CHARADAS: Uma proposta para uso de CHAve de grupo no Roteamento Através de Distribuição Assimétrica Segura

Natalia Castro Fernandes, Otto Carlos Muniz Bandeira Duarte

[1]Grupo de Teleinformática e Automação – Universidade Federal do Rio de Janeiro (UFRJ)
C. P. 68504 - 21945-970, Rio de Janeiro, RJ - Brasil

{natalia,otto}@gta.ufrj.br

Abstract. *This paper proposes a hybrid group key distribution protocol called CHARADAS. It is efficient with high rates of key renewal, network partitions and new nodes entering the network. CHARADAS was designed to be used with the Secure Optimized Link State Routing Protocol (SOLSR), safeguarding routing messages integrity. The main objective is to allow the group key exchange automatically, using the SOLSR flooding control mechanism called Multipoint Relays (MPR), to avoid non-authorized access. The key exchange process uses asymmetric cryptography to identify the users and it can be initiated periodically, by an administrator or by an intrusion detect system request. The proposal is adapted to Internet of Things and local area networks scenarios.*

Resumo. *Este artigo propõe o protocolo híbrido CHARADAS de troca de chave de grupo, eficiente com altas taxas de renovação de chaves, partições na rede e entrada de novos nós. O CHARADAS foi projetado para utilização com o Secure Optimized Link State Routing Protocol (SOLSR), auxiliando na proteção da integridade das mensagens de roteamento. O objetivo é permitir a troca de chaves de forma automática, utilizando a técnica de controle de inundação dos Multipoint Relays, para evitar o acesso de usuários não-autorizados. O processo de troca de chaves, que faz uso de criptografia assimétrica para a identificação dos usuários autorizados, pode ser iniciado periodicamente, ou ainda por pedido do administrador ou de um sistema de detecção de intrusão. A proposta se adapta tanto a cenários de Internet de Coisas quanto a redes locais de usuários.*

1. Introdução

A popularização do uso de redes móveis permitiu o desenvolvimento de novas tecnologias tanto para redes com ponto de acesso como para redes ad hoc para o uso doméstico, empresarial, industrial e comunitário. O uso cada vez maior dessas redes leva a uma busca por mecanismos seguros que permitam garantir a integridade e privacidade dos dados. Além disso, os investimentos previstos para os próximos anos atingem grandes cifras, o que incentiva o surgimento de novas aplicações para redes ad hoc, como o controle automático de estoques, assistência remota de convalescentes, *Body Area Networks*, Internet de Coisas, entre outros. No entanto, muitas dessas aplicações utilizam equipamentos com pouca capacidade de processamento e armazenamento, o que restringe o conjunto de métodos de segurança que podem se utilizados. Outra possível restrição é o uso de bateria, em especial nos dispositivos móveis. Assim, é necessário o desenvolvimento de medidas de segurança que consigam poupar ao máximo os recursos dos dispositivos.

As redes ad hoc móveis são baseadas em roteamento colaborativo por múltiplos saltos, onde todos os nós da rede são roteadores. Essa característica confere a essas redes inúmeras vulnerabilidades, pois o comportamento malicioso de um único nó pode impedir o funcionamento de toda a rede. Por essa razão, protocolos como o *Authenticated Routing for Ad-Hoc Networks* (ARAN) [Sanzgiri et al., 2002], *Secure Ad hoc On-Demand Distance Vector Protocol* (SAODV) [Zapata, 2002] e o *Secure Optimized Link State Routing Protocol* (SOLSR) [Hafslund et al., 2004] foram propostos com a intenção de adicionar segurança ao roteamento, através de técnicas de autorização e garantia de integridade das mensagens de roteamento. No entanto, todos os protocolos de roteamento seguro propostos supõem a existência de um sistema de distribuição de chaves, o que não é um problema resolvido para redes ad hoc, em especial devido à característica de ausência de infra-estrutura dessas redes.

A utilização de assinaturas nas mensagens de roteamento permite que os nós da rede verifiquem a integridade da mensagem. Para isso, existem as abordagens da assinatura digital, que utiliza chaves assimétricas e permite a identificação do usuário, e da assinatura com chaves simétricas de grupo, que permite identificar se o nó pertence ao grupo dos nós autorizados. O uso de chaves de grupo tem como vantagem o baixo gasto de energia, quando comparado aos protocolos que utilizam criptografia assimétrica. Por outro lado, a desvantagem é não proteger a rede contra nós que possuem a chave de grupo e têm atitude maliciosa. Além disso, existe o problema de controle de acesso, pois qualquer usuário pode repassar a chave de grupo, deixando a rede exposta.

Esse artigo apresenta uma solução de sistema de distribuição de chaves de grupo simétricas para o SOLSR, baseado na troca periódica ou por requisição da chave de grupo, com autenticação assimétrica. O objetivo desse sistema é prover segurança com poucos gastos de recursos, se adequando a diversos cenários. Na Figura 1 está representado o gasto de energia com criptografia e transmissão do protocolo SOLSR, caso ele fosse modificado para utilizar criptografia assimétrica. Essa modificação se justifica por aumentar a robustez do protocolo contra possíveis atacantes internos, ou seja, nós, autorizados ou não, que possuem o segredo da rede e participam desta com o objetivo de causar problemas, como *loops* de roteamento. Ao se utilizar chaves de grupo, qualquer usuário autorizado da rede pode repassar a chave de grupo com a qual assina as mensagens de roteamento para outro usuário não autorizado. Desta forma, o usuário não-autorizado ganha o direito de participar da rede, podendo realizar ações maliciosas sem ser identificado. Quando se utiliza criptografia assimétrica para assinar as mensagens de roteamento, é possível garantir que nenhum usuário intermediário que encaminhou a mensagem modificou o seu conteúdo. Além disso, é possível saber se um usuário é autorizado ou não para utilizar a rede observando a sua chave pública, supondo que existe uma lista de identificações e chaves públicas dos nós autorizados a utilizar a rede. Por outro lado, a criptografia assimétrica consome muita energia, o que impede o seu uso em situações em que existam nós com restrições de recursos. Desta forma, existe a necessidade de um sistema de distribuição de chaves de grupo que não utilize muitos recursos dos nós e que dê maior segurança ao roteamento na rede.

Este artigo está organizado da seguinte forma: a Seção 2 faz uma descrição do estado da arte das propostas para distribuição de chaves de grupo, enquanto que a Seção 3 faz uma breve descrição do funcionamento dos protocolos *Optimized Link State Routing*

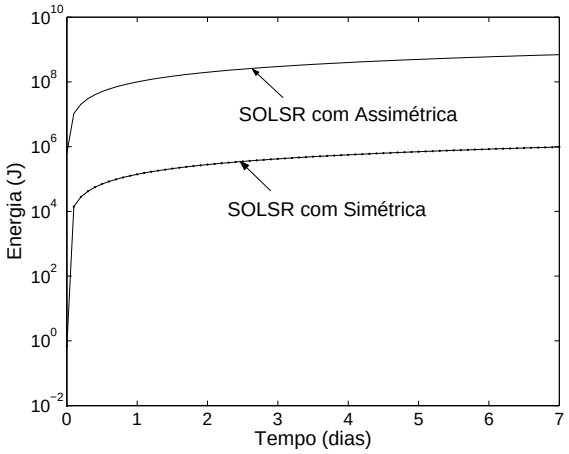


Figura 1. Custo energético do SOLSR com criptografia simétrica e assimétrica.

protocol (OLSR) e SOLSR. Na Seção 4 é feita uma descrição do cenário e suposições para o funcionamento correto do CHARADAS. A Seção 5 faz a descrição do protocolo proposto e a Seção 6 traz uma comparação matemática entre o uso do SOLSR com chaves de grupo simétricas e com o CHARADAS e o SOLSR com criptografia assimétrica. Por fim, na Seção 7, são apresentadas as conclusões do artigo.

2. Sistemas de troca de chave de grupo

Os protocolos de gerenciamento de chave de grupo podem contar com uma pré-distribuição de chaves, realizar trocas de chaves observando a contribuição de cada nó da rede ou utilizar uma origem que dissemina o segredo para os demais nós da rede. Neste terceiro caso, a origem do grupo é responsável pela geração e distribuição da chave para cada membro do grupo. As ações de gerar e distribuir as chaves são realizadas após a observação dos eventos de entrada e saída, seguindo as políticas de segurança consideradas pela aplicação. A principal desvantagem desta proposta centralizada é que a origem do grupo representa um ponto de falha, quando são considerados os problemas relacionados à segurança e ao gargalo na rede [Bouassida et al., 2006]. O CHARADAS utiliza distribuição pela origem, mas trata o problema de falha e sobrecarga da origem através mecanismos próprios de troca da origem e substituição em caso de falha.

Muitas propostas de sistema de distribuição de chaves têm como objetivo o gerenciamento de chaves para grupos *multicast*. Entre essas, existem propostas de gerenciamento distribuído, na quais o segredo é alcançado pela cooperação e colaboração de todos os membros de um grupo *multicast*. Portanto, o objetivo é assegurar uma comunicação segura entre os membros pertencentes a este grupo. Nesta linha, foi proposto um protocolo para gerenciamento distribuído de chave de grupo baseado em medidas GPS (*Global Positioning System*) e no protocolo *Group Diffie Helmann* (GDH) [Chiang e Huang, 2003]. Neste protocolo, cada nó da rede ad hoc envia sua posição geográfica obtida através do GPS e sua chave pública para todos os outros nós, o que gera um alto consumo de energia e banda, com o objetivo de permitir a construção da topologia da rede.

Salah e Festor propõem um modelo de clusterização eficiente para a distribuição de chaves *multicast* na camada de aplicação em redes ad hoc [Bouassida et al., 2006]. Neste trabalho é mostrado que a proposta pode ser combinada com a técnica *Multipoint*

Relaying (MPR), de diversas e eficientes formas, de acordo com a localização dos membros de grupo e da mobilidade. A eficiência considerada está relacionada com a latência média da entrega de chaves, o consumo de energia e a razão de entrega de chaves. O CHARADAS utiliza os MPRs do protocolo OLSR, com o objetivo de reduzir o número de retransmissões e estabelecer uma árvore de transmissão da nova chave de grupo. No entanto, o modelo proposto visa à troca de chaves para proteção do roteamento.

Outros protocolos também foram propostos para a distribuição de chaves em redes ad hoc. Liao faz um estudo de protocolos como o *Tree-Based Group Diffie-Hellman Protocol*(TGDH), além de propor otimizações [Liao, 2005].

3. Protocolos *Optimized Link State Routing protocol* (OLSR) e *Secure Optimized Link State Routing protocol* (SOLSR)

O OLSR [Jacquet et al., 2001] é um protocolo de roteamento para redes ad hoc móveis pró-ativo, ou seja, que calcula as rotas para todos os possíveis destinos em avanço, baseado em estado de enlace. Na técnica de estado de enlace o protocolo mantém um mapa da topologia completa da rede, através do qual ele irá calcular a sua tabela de roteamento. Para obter essa informação o protocolo utiliza mensagens de controle enviadas periodicamente, que podem ser transmitidas por difusão ou inundação. Para evitar problemas com as constantes inundações, o OLSR possui um mecanismo de controle de inundação chamado de *Multipoint Relay* (MPR). Neste mecanismo, apenas os nós escolhidos como MPRs de um determinado nó reencaminham os pacotes deste nó. Os MPRs são selecionados por cada nó dentre o seu conjunto de vizinhos de um salto de forma a atingir todos os vizinhos por dois saltos. Dessa forma, é feito um controle de tráfego gerado pelo protocolo de roteamento eficiente.

O protocolo OLSR possui três tipos de mensagens: `HELLO`, `TC` e `MID`. As mensagens de `HELLO` são responsáveis pela detecção do tipo de enlace, detecção de vizinhança e sinalização de *Multipoint Relays* (MPRs) . As mensagens de `TC` (*Topology Control*) descrevem a topologia, anunciando os estados dos enlaces. Por fim, as mensagens de `MID` (*Multiple Interface Declaration*) declaram a existência de múltiplas interfaces no nó. Outros tipos de mensagem também são permitidos, seja para funções de conservação de energia, roteamento *multicast*, suporte para enlaces unidirecionais, determinação automática de endereços, entre outros.

O SOLSR [Hafslund et al., 2004, Tønnesen, 2004] é uma extensão para prover segurança ao protocolo OLSR. A idéia do protocolo é assinar usando chaves simétricas cada pacote de controle do OLSR, a fim de garantir a autenticidade das mensagens. Considera-se que todos os membros da rede possuem a chave de grupo simétrica e não realizam ações maliciosas.

No SOLSR, todo tráfego é assinado salto a salto, pois existe uma confiança em todos os membros da rede. Ao assinar o pacote de controle, o nó autorizado garante a integridade do conteúdo da mensagem e que a mensagem realmente foi originada por um nó do grupo. Por outro lado, a desvantagem é que a abordagem salto a salto não garante assinaturas fim-a-fim, já que um pacote recebido por um nó não terá sido assinado pelo nó de origem, mas apenas pelo nó anterior. Por essa razão, o protocolo determina que os nós só devem encaminhar pacotes oriundos de nós confiáveis. Conseqüentemente, os nós de uma dada rota são confiáveis, dois a dois. O processo de assinatura digital utiliza uma

função *hash* com chave, de forma que um nó que não tenha acesso à chave secreta não pode reproduzir a assinatura.

Para o SOLSR foram definidos quatro tipos de mensagem, sendo uma para transportar a assinatura e três para realizar a troca de estampas de tempo. A assinatura é anexada a todos os pacotes do SOLSR, enquanto que as mensagens de estampa de tempo são trocadas apenas no primeiro encontro entre dois nós.

As mensagens de estampa de tempo têm como principal objetivo evitar o ataque da replicação de pacotes [Fernandes et al., 2006], através do controle do atraso médio entre os pacotes trocados entre dois nós. Qualquer mensagem recebida que esteja fora do intervalo esperado é considerada como uma replicação do tráfego real por um nó malicioso. Uma das conseqüências desse processo é que os nós passam a conhecer a diferença entre seus relógios, de forma que essa informação pode ser utilizada para outros processos que exigem algum tipo de sincronização.

4. Cenários de Aplicação do Protocolo de Troca de Chaves de Grupo CHARADAS

A utilização de chaves de grupo não é considerada a melhor opção para cenários onde não existe confiança em todos os membros da rede. Nesses casos, as soluções mais simples são o uso de uma chave simétrica por par de nós ou a utilização de chaves assimétricas. A primeira solução dificulta a entrada de novos nós na rede, pois é necessário cadastrar uma chave nova em todos os nós, além do alto gasto de memória com armazenamento. Outro problema é o tratamento das mensagens enviadas em difusão ou inundação, que precisariam ser assinadas para todos os destinos. A segunda solução, que utiliza criptografia assimétrica, tem um alto custo computacional, o que pode ser restritivo para alguns dispositivos. Assim, esse artigo propõe a utilização de uma metodologia híbrida, onde as identidades são identificadas com criptografia assimétrica e a integridade das mensagens é garantida com criptografia simétrica.

O objetivo do protocolo CHARADAS é promover uma troca de chaves periódica, após a união de redes particionadas e sempre que um usuário for expulso pelo administrador ou bloqueado por algum sistema de identificação de intrusão. A troca de chaves permite que o nó que saiu da rede não possa mais assinar novas mensagens. Além disso, também é importante garantir que um nó que possua uma chave antiga não consiga obter a nova chave. O sistema visa também realizar o controle de acesso de usuários não-maliciosos, mas não-autorizados, que obtiveram a chave com algum usuário autorizado de forma lícita ou ilícita. O controle e troca de chaves deve ser feito de forma automática, sem intervenção do administrador, mesmo em caso de bipartições da rede.

Para garantir baixo custo de banda, energia, processamento e memória, o processo de troca deve ser realizado o menor número de vezes possível, sem que isso atinja o nível de segurança que se deseja aplicar à rede.

4.1. Sistema de Autenticação

Redes ad hoc têm como premissa a ausência de infra-estrutura. Assim, a inserção de servidores de autenticação vai contra as características básicas desse tipo de rede. Por essa razão, o sistema proposto supõe a existência de um esquema de autenticação simples,

que dispensa infra-estrutura de servidores. Neste, cada nó deve guardar a chave pública do administrador, a estampa de tempo do momento de autorização de acesso do nó à rede, assinado pelo administrador, um par de chaves próprio, o momento em que entrou na rede e uma lista dos nós cadastrados. Essa lista não implica em um aumento significativo de memória, pois uma característica do OLSR é guardar uma entrada para cada nó da rede em sua tabela de roteamento. Os registros que são adicionados são os nós autorizados que estão ausentes, os nós bloqueados, caso exista um sistema de detecção de intrusão e os nós excluídos. Os registros de nós excluídos devem ser guardados apenas enquanto existirem nós ausentes que não foram notificados da saída do nó, ou nós que estavam ausentes, voltaram à rede, mas ainda não participaram de uma autenticação.

4.2. Sistema de Detecção de Intrusão

O sistema proposto suporta a existência de um sistema de detecção de intrusão (SDI) que detecte ações maliciosas em qualquer camada do modelo TCP/IP, e que pode aplicar punições como a exclusão temporária de um nó da rede. O SDI é importante mesmo nos casos de protocolos de roteamento que utilizam criptografia assimétrica, pois ela é capaz de detectar modificações dos pacotes e permite identificar o nó que realizou cada ação, mas não é capaz de detectar todas as ações maliciosas.

O cenário suposto para uso do SOLSR com o CHARADAS supõe que todos os usuários autorizados, ou seja, que possuem a chave de grupo, são confiáveis. No entanto, pode ocorrer o roubo da chave de grupo ou da chave privada do nó. Quando ocorre o roubo da chave de grupo, o SDI pode identificar ações maliciosas e iniciar um processo de troca, excluindo o nó intruso da rede. No caso de roubo da chave privada, existiriam duas autenticações iguais no processo de troca e o SDI também poderia bloquear o nó autorizado até que ele trocasse de chave com o administrador, impedindo também as ações maliciosas. Dessa forma, a introdução da autenticação para troca de chave de grupo permite excluir nós que roubaram a chave de grupo ou alguma identidade válida na rede.

O uso da chave de grupo para assinar todas as mensagens de controle que transitam na rede não permite ao SDI descobrir qual é o nó que está agindo de forma maliciosa. Ao detectar problemas de roteamento, a única opção é requisitar que se troque a chave, pois é possível que usuários sem autorização tenham obtido a chave e uma identificação válida. Supondo que existam nós internos maliciosos, a única forma de detectar o usuário mal-intencionado seria pela observação das camadas superiores, caso essas utilizem algum tipo de autenticação. Além disso, uma troca freqüente de chaves pode gerar uma notificação ao administrador, indicando que existe algum usuário autorizado agindo de forma incorreta na rede. Caso a única ação maliciosa desse usuário seja repassar a chave de grupo e uma identificação válida, as conseqüências dessa ação podem ser controladas com a troca da chave após a detecção de mau comportamento ou ainda após a troca periódica da chave de grupo. Para evitar os casos em que o usuário não é malicioso, mas teve sua máquina invadida, deve-se utilizar os métodos comuns de segurança, como a utilização de *firewalls* e antivírus.

O papel do administrador, na presença ou não de um sistema de detecção de intrusão (SDI), é apenas de cadastrar e excluir nós da rede, e as demais ações devem transcorrer de forma automática e transparente. No caso do SDI detectar a existência de usuários autorizados maliciosos, ele pode notificar ao administrador, que pode optar por excluir definitivamente ou não o nó malicioso da rede.

Desta forma, o CHARADAS permite a troca automática de chaves devido à exclusão ou bloqueio de um nó da rede, além de evitar a ação de usuários autorizados que não tem a intenção de prejudicar a rede, mas que repassam a chave de grupo para usuários não autorizados. Assim, é possível evitar ações maliciosas de nós que obtém a chave de grupo e utilizam a rede sem autorização.

5. Protocolo CHARADAS

O CHARADAS (**CHA**ve de grupo no **R**oteamento **A**través de **D**istribuição **A**ssimétrica **S**egura) utiliza três processos principais, sendo eles a troca de chave de grupo, a entrada de novos nós e a eleição do líder. Através desses processos, são tratadas as requisições de troca, sejam por periodicidade ou por notificação do administrador ou do sistema de detecção de intrusão.

5.1. Processo de Troca de Chave de Grupo

O processo de troca de chaves do CHARADAS é iniciado pelo nó líder, que deve escolher a nova chave, iniciar o processo de disseminação dos segredos entre os nós autorizados e escolher o novo líder. O novo líder deve ser o nó que minimiza o número de saltos até as bordas, excluindo-se o líder atual. Inicialmente, o nó líder é representado pelo primeiro nó na rede.

A troca de chaves é disparada por um pedido do administrador ou do sistema de detecção de intrusão (SDI), pela expiração da chave ou ainda devido à união de duas partições da rede. A troca devido à expiração da chave é importante para evitar o uso da rede por nós não autorizados. É importante ressaltar que um usuário que repasse a chave de grupo para algum outro usuário que ele considere de confiança não representa uma ação mal intencionada, mas que pode colocar a rede em risco pela inserção de nós não autorizados. A troca periódica tem a motivação de eliminar esses usuários da rede.

Devido ao processo de troca de estampas de tempo do protocolo SOLSR, os nós conhecem a diferença aproximada entre os relógios de cada nó da rede. Assim, o nó líder deve anunciar quando o processo de troca se iniciou para ele, e cada nó que transmitir a informação deve trocar esse dado para a sua estampa de tempo correspondente, permitindo que todos os nós da rede saibam o momento aproximado do início do processo de troca e possam calcular o momento da próxima troca de chaves na rede. O momento de troca é atualizado sempre que existir um pedido de troca assíncrono por parte do administrador ou do SDI.

A transmissão da chave é feita utilizando os *Multipoint Relays* (MPRs). O nó líder inicia a troca, anunciando que possui a nova chave. Os seus vizinhos respondem e recebem a chave do líder. Em seguida, os vizinhos que são MPR do líder devem retransmitir o anúncio de chave, e os vizinhos por dois saltos devem escolher um MPR entre os MPRs escutados para realizar o processo de troca. Assim, os MPRs não precisam realizar a troca com todos os vizinhos, o que é importante para poupar energia do nó. Esse processo de transmissão pelos MPRs continua até que todos os nós da rede tenham recebido a chave de grupo.

O processo de troca consiste de três mensagens trocadas por cada par de nós formado durante o processo. Primeiramente, é enviada a mensagem de anúncio, que deve conter a identificação do nó de origem, o número de seqüência da chave nova, a estampa

de tempo do líder no início do processo e o novo líder. Todos esses campos devem ser assinados com a chave pública do nó que está enviando o anúncio. O certificado do nó, assinado pelo administrador, também deve ser enviado. A assinatura assimétrica dessa mensagem ao invés da assinatura simétrica é importante para evitar ataques de negação de serviço por possíveis nós maliciosos que entrem na rede. Estes nós poderiam iniciar consecutivos processos de troca, se passando pelo líder, apenas para consumir recursos da rede.

Como resposta à mensagem de anúncio, deve ser enviada uma mensagem em *unicast* contendo a identificação do nó de origem da resposta, a identificação do MPR escolhido, o número de seqüência da chave nova, que permite a identificação do processo, e assinatura assimétrica do nó, junto com seu certificado. Essa assinatura também é importante para evitar que nós maliciosos façam pedidos falsos com a finalidade de sobrecarregar os MPRs não escolhidos ou de realizar um ataque do direcionamento falso [Fernandes et al., 2006] contra os nós cuja identidade foi falsificada. A terceira mensagem é enviada pelo MPR escolhido também em *unicast*, como resposta para o nó que o escolheu, e contém a nova chave criptografada com a chave pública do nó que o escolheu. Essa mensagem contém ainda a identificação do MPR, o número de seqüência da nova chave, e uma assinatura. Cabe observar que essa mensagem com a chave só é enviada se o nó de destino estiver na lista dos nós válidos.

Com esse processo de troca se garante que mesmo que um nó malicioso obtenha a chave de grupo anterior, ele não conseguirá obter a nova chave, pois ela foi assinada com a chave pública do nó de destino. Além disso, se um nó obteve de forma ilícita a chave de grupo e a utilizava sem autorização, ao se realizar o processo ele não obteria a nova chave, pois não conseguiria se autenticar. Caso o nó sem autorização também possua uma cópia da chave privada de um nó autorizado, essa ação também poderia ser identificada, pois o mesmo nó se autenticaria duas vezes, de forma que o SDI, caso ele exista, identificaria o problema e bloquearia o nó.

O uso da nova chave também deve ocorrer de forma sincronizada. Para isso, cada nó deve consultar na sua tabela de topologia o número máximo de saltos na rede a partir do nó líder até as extremidades da rede e calcular o tempo dado pela Equação 1. Nesta equação, $T_{passagem}$ representa o tempo médio de transmissão de um MPR para todos os vizinhos que o selecionaram, δ representa uma variação tolerada nesse tempo, devido a perdas e atrasos e $NumMPR_{max}$ representa o número de MPRs do líder até o nó mais distante dele na rede. Os nós devem iniciar o uso da nova chave após T_{espera}, embora devam aceitar como válidas as mensagens assinadas com a chave nova ou a velha no período compreendido entre $T_{espera} - \alpha$ e $T_{espera} + \alpha$. Após $T_{espera} + \alpha$, as mensagens que não forem assinadas com a nova chave devem ser descartadas. Os nós que, por alguma razão, não conseguirem obter a chave dentro do período esperado devem ser tratados como novos nós, o que é descrito na Seção 5.2.

$$T_{espera} = T_{passagem} * NumMPR_{max} + \delta \quad (1)$$

5.2. Entrada de Novos Nós

Os objetivos do mecanismo para aceitar novos nós são dar maior tolerância a atrasos no processo de troca, a perdas de enlace e ainda a períodos de ausência do nó. Assim,

qualquer nó que não possui a chave de grupo pode obtê-la com qualquer nó da rede, desde que possua o seu par de chaves, o seu certificado, e que esteja presente na lista de nós válidos.

Para aceitar um nó novo, é necessário observar uma seqüência de regras. Se o novo nó possui certificado e está na lista dos nós autorizados ativos ou ausentes, ele pode iniciar o processo de obtenção de chaves. Caso contrário, deve-se analisar a possibilidade de o nó ter sido adicionado à rede em um momento em que ela estava bipartida, de forma que apenas uma parte da rede teve acesso à notificação do administrador e adicionou o nó à lista de válidos. Neste caso, o novo nó deve informar a identidade do nó que lhe passou a chave de grupo da partição, o qual deve estar na lista de ausentes do nó que foi abordado. Além disso, o certificado do novo nó deve possuir uma estampa de tempo de autorização pelo administrador posterior ao momento que o nó indicado se ausentou, o que comprovaria a existência da partição da rede. Caso algum desses requisitos não seja alcançado, o novo nó não receberá a chave de grupo atual.

O processo de entrada de nó é iniciado sempre que um nó escutar um HELLO de algum nó válido assinado com chave diferente da que possui, fora do intervalo da troca de chaves. O nó que iniciar o processo deve enviar um pedido de entrada, com um *nonce* (*Number used ONCE*), para evitar ataques da replicação, o ID do nó autorizado cujo HELLO foi escutado, o ID do nó que lhe repassou a chave de grupo, a assinatura desses campos e um certificado, para provar que também tem autorização de uso da rede. O nó que recebe esse pedido, verifica a sua lista de nós válidos e se o nó estiver presente, responde com uma mensagem com o *nonce* do novo nó, um *nonce* próprio, a chave de grupo atual, criptografada com a chave pública do nó novo, o momento da próxima troca de estampa, a assinatura de todos esses campos e o certificado, para provar que também possui autorização para utilizar a rede. Além disso, também é enviada uma lista de parâmetros da rede, que contém as atualizações realizadas enquanto o nó esteve ausente, o que inclui as notificações de nós novos autorizados, nós ausentes, nós bloqueados e nós excluídos, todos com suas respectivas estampas de tempo do momento da ação sob o referencial do nó que está repassando as informações. O novo nó deve responder com o *nonce* do nó que o está recebendo na rede, os parâmetros da rede, caso esteja em uma partição e não sozinho, a chave que está utilizando no momento, criptografada com a chave pública do nó de destino, e uma assinatura utilizando criptografia simétrica com a nova chave de grupo, provando que ele é quem diz ser. Para finalizar o processo, ambos os nós devem repassar por inundação os novos parâmetros para o resto da rede, indicando apenas as diferenças válidas. Caso um dos nós esteja sozinho, esse processo de inundação não é necessário, pois os seus HELLOS passarão a ser válidos e ele será retirado da lista de ausentes.

Caso o nó que iniciou o pedido de troca não pertença à lista de nós autorizados do nó abordado, um segundo processo deve ser iniciado. Se o nó indicado como o responsável pela passagem da chave para esse nó também não possuir autorização para a rede, a chave não será trocada com o novo nó. Se pertencer, o processo deve ser realizado entre o nó abordado e o nó indicado, por intermédio do nó que iniciou o processo.

Cabe ressaltar que, ao iniciar o processo de entrada, nenhum dos dois nós deve responder a nenhum outro pedido de entrada de novo nó, até que o primeiro processo se finalize. Isso se justifica devido à possibilidade do novo pedido de entrada partir de um nó que será adicionado à rede após o término do primeiro processo. Além disso, para

evitar ataques de negação de serviço, que poderiam ser realizados por nós maliciosos que repetissem o pedido de entrada inúmeras vezes, cada nó possui um temporizador para respostas de pedido de entrada de novos nós.

Após a troca de chaves entre os dois nós, é necessário que as duas partições da rede possuam a mesma chave de grupo. Para isso, o nó que possuir a menor partição deve se anunciar como líder imediato e iniciar um processo de troca de chaves. Uma vez que esse pedido é assinado com a chave da menor partição, ele não será considerado válido por nenhum nó da maior partição.

5.3. Eleição do Líder

O líder inicia o processo de troca de chaves e deve ser trocado a cada rodada. O critério de escolha visa à seleção de nós centrais, de forma a reduzir os atrasos com a transmissão da chave. O próximo líder deve ser escolhido pelo líder atual e deve ser anunciado para a rede durante a troca de chaves.

Dado que no ambiente de redes ad hoc é possível ocorrer partições e os nós podem ficar ausentes, é possível que o líder escolhido não esteja disponível no momento da troca de chaves. Por essa razão, cada nó deve calcular o tempo de espera pela nova chave. Esse tempo deve considerar atrasos de transmissão e está representado na Equação 2. Nesta equação, N_{saltos} representa o número de saltos do líder até o nó que está esperando a chave e δ representa tolerância ao atraso. A variável $T_{passagem}$ representa o atraso médio devido à transmissão da chave de um MPR para todos os seus vizinhos. Se após T_{chave} a nova chave não tiver chegado, o líder é considerado como ausente. Assim, o nó de maior endereço IP deve iniciar o processo de troca de chaves como o novo líder. Um novo tempo T_{chave} é calculado para o novo líder, levando em consideração o atraso até que esse nó também descubra que o líder está ausente. Da mesma forma, o tempo para utilização da chave nova é reinicializado para o novo líder. Essa eleição automática pode se repetir, caso o novo líder eleito também não inicie o processo. O processo de eleição só terminará quando todos os nós obtiverem a chave.

$$T_{chave} = T_{passagem} * N_{saltos} + \delta \tag{2}$$

Caso se obtenha diversas chaves com atrasos inferiores a T_{espera}, embora superiores ao T_{chave}, o nó deve aceitar a chave do líder mais antigo e deve atualizar o seu $T_{passagem}$. Nessa situação, a chave dos líderes mais novos não deve ser retransmitida.

5.3.1. Tratamento para bipartições

Bipartições podem ocorrer por mobilidade ou por períodos de ausência. A eleição do líder acontecerá de forma automática nessas bipartições, devido à característica do processo de eleição do líder de selecionar automaticamente um novo líder até que o processo se inicie.

Um caso especial pode ocorrer após a junção de duas partições, como foi descrito na Seção 5.1. Nesse caso, a chave deve ser trocada imediatamente após a união de duas partições, pela partição de menor número de nós. Para tanto, o nó da menor partição que obteve a chave da partição maior deve assinar e inundar a rede com a segunda mensagem

do processo de aceitação de novos nós. O envio dessa mensagem como anúncio de novo líder e nova chave é necessária pois ela é assinada por um nó da outra partição, provando que a troca realmente é necessária. Essa mensagem é interpretada pelos outros nós da mesma forma que a mensagem de anúncio do processo de troca de chaves.

6. Análise Matemática

Para análise de desempenho do protocolo, foi utilizada a ferramenta Matlab 6.5. O objetivo da análise é comparar o custo em termos de energia gasta por nó do protocolo SOLSR utilizando criptografia assimétrica, simétrica e simétrica com o CHARADAS. Para tanto, realizou-se análises de gasto de energia no pior caso, o que significa que o desempenho dos protocolos é superior ao observado nos gráficos em situações normais.

Os gastos de energia com criptografia e transmissão considerados são relativos a equipamentos portáteis de pequeno porte [Potlapally et al., 2003, Karri e Mishra, 2002] e estão representados na Tabela 1. Como algoritmo para realizar a assinatura digital e criptografia da chave de grupo, utilizou-se o RSA com uma chave de 1024 bits. Para realizar a assinatura simétrica, utilizou-se o HMAC (*keyed-Hash Message Authentication Code*) com chave de 128 bits.

Tabela 1. Custos considerados na análise matemática.

Ação	**Custo Energético**
Assinatura com HMAC-128	$0.145 * 10^{-6}$ J/b
Verificação de assinatura com HMAC-128	$0.145 * 10^{-6}$ J/b
Transmissão	$0.6582 * 10^{-6}$ J/b
Escuta	$0.28335 * 10^{-6}$ J/b
Assinatura com RSA-1024	0.816 J
Verificação de assinatura com RSA-1024	0.816 J
Criptografia com RSA-1024	0.0192 J

Dado que os custos apresentados são função do tamanho do pacote, foi necessário o cálculo do tamanho de cada pacote do SOLSR e do CHARADAS. Os parâmetros de rede utilizados para a esse cálculo foram escolhidos de forma a gerar o pior caso para o nó analisado, de forma a obter o maior gasto de energia possível. A análise foi realizada para uma rede com mil nós, em um período de uma semana. As taxas de envio de pacotes de controle do SOLSR estão na Tabela 2.

Tabela 2. Taxas do OLSR.

Mensagem	**Taxa de Emissão (pacotes/s)**
HELLO	0.5
MID	0.2
TC	0.2

Primeiramente, analisaram-se as influências da criptografia simétrica com HMAC-128 e assimétrica com RSA-1024 e do protocolo CHARADAS. Na Figura 2 está representado o período de uma semana utilizando as três possibilidades. O que se observa é que o protocolo SOLSR utilizando criptografia assimétrica teve um gasto de

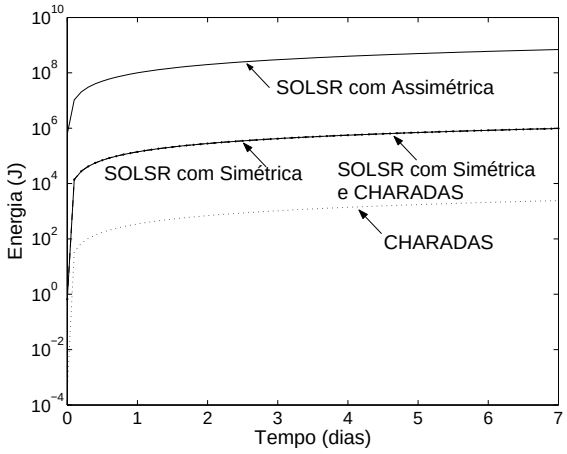


Figura 2. Comparação do SOLSR com criptografia assimétrica, simétrica e simétrica com sistema de distribuição de chaves após uma semana de uso.

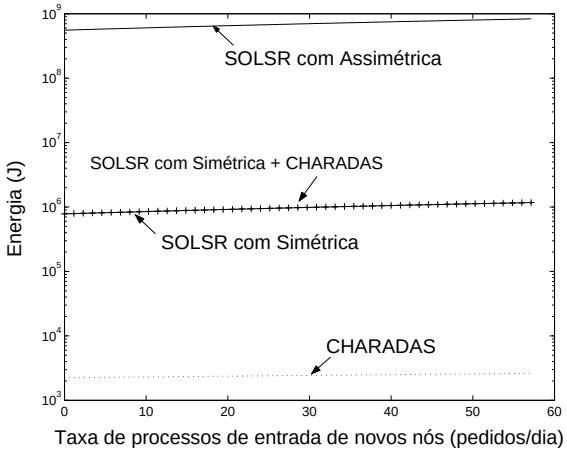
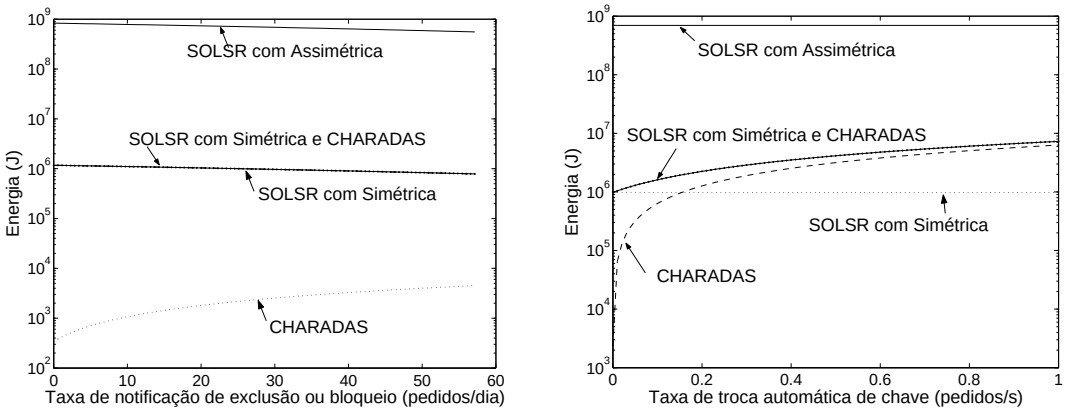


Figura 3. Gasto energético com o aumento da taxa de processos de entrada de nó, considerando que o nó analisado está sempre na menor partição.

energia muito superior, enquanto que a utilização do protocolo de distribuição de chaves não representou um alto gasto de energia, embora aumente a segurança e a simplicidade oferecida ao se utilizar o SOLSR com chave de grupo. Por esta figura também nota-se que o gasto de energia do CHARADAS é muito inferior ao SOLSR utilizando criptografia simétrica, o que se justifica principalmente pelo fato de o protocolo ser utilizado poucas vezes, quando comparado à freqüência de emissão de mensagens de controle do SOLSR.

A entrada de novos nós influencia diretamente no desempenho do protocolo, pois pode gerar novos processos de troca de chave por diversos nós, além de aumentar o número de nós na rede. Para avaliar o impacto dessa situação, variou-se, para um período de uma semana, a taxa de processos de entrada de novos nós, nos quais o nó analisado sempre é parte do processo e está na menor partição. Este resultado, que está representado na Figura 3, mostra que o custo do sistema cresce lentamente e continua muito inferior ao custo do sistema com criptografia assimétrica. Nesta análise considerou-se a taxa de notificação de exclusão e bloqueio igual a 200 pedidos/semana.

Outra análise realizada foi a do impacto do aumento da taxa de troca automática



(a) Variação da taxa de notificações de exclusão ou bloqueio.

(b) Variação a taxa de troca de chaves.

Figura 4. Gasto de energia ao se variar as taxas de notificações de exclusão ou bloqueio e de troca da chaves.

da chave e do aumento do número de notificações do administrador para exclusão ou do sistema de detecção de intrusão (SDI) para bloqueio de algum nó. Esses parâmetros regem a inicialização dos processos de troca de chave na rede, o que gera gastos, em especial com criptografia assimétrica. A Figura 4(a) apresenta o efeito do aumento da taxa de notificações do SDI e do administrador com relação ao custo em termos de energia dos protocolos, para um período de uma semana. Supõe-se que cada notificação leva a uma exclusão e que a taxa de entrada de nós se manteve em 200 nós/semana. Novamente, o CHARADAS com o SOLSR não apresentou um gasto muito alto, quando comparado ao SOLSR com criptografia assimétrica. O aumento da taxa de troca automática da chave tem um comportamento representado na Figura 4(b). Para essa curva, foi suposto que ambas as taxas de notificação e de entrada de nós eram de 200 nós/semana.

7. Conclusões

Neste artigo foi apresentado o protocolo de distribuição de chaves de grupo CHARADAS (**CHA**ve de grupo no **R**oteamento **A**través de **D**istribuição **A**ssimétrica **S**egura) para o SOLSR, que tem como objetivo trocar de chaves de grupo automaticamente após períodos pré-determinados ou ainda após a exclusão ou bloqueio de algum nó. A utilização de chaves de grupo pode representar uma grande vulnerabilidade em ambientes nos quais não existe confiança absoluta que os membros da rede não repassam a chave para outros usuários não-autorizados. O uso do CHARADAS impede a entrada de usuários não autorizados com a renovação periódica da chave utilizando criptografia assimétrica. Assim, a sua utilização diminui as vulnerabilidades geradas pelo uso de chaves de grupo no roteamento, sem que isso acarrete em um aumento significativo dos gastos energéticos com o protocolo. A desvantagem do uso do CHARADAS é que ele aumenta a memória necessária em cada nó, mas dadas as características de estado de enlace do SOLSR, a quantidade de dados armazenados extra não chega a ser significativa.

A análise matemática do pior caso do protocolo CHARADAS mostrou que ele não gera um grande gasto de energia ao viabilizar a utilização de criptografia simétrica

para dar segurança ao roteamento. Sua utilização se mostra interessante, em especial, em cenários onde equipamentos com pouca inteligência ou com restrições de bateria são utilizados, pois nessas situações, o uso de criptografia assimétrica pode ser impraticável. Sua capacidade de lidar com partições da rede permite que ele seja usado em cenários com mobilidade e com números de nós e conectividade variáveis. Desta forma, ele se aplica corretamente para redes ad hoc de pequeno e médio porte, desde que o SOLSR represente uma boa solução para essa rede.

Referências

Bouassida, M. S., Chrisment, I. e Festor, O. (2006). Efficient group key management protocol in manets using the multipoint relaying technique. Em *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies - ICN/ICONS/MCL 2006*, volume 4, páginas 64 – 71.

Chiang, T. e Huang, Y. (2003). Group keys and the multicast security in ad hoc networks. Em *2003 International Conference on Parallel Processing Workshops - ICPP 2003 Workshops*, páginas 385–390.

Fernandes, N. C., Moreira, M. D. D., Velloso, P. B., Costa, L. H. M. K. e Duarte, O. C. M. B. (2006). Ataques e mecanismos de segurança em redes ad hoc. *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, páginas 49–102.

Hafslund, A., Tønnesen, A., Rotvik, R. B., Andersson, J. e Øivind Kure (2004). Secure extension to the OLSR protocol. Em *OLSR Interop and Workshop*, páginas 1–4, San Diego, California.

Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A. e Viennot, L. (2001). Optimized link state routing protocol for ad hoc networks. Em *5th IEEE Multi Topic Conference (INMIC 2001)*, páginas 62–68.

Karri, R. e Mishra, P. (2002). Minimizing energy consumption of secure wireless session with qos constraints. Em *IEEE International Conference on Communications - ICC 2002*, volume 4, páginas 2053 – 2057.

Liao, L. (2005). Group key agreement for ad hoc networks. Master's thesis, Ruhr-University Bochum.

Potlapally, N. R., Ravi, S., Raghunathan, A. e Jha, N. K. (2003). Analyzing the energy consumption of security protocols. Em *International Symposium on Low Power Electronics and Design - ISLPED '03*, páginas 30–35.

Sanzgiri, K., Dahill, B., Levine, B. N. e Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. Em *10th IEEE International Conference on Network Protocols*, páginas 78–87.

Tønnesen, A. (2004). Implementing and extending the optimized link state routing protocol. Master's thesis, University of Oslo.

Zapata, M. G. (2002). Secure ad hoc on-demand distance vector (SAODV) routing. *ACM Mobile Computing and Communications Review*, 6(3):106–107.