jan. 1999. RFC2501.

FEENEY, L.M., AHLGREN, B., WESTERLUND, A. (2001). Spontaneous network: an application oriented approach to ad hoc networking. **IEEE Communications Magazine**, v.39, i.6, p.176-181, Jun. 2001.

KELSEY, J. et al. (1998). Cryptanalytic attacks on pseudorandom number generators. In: INTERNATIONAL WORKSHOP ON FAST SOFTWARE ENCRYPTION, 5., Lecture Notes in Computer Science, Springer-Verlag, Mar. 1998. **Proceedings**. Paris, France, 1998. p. 168-188.

KELSEY, J.; SCHNEIER, B.; FERGUSON, N. (1999). Yarrow-160: Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In: INTERNATIONAL WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY, 6., Lecture Notes in Computer Science, Springer-Verlag, Aug. 1999. **Proceedings**. Kingston, Ontario, Canada, 1999. p.13-33.

MARTUCCI, L.A. (2002). **Domínios Virtuais para Redes Móveis Ad Hoc**: um mecanismo de segurança. 2002. 136p. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo. São Paulo.

MENEZES, A.J.; OORSCHOT, P.C.V.; VANSTONE, S.A. (1996). **Handbook of Applied Cryptography**. Boca Raton, Florida, USA: CRC Press, 1996. 816p.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST (2000). **FIPS 186-2: Digital Signature Standard** (DSS). Federal Information Processing Standards Publication 186-2. Gaithersburg, Maryland, USA: NIST, Jan. 2000. App.3. p.16-19: Random number generation for the DSA.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST (2001). **FIPS PUB 140-2: Security Requirements for Cryptography Modules**. Federal Information Processing Standards Publication 140-2. Gaithersburg, Maryland, USA: NIST, May. 2001. 64p.

RSA LABORATORIES (1994). **RSAREF: a cryptographic toolkit**. version 2.0. RSA Data Security, Inc, Mar. 1994. Disponível em: <ftp://ftp.funet.fi/pub/crypt/ cryptography/ asymmetric/rsa/rsaref2.tar.gz>. Acesso em: 15 Jun. 2002.

RSA SECURITY INC. (2002). **RSA SecurID Authentication**: a better value for a better ROI. RSA Whitepaper. Disponível em: <http://www.rsasecurity.com/products/ securid/>. Acesso em: 15 Aug. 2002.

STAJANO, F. (2000). The resurrecting duckling: what next? In: INTERNATIONAL WORKSHOP ON SECURITY PROTOCOLS, 8., Lecture Notes in Computer Science, Springer-Verlag, Apr. 2000. **Proceedings**. Santa Barbara, CA, USA, 2000.

STALLINGS, W. (1998) **Cryptography and network security**: principles and practice. 2.ed. Upper Saddle River, New Jersey: Prentice Hall, 1998. 569p.

VENTURINI, Y.R. et al. (2002). Security model for ad hoc networks. In: INTERNATIONAL CONFERENCE ON WIRELESS NETWORKS – ICWN'02. Las Vegas: CSREA Press, Jun. 2002. **Proceedings**. Las Vegas, NV, USA, 2002.

ZHOU, L., HAAS, Z.J. (1999). Securing Ad Hoc Networks. **IEEE Network**, v.13, i.6, p.24-30, Nov./Dec. 1999.