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

Natalia Castro Fernandes, Otto Carlos Muniz Bandeira Duarte *

***Resumo*— Este artigo propõe e especifica o protocolo híbrido CHARADAS de troca de chave criptográfica de grupo, eficiente para altas taxas de renovação de chaves, partições na rede e admissão/exclusão de nós. O CHARADAS é projetado para utilização com o *Secure Optimized Link State Routing Protocol* (SOLSR) e faz uso de criptografia assimétrica na troca de chaves para a identificação dos nós do grupo. As análises formal de protocolo e de desempenho energético são feitas utilizando as ferramenta ARP e Matlab, respectivamente. Os resultados mostram que o CHARADAS torna o roteamento ad hoc através do SOLSR mais robusto com um pequeno acréscimo de consumo de energia.**

***Palavras-Chave*— Segurança, Redes Ad Hoc, Distribuição de Chaves**

***Abstract*— This paper proposes and specifies a hybrid group cryptographic key distribution protocol called CHARADAS. It is efficient with high rates of key renewal, network partitions and new nodes entering or leaving the network. CHARADAS was designed to work with the Secure Optimized Link State Routing Protocol (SOLSR) and uses asymmetric cryptography to identify group nodes in the key exchange process. The tools Matlab and ARP were used for an energetic performance and formal analysis, respectively. The results showed that CHARADAS make the ad hoc routing more robust by SOLSR with a small addition in the energy consumption.**

***Keywords*— Security, Ad Hoc Networks, Key Distribution**

I. INTRODUÇÃO

As redes ad hoc móveis de múltiplos saltos possuem muitas vulnerabilidades devido ao roteamento colaborativo. Nestas redes, o comportamento malicioso de um único nó pode impedir o funcionamento de toda a rede. Por essa razão, protocolos foram propostos com a intenção de adicionar segurança ao roteamento. Um ponto em comum destes protocolos é a utilização de assinaturas para garantir a autenticidade e a integridade das mensagens de roteamento, impedindo que nós maliciosos não-autorizados criem mensagens com endereços de origem forjados ou modifiquem o conteúdo transmitido.

O uso de chaves criptográficas simétricas é normalmente empregado por cada par de nós comunicantes e, assim, para proteger o roteamento em uma rede ad hoc, seriam necessárias $n(n-1)$ chaves na rede, o que tornaria o gerenciamento de chaves muito complexo, além de dificultar o procedimento de inundação. O uso de chaves criptográficas assimétricas requer n chaves privadas e n chaves públicas. Além do menor número de chaves, a criptografia assimétrica permite a verificação de assinaturas fim-a-fim, eliminando a necessidade de confiar em todos os nós intermediários da rota, o que torna o roteamento mais robusto. Protocolos como o *Secure Ad hoc On-Demand Distance Vector Protocol* (SAODV) [Zapata, 2002] se servem de chaves assimétricas. A principal desvantagem desta abordagem é o grande consumo de energia requerido pela criptografia assimétrica, que dificulta sua utilização em ambientes de restrição de energia. Além disso, o seu uso exige que uma autoridade certificadora esteja sempre disponível para todos os usuários, o que pode não ser possível em redes ad hoc móveis. Uma alternativa mais simples de se gerenciar e econômica em consumo de energia é o uso de uma única chave simétrica para todos os nós da rede, denominada chave de grupo. O *Secure Optimized Link State Routing Protocol* (SOLSR) [Hafslund et al., 2004] é um exemplo de protocolo que se serve desta técnica. A desvantagem da utilização de chaves simétricas de grupo é que, uma vez a chave sendo revelada, toda a rede fica comprometida e não é possível identificar o nó malicioso.

Uma particularidade dos mecanismos criptográficos é de se basearem na manutenção do segredo da chave secreta, para o mecanismo de chave simétrica, e da chave privada, para o mecanismo de chaves assimétricas. A quebra do segredo, seja pela violação do dispositivo sem fio móvel, que normalmente é mais vulnerável que um dispositivo cabeado fixo, ou até pela simples 'revelação voluntária' da chave de um nó para outro, implica a quebra da segurança das mensagens de roteamento e a vulnerabilidade de toda a rede. Além disso, uma estação autorizada, que possui licitamente a chave criptográfica, pode também ter atitudes maliciosas ou não cooperativas. No caso da chave de grupo simétrica, este fato é ainda mais grave, pois o nó malicioso ou mal comportado é de difícil detecção. Por exemplo, em uma rede ad hoc comunitária é possível, e até provável, que um usuário passe a chave de grupo simétrica para um vizinho, ou um conhecido, que more na comunidade uma vez que não é possível saber qual o usuário legítimo passou a chave.

Outro ponto importante característico das redes ad hoc são problemas de conectividade. É comum o particionamento da rede e até o isolamento de alguns nós, seja pela mobilidade ou também pela variação das características de propagação do sinal.

Para atender à particularidade de ambientes onde podem ocorrer freqüentes violações da chave e partições na rede ad hoc, este artigo propõe o protocolo de distribuição de chaves de grupo CHARADAS (**CHA**ve de grupo no **R**oteamento

* Apoiado pelos recursos da CAPES, CNPq, FAPERJ, FINEP, FUJB, RNP e FUNTTEL.

Através de **D**istribuição **A**ssimétrica **S**egura) para o SOLSR. Para impedir que usuários não-autorizados acessem os recursos da rede, é proposto um mecanismo de troca periódica da chave de grupo baseado em criptografia assimétrica. Devido às características de baixa conectividade das redes ad hoc, o protocolo possui um mecanismo de união de partições e admissão de nós ausentes. Além disso, dado que nós com restrições de energia podem ser desligados a qualquer momento, existe um mecanismo que dá maior robustez ao protocolo elegendo automaticamente o nó que deve escolher a nova chave.

A análise do protocolo CHARADAS foi feita com a ferramenta ARP (Analisador de Redes de Petri), para garantir que o protocolo é exeqüível e possui as características de funcionamento desejadas. Também foi avaliado, através do Matlab, o impacto energético do CHARADAS baseado em uma estimativa do número de mensagens de controle trocadas.

II. Trabalhos Relacionados

Os protocolos de gerenciamento de chave simétrica de grupo podem ser classificados em: pré-distribuição de chaves, disseminação por entidade centralizada e estabelecimento contributivo de chaves, onde cada nó da rede contribui para a geração da chave. A utilização da contribuição de todos os nós para a criação da chave de grupo tem como principal desvantagem uma alta sobrecarga com mensagens de controle. Já as propostas com pré-distribuição de chave têm como ponto negativo a necessidade de existir uma entidade que faça a distribuição prévia das chaves e conheça o número total de nós. Além disso, a pré-distribuição de chaves pode aumentar o tamanho das rotas na rede e indicar como desconexos nós que possuem uma rota. Luo *et al.* propuseram um sistema de troca baseado em pré-distribuição e em contribuição de todos os nós para a criação das novas chaves de grupo [Luo et al., 2006]. Nesse protocolo, deve ser guardada uma lista com todos os nós excluídos e as chaves que o nó excluído possuía devem ser descartadas.

Puzar *et al.* propuseram o protocolo SKiMPy, para distribuição de chaves em redes ad hoc estabelecidas em casos de emergência [Puzar et al., 2005]. Os autores supõem a existência de um sistema de autenticação com certificados sem validade, assinados por alguma autoridade responsável pela operação de emergência. No SKiMPy, a troca periódica é feita através de operações de *hash* nas chaves antigas. Para impedir que os nós excluídos participem, existe uma lista negra e todas as mensagens geradas por esses nós devem ser descartadas. No entanto, a verificação da origem das mensagens no sistema proposto exige a utilização de criptografia assimétrica.

Li *et al.* propõem o *Distributed, Efficient Clustering Approach* (DECA), um modelo de clusterização eficiente para a distribuição de chaves em redes ad hoc [Li et al., 2006]. Neste trabalho é mostrado que a proposta pode ser combinada com a técnica *Multipoint Relay* (MPR) de acordo com a localização dos usuários do grupo e da mobilidade. A desvantagem deste protocolo é o alto consumo de energia devido à emissão periódica muito freqüente de mensagens de controle.

O CHARADAS, proposto neste artigo, também utiliza certificados sem validade e baseia o seu mecanismo de distribuição da chave de grupo nos MPRs. A sua vantagem é ter um baixo gasto de energia por enviar poucas mensagens de controle para a troca de chaves. O CHARADAS não necessita da emissão de mensagens de controle freqüentes, como o DECA, e não precisa que todos os nós troquem informações para a formação da chave, o que evita muitos gastos com transmissão e operações criptográficas. O CHARADAS também não precisa de informações prévias sobre a rede, como nos protocolos de pré-distribuição de chaves, o que poderia restringir os cenários de utilização do protocolo. Além disso, o CHARADAS realiza o controle de acesso apenas pela lista de nós autorizados, o que evita uma sobrecarga de dados de nós excluídos, após longo tempo de funcionamento da rede. O CHARADAS também prevê procedimentos de união de partições da rede devido às freqüentes perdas de conectividade das redes ad hoc, o que não é solucionado por todos os protocolos de gerenciamento de chaves.

III. Os Protocolos OLSR e SOLSR

O *Optimized Link State Routing protocol* (OLSR) é um protocolo de roteamento para redes ad hoc pró-ativo, ou seja, que calcula, em avanço, as rotas para todos os destinos, baseado na técnica de estados de enlace. Portanto, 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, para coleta dos dados de estado de enlace, ou inundação, para disseminar esses dados pela rede. Para reduzir o número de mensagens de controle nas constantes inundações, o OLSR possui um mecanismo de controle de inundação chamado de *Multipoint Relay* (MPR). Neste mecanismo, apenas os nós escolhidos como MPRs, ao invés de todos os nós da rede, reencaminham as mensagens. Os MPRs são nós selecionados por cada nó da rede dentre o conjunto de nós vizinhos de um salto de forma a atingir todos os vizinhos por dois saltos.

Para prover segurança ao protocolo OLSR, foi proposto o *Secure OLSR* (SOLSR). No SOLSR, todas as mensagens são assinadas salto-a-salto com a chave simétrica de grupo. Ao assinar a mensagem de controle, o nó autorizado garante a integridade do conteúdo da mensagem e que a mensagem foi originada por um nó do grupo. O processo de assinatura utiliza uma função *hash* com chave, de forma que um nó que não possua a chave secreta não possa reproduzir a assinatura.

Para o SOLSR foram definidos mais quatro novas mensagens de controle, sendo uma para transportar a assinatura e três para realizar a troca de estampas de tempo. A assinatura é anexada a todas as mensagens de controle do SOLSR, enquanto que as mensagens de estampa de tempo, que são trocadas apenas no primeiro encontro entre dois nós, tem como objetivo determinar o atraso médio de entrega de mensagens entre os dois nós. É importante conhecer esse atraso para evitar a replicação de mensagens [Fernandes et al., 2006] por nós maliciosos em outros pontos da rede. Ao receber uma mensagem de controle, o nó verifica se o atraso de entrega está dentro de um limite esperado. Se a mensagem de controle for uma replicação de um nó malicioso, o atraso será superior ao esperado e o ataque será identificado. Uma das conseqüências

do processo de troca de estampa de tempo é o conhecimento da diferença entre os relógios dos nós.

O SOLSR não implementa e deixa a cargo do usuário a distribuição e gerência de chaves e, portanto, é necessário um sistema de distribuição e gerenciamento da chave de grupo simétrica, o que é o foco deste artigo.

IV. O PROTOCOLO CHARADAS

O CHARADAS é um protocolo de gerenciamento e distribuição de chaves apropriado para um ambiente onde a chave de grupo pode ser obtida por nós não autorizados seja por violação ou pela 'revelação voluntária' de um nó autorizado a um nó não autorizado. É importante ressaltar que qualquer nó autorizado pode passar a chave de grupo simétrica para um nó não autorizado sem que sua identidade seja revelada. Para dificultar o acesso de nós não-autorizados, a chave de grupo é periodicamente modificada. Além da mudança periódica da chave de grupo simétrica, o CHARADAS permite a entrada e a exclusão segura de nós no grupo. O procedimento de entrada/exclusão de um nó no grupo se faz através de criptografia assimétrica para uma maior segurança. A exclusão de um nó requer a passagem de uma nova chave de grupo simétrica para todos os nós da rede. A entrada de um nó na rede requer apenas a passagem da chave de grupo para este nó solicitante, pois no roteamento as informações de controle não são sigilosas. Por fim, o CHARADAS possui um processo particular para distribuição e gerenciamento da chave de grupo simétrica na ocorrência de partições da rede ad hoc. A troca da chave de grupo é iniciada por um 'nó líder' que é substituído a cada troca de chave para distribuir a sobrecarga.

O protocolo CHARADAS requer uma entidade que determine quais usuários podem acessar a rede. Essa entidade funciona como um administrador que registra usuários e pode ser implementada de forma centralizada ou distribuída. A função desta entidade é similar à autoridade administrativa de certificados digitais utilizada na criptografia assimétrica. A maioria das propostas de gerenciamento de chaves assume esta mesma entidade administrativa ou algo com função similar. Para um nó receber a nova chave e poder utilizar a rede, ele deve possuir um certificado contendo a sua chave pública e a sua identificação, assinadas com a chave privada da entidade administrativa. Um nó só pode receber a chave de grupo simétrica se ele estiver na lista de nós autorizados, possuir o certificado e for capaz de assinar mensagens com sua chave privada. Quando o nó é excluído, ele é retirado da lista dos nós autorizados, de forma que, mesmo possuindo o certificado, ele não pode receber a nova chave. É importante também ressaltar que o CHARADAS se torna mais robusto quando usado associado a um sistema de detecção de intrusão (SDI), que detecta os nós mal comportados.

O CHARADAS possui três procedimentos principais, que são a troca automática da chave,a substituição automática do líder e a entrada de nós que estão sós ou em partições.

A. Processo de Troca de Chave de Grupo

O processo de troca de chaves do CHARADAS é iniciado pelo nó líder, nas situações de notificação de exclusão de usuário, de detecção de ação maliciosa por um sistema de detecção de intrusão (SDI), de expiração do tempo de uso da chave simétrica ou ainda de união de duas partições da rede.

A transmissão da chave é iniciada pelo nó líder, através do *broadcast* da mensagem Anúncio, que indica a existência de uma nova chave. Os vizinhos do líder, ao escutarem o Anúncio, enviam a mensagem Pedido indicando que desejam receber a chave. O líder finaliza o processo com seus vizinhos enviando a mensagem Resposta, que contém a nova chave de grupo criptografada com a chave pública do nó vizinho. Em seguida, os vizinhos que são *Multipoint Relays* (MPRs) do líder devem retransmitir o Anúncio, e os vizinhos por dois saltos devem escolher um MPR para realizar o processo de troca.

A assinatura nas mensagens, em conjunto com o certificado, é importante para provar a identidade do nó que está enviando a mensagem e para garantir a integridade do conteúdo. Cabe observar que sem a assinatura e o certificado no Anúncio e no Pedido, o processo de troca não poderia ser realizado, pois é preciso provar que ambos os nós estão na lista de autorizados e são quem dizem ser.

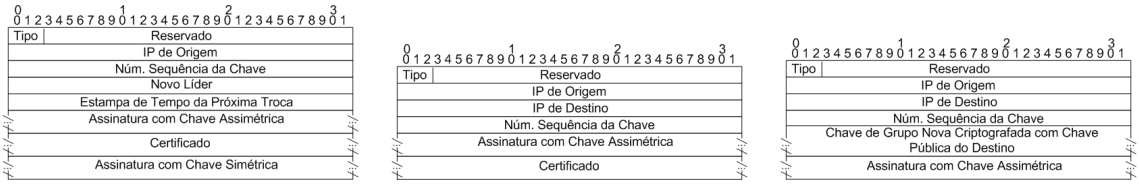
Com esse processo de troca se garante que mesmo que um nó malicioso possua a chave de grupo anterior, ele não conseguirá obter a nova chave, pois a nova chave é assinada com a chave pública do nó de destino e o nó não autorizado não consegue se autenticar.No caso da existência de um sistema de detecção de intrusão, se o nó malicioso também possuísse a chave privada de algum nó autorizado, aconteceriam duas trocas com o mesmo par de chaves assimétricas. Assim, o roubo da chave privada seria detectado e tanto o nó malicioso quanto o nó autorizado seriam bloqueados. Um novo processo de troca seria iniciado, e o nós bloqueados não receberiam a nova chave. Dessa forma, o processo de troca de chaves proposto dá maior segurança ao roteamento com chave simétrica de grupo, sem aumentar muito a quantidade de energia gasta.

O uso da nova chave 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 da chave de um MPR para todos os vizinhos que o selecionaram e $NumSaltos_{max}$ representa o número de saltos entre o líder e o nó mais distante dele na rede. Os nós devem iniciar o uso da nova chave após T_{espera}, embora devam classificar como válidas as mensagens assinadas com a chave nova ou antiga no período entre $T_{espera} - \alpha$ e $T_{espera} + \alpha$, onde α é uma constante que representa a tolerância ao atraso. 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 nova dentro do período esperado devem ser tratados como novos nós, o que é descrito na Seção IV-B.

$$T_{espera} = T_{passagem} * NumSaltos_{max} \quad (1)$$

B. Processo de Entrada de Novos Nós e União de Partições

O mecanismo de entrada de novos nós permite que nós autorizados que não possuam a chave de grupo a obtenham,



(a) Mensagem Anúncio. (b) Mensagem Pedido. (c) Mensagem Resposta.

Fig. 1. Mensagens para a troca de chave de grupo.

além de permitir a união de partições, formadas por problemas de conexão na rede. Assim, os objetivos desse mecanismo 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 outro nó, desde que possua o seu par de chaves assimétricas, o seu certificado, e que esteja presente na lista de nós autorizados. No fim do processo, os nós envolvidos terão trocado as suas chaves de grupo atuais e poderão avaliar qual das duas chaves simétricas deve ser utilizada até a próxima troca de chave.

O processo de entrada de nó, representado na Figura 2(a), é iniciado quando um nó escuta um HELLO de um nó autorizado assinado com chave diferente da que possui, fora do intervalo da troca de chaves, como mostrado com o nó B. O nó B, então, inicia o processo de troca através do envio de uma mensagem Entrada em *unicast*. O nó A, ao receber a Entrada, verifica a sua lista de nós ausentes autorizados e, se o nó B estiver presente, responde com uma mensagem Passagem. A mensagem Passagem envia para o nó B a chave de grupo e as informações de número de nós na partição, nós excluídos, ausentes e novos, da partição de A, através do campo Lista de Parâmetros. Por fim, é enviada a mensagem Confirmação, que indica que a chave foi recebida e repassa a chave e as informações da partição de B. Para finalizar o processo, ambos os nós devem repassar por inundação os novos parâmetros para o resto da rede. Os campos das mensagens de entrada de novos nós são apresentados na Figura IV-B.

Caso o nó B, que iniciou o pedido de troca, não pertença à lista de nós autorizados do nó A, um segundo processo deve ser iniciado, pois pode ter existido uma notificação de entrada de nó que ficou restrita à partição de B. Se o nó indicado do grupo do nó B na mensagem Entrada também não estiver na lista de nós ausentes autorizados de A, a chave não será trocada com o nó B. Se estiver presente, o processo deve ser realizado entre o nó A e o nó indicado por B, por intermédio do próprio B, que conhece a rota para esse nó. Assim, o processo de troca fica mais robusto, pois aumenta a probabilidade de sucesso na união das partições.

Devido ao procedimento de entrada de nós e união de partições é necessário guardar o momento de ausência dos nós ausentes, de saída dos nós recentemente excluídos e entrada dos adicionados. De fato, as informações de excluídos e adicionados devem ser guardadas até que todos os nós que estavam ausentes quando as notificações foram feitas passem a ficar presentes e atualizem suas listas de nós autorizados. Após essa atualização, as informações podem ser descartadas, assim como a informação de quando foi iniciada a ausência do nó.

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 estiver na menor partição deve se anunciar como líder imediato e iniciar um processo de troca de chaves com uma mensagem de Anúncio. A informação da menor partição é conhecida pois em um protocolo de estado de enlace, como o SOLSR, todos os nós conhecem todos os enlaces da rede. Uma vez que esse pedido é assinado com a chave de grupo da menor partição, ele não será considerado válido por nenhum nó da maior partição.

C. Eleição do Líder

O nó líder tem o papel de iniciar o processo de troca de chaves. Ele deve ser trocado a cada rodada, impedindo a sobrecarga de um único nó com a inicialização do processo de troca, ou quando o processo de troca não se iniciar automaticamente, representando que o líder está ausente.

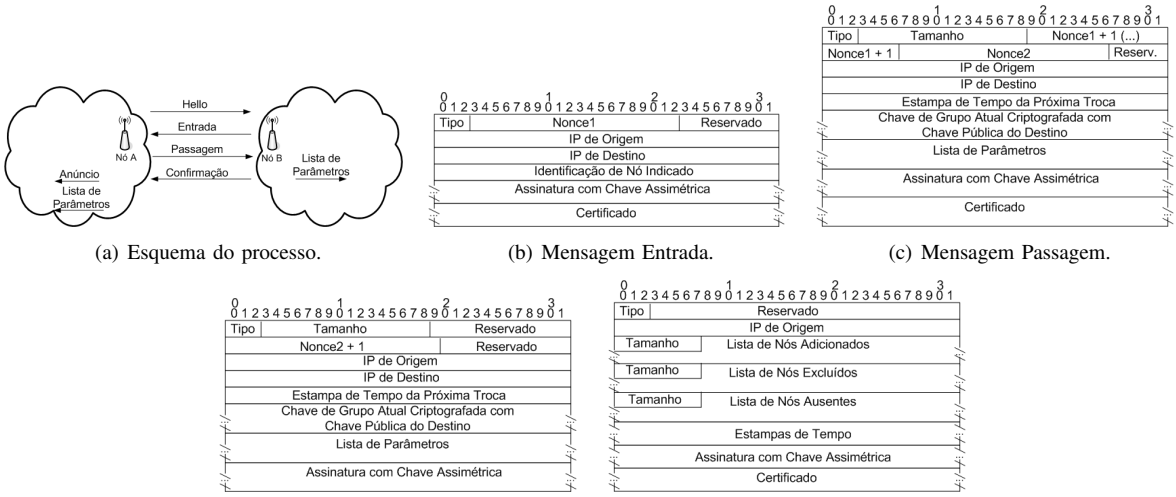
No caso da troca a cada rodada, o próximo líder é escolhido pelo atual usando como critério escolher o nó que minimiza o número de saltos até as bordas, excluindo-se o líder atual, de forma a reduzir os atrasos com a transmissão da chave. Essa informação é difundida com a mensagem Anúncio. No caso de falha ou ausência do líder, a eleição do próximo líder se faz de forma distribuída, escolhendo o nó de maior IP, e é controlada pelo tempo esperado de difusão da chave.

A eleição de um novo líder de forma distribuída implica em um novo cálculo do tempo espera pela chave, dado pela 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 IP deve iniciar o processo de troca de chaves como o novo líder. Um novo tempo T_{chave} é calculado para o novo líder, considerando 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. A eleição só é finalizada para um nó quando ele obtém a nova chave. 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 $T_{passagem}$.

$$T_{chave} = T_{passagem} * N_{saltos} + \delta \quad (2)$$

V. Análise do protocolo CHARADAS

O CHARADAS foi modelado em uma rede predicado-ação com os três procedimentos do protocolo. Essa rede foi



(a) Esquema do processo. (b) Mensagem Entrada. (c) Mensagem Passagem.

(d) Mensagem Confirmação. (e) Mensagem Lista de Parâmetros.

Fig. 2. Processo de entrada de nós e união de partições.

convertida em uma rede de Petri para avaliar o atendimento das propriedades clássicas, através do uso da ferramenta ARP (Analisador de Rede de Petri) versão 2.3. O resultado desta análise mostra que o protocolo atende às propriedades desejadas [Ramamoorthy e Yaw, 1986]: de ser uma rede limitada, pois o protocolo possui um número finito de estados; de ser viva, pois todos os estados são alcançáveis a partir de um estado inicial e então todas as ações que se deseja realizar são possíveis e de ser reiniciável, pois é possível retornar ao estado inicial a partir de qualquer estado da rede. A análise demonstrou também que o protocolo não possui *loops* ou pontos de onde não é possível avançar para outro estado.

A segunda análise realizada foi a de desempenho energético do CHARADAS, com o objetivo de verificar o custo em termos de energia consumida por nó usando o protocolo SOLSR com o protocolo CHARADAS. Como as funcionalidades providas pelo CHARADAS não seriam necessárias se assinatura com chaves assimétricas fosse utilizada, foi também analisado o consumo de energia do SOLSR com o uso de chaves assimétricas e comparado com o SOLSR com chave de grupo simétrica mais o CHARADAS.

A análise de desempenho do protocolo utilizou a ferramenta Matlab 6.5. 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 I. Como algoritmo para realizar a assinatura com chaves assimétricas e criptografia da chave de grupo, utilizou-se o RSA com uma chave de 1024 bits. Para realizar a assinatura com chave simétrica, utilizou-se o HMAC (*keyed-Hash Message Authentication Code*) com chave de 128 bits.

Os custos energéticos apresentados são funções do tamanho do pacote. Portanto, é necessário o cálculo do tamanho de cada pacote do SOLSR e do CHARADAS. As taxas de envio de pacotes de controle do SOLSR consideradas são as recomendadas em [Clausen e Jacquet, 2003], ou seja, um HELLO a cada 2 s e um TC a cada 5 s. A análise foi realizada supondo a existência de cem nós, durante o período de uma semana. Os parâmetros do CHARADAS considerados foram duas trocas automáticas por dia, dez nós adicionados por

TABELA I

CUSTOS CONSIDERADOS NA ANÁLISE MATEMÁTICA.

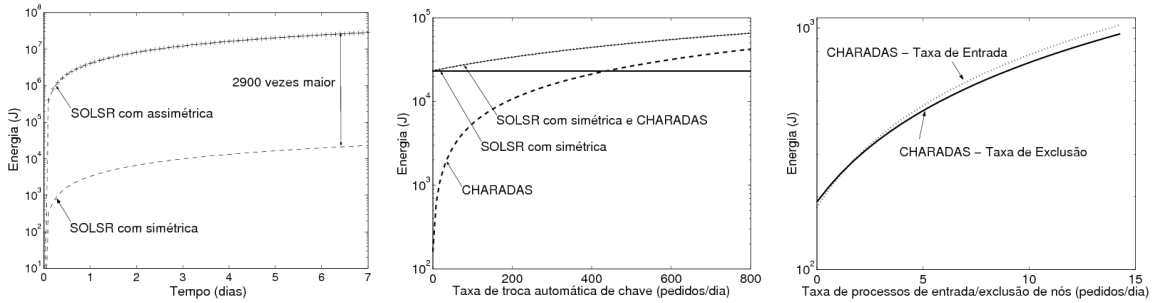
Ação	**Custo Energético**
Assinatura com HMAC-128	$1.16 * 10^{-6}$ J/b
Verificação de assinatura com HMAC-128	$0.145 * 10^{-6}$ J/b
Transmissão	$0.6582 * 10^{-6}$ J/b
Recepção	$0.28335 * 10^{-6}$ J/b
Assinatura com RSA-1024	0.816 J
Verificação de assinatura com RSA-1024	0.816 J
Criptografia com RSA-1024	0.0192 J

semana e dez nós excluídos por semana. Essas taxas devem ser ajustadas de acordo com a freqüência de ações maliciosas na rede e com a freqüência de entrada e saída dos nós. O impacto da variação desses parâmetros também foi analisado. Na entrada de nós, considerou-se que o nó analisado sempre está na menor partição, o que representa o pior caso para o CHARADAS, pois o nó terá que iniciar um processo de troca com a sua partição.

O cálculo energético também depende do cenário, pois o número de transmissões depende do número de vizinhos e MPRs de cada nó. Considerou-se um cenário mais denso do que o de uma rede comunitária [Campista et al., 2007], o que novamente representa o pior caso para o CHARADAS, pois ele sofre impactos com o aumento do número de vizinhos a serem servidos. Assumiu-se a tecnologia IEEE 802.11 a 54 Mbps, alcance de 12,8 m e nós dispostos em grade com 8 m de distância entre nós.

A Figura 3(a) mostra o custo energético do SOLSR usando chave de grupo simétrica (HMAC-128) e chaves assimétricas (RSA-1024). Em uma semana de uso, o SOLSR com assinatura assimétrica tem um consumo 2900 vezes maior do que o SOLSR com assinatura simétrica. O resultado comprova o alto consumo de energia das chaves assimétricas e a razão de se descartar o seu emprego em dispositivos com restrição de energia.

O custo energético do CHARADAS que é adicionado ao SOLSR pode ser observado na Figura 3(b). A curva do gasto de energia do CHARADAS foi apresentada para avaliação do impacto do protocolo sobre o SOLSR. Pelo gráfico, que representa uma semana de uso para um nó, é possível concluir



(a) Custo energético do SOLSR.

(b) Custo energético em função da taxa de troca automática de chave.

(c) Custo energético em função das taxa de entrada/exclusão de nós.

Fig. 3. Custo energético do SOLSR e do CHARADAS.

que o CHARADAS não representa um alto custo energético mesmo em situações extremas, como 800 pedidos de troca por dia, quando comparado ao uso contínuo de criptografia assimétrica. De fato, nessa situação, o SOLSR com criptografia assimétrica tem um custo 1.730 vezes superior ao uso de criptografia simétrica com o CHARADAS. Isso se explica pelo volume de mensagens de controle de roteamento que cada nó recebe ser muito superior ao número de mensagens geradas pelo CHARADAS. É importante ressaltar que esse processo periódico é necessário para a exclusão dos nós sem autorização que estão utilizando a rede e não apenas para impedir a quebra da chave simétrica. De fato, a probabilidade de quebra da chave simétrica, utilizando um algoritmo criptográfico robusto e uma chave grande, é muito baixa.

A entrada e a exclusão de nós influenciam diretamente no desempenho do protocolo, pois podem gerar novos processos de troca de chaves. Para avaliar o impacto desses comportamentos, foi variada, para um período de uma semana, a taxa média de processos de exclusão e de processos de entrada de nós autorizados que estavam ausentes ou desconectados, nos quais o nó analisado sempre está envolvido no processo de união de partição e está na menor partição, o que, novamente, representa a análise do pior caso para o CHARADAS. O resultado desta análise, que está representado na Figura 3(c), mostra que o consumo de energia do sistema cresce lentamente. De fato, o SOLSR com criptografia assimétrica possui um custo 10.900 vezes maior que o SOLSR com chaves simétricas funcionando com o CHARADAS com uma taxa média de 15 uniões de partições por dia.

VI. 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. O uso do CHARADAS restringe a entrada de usuários não-autorizados com a renovação periódica da chave utilizando criptografia assimétrica, tornando mais seguro o roteamento através de um controle preciso da lista de nós autorizados. Além disso, sincroniza o uso da chave nova e possui alta robustez contra falhas de nós e partições da rede. Com o uso de um sistema de detecção de intrusão, a segurança é ainda maior, pois nós maliciosos que utilizam a chave privada de nós autorizados também são excluídos da rede.

A análise de desempenho do CHARADAS indica um gasto energético não muito importante enquanto provê uma maior segurança no roteamento com chaves de grupo. Sua utilização se mostra interessante, em especial, em cenários onde equipamentos com pouca capacidade ou com restrições de bateria são utilizados. Além disso, sua alta tolerância a falhas permite que ele seja usado em cenários com mobilidade e com números de nós e conectividade variáveis.

Referências

[Campista et al., 2007] Campista, M. E. M., Moraes, I. M., Esposito, P., Amodei Jr., A., Costa, L. H. M. K. e Duarte, O. C. M. B. (2007). The ad hoc return channel: a low-cost solution for brazilian interactive digital TV. *IEEE Communications Magazine*, 45(1):136–143.

[Clausen e Jacquet, 2003] Clausen, T. e Jacquet, P. (2003). *Optimized Link State Routing Protocol (OLSR)*. RFC 3626.

[Fernandes et al., 2006] 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 SBSeg'2006*, páginas 49–102.

[Hafslund et al., 2004] 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.

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

[Li et al., 2006] Li, J. H., Levy, R., Yu, M. e Bhattacharjee, B. (2006). A scalable key management and clustering scheme for ad hoc networks. Em *First International Conference on Scalable Information Systems (INFOSCALE'06)*, página 28.

[Luo et al., 2006] Luo, L., Safavi-Naini, R., Baek, J. e Susilo, W. (2006). Self-organised group key management for ad hoc networks. Em *ASIACCS'06*, páginas 138–147.

[Potlapally et al., 2003] Potlapally, N. R., Ravi, S., Raghunathan, A. e Jha, N. K. (2003). Analyzing the energy consumption of security protocols. Em *ISLPED '03*, páginas 30–35.

[Puzar et al., 2005] Puzar, M., Andersson, J., Plagemann, T. e Roudier, Y. (2005). SKiMPy: A simple key management protocol for manets in emergency and rescue operations. Em *ESAS 2005*, páginas 14–26.

[Ramamoorthy e Yaw, 1986] Ramamoorthy, C. V. e Yaw, Y. (1986). A petri net reduction algorithm for protocol analysis. Em *ACM SIGCOMM'86*, páginas 157–166.

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