ANÁLISE DE DESEMPENHO DE PROTOCOLOS PARA
ESTABELECIMENTO DE CHAVE DE GRUPO EM REDES AD HOC

Eric Ricardo Anton

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. Otto Carlos Muniz Bandeira Duarte, Dr. Ing.

Prof. Marcelo Gonçalves Rubinstein, D.Sc.

Luís Henrique Maciel Kosmalski Costa, Dr.

Prof. Fabio Kon, Ph. D.

RIO DE JANEIRO, RJ - BRASIL

MARÇO DE 2003

ANTON, ERIC RICARDO

Análise de Desempenho de Protocolos para Estabelecimento de Chave de Grupo em Redes Ad Hoc [Rio de Janeiro] 2003

X, 53 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2003)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Redes sem fio ad hoc
2. Segurança
3. Mobilidade

I. COPPE/UFRJ II. Título (série)

À Ana Carolina.

Agradecimentos

À minha família, principalmente meus pais, por todo o amor, orientação e apoio ao longo da minha vida.

À minha querida Ana Carolina e à sua família pela maravilhosa presença na minha vida.

Ao professor Otto por toda a orientação e conselhos no andamento da tese.

A toda a equipe do GTA, em particular aos amigos Pedro, Kleber, Rubi, Doc, Luis Henrique e Rezende, pela amizade e pela ajuda com o desenvolvimento da tese.

Ao Fabio Kon pela presença na banca examinadora.

Ao PEE/COPPE, pelas instalações e equipamentos utilizados.

À CAPES, pelo financiamento da pesquisa.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

ANÁLISE DE DESEMPENHO DE PROTOCOLOS PARA
ESTABELECIMENTO DE CHAVE DE GRUPO EM REDES AD HOC

Eric Ricardo Anton

Março/2003

Orientador: Otto Carlos Muniz Bandeira Duarte
Programa: Engenharia Elétrica

As redes sem fio ad hoc possuem duas características principais: ausência de infra-estrutura e possibilidade de conectar dispositivos móveis. No entanto, estas redes são muito frágeis com relação à segurança. Este trabalho foca a questão do estabelecimento de uma chave criptográfica secreta entre um grupo de dispositivos que fazem parte de uma rede ad hoc. Os principais protocolos para o estabelecimento de chave de grupo são analisados e são simulados os dois que apresentaram desempenhos superiores aos demais. As simulações visam avaliar a taxa de sucesso do estabelecimento de uma chave de grupo e o tempo necessário para o estabelecimento desta chave. As simulações são efetuadas para dois tipos de cenários: movimentação individual e em grupo. Os resultados indicam que a conectividade entre os dispositivos é o maior problema deste ambiente onde é requerida uma alta densidade de dispositivos móveis para se ter sucesso no estabelecimento da chave de grupo. Cenários com movimentação em grupo exigem bem menos mensagens apesar de exigirem maiores densidades de dispositivos para garantir o estabelecimento da chave de grupo.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

PERFORMANCE ANALYSIS OF GROUP KEY
ESTABLISHMENT PROTOCOLS IN AD HOC NETWORKS

Eric Ricardo Anton

March/2003

Advisor: Otto Carlos Muniz Bandeira Duarte

Department: Electrical Engineering

Wireless ad hoc networks have two main characteristics: absence of infrastructure and the possibility to connect mobile devices. These networks are however very fragile regarding security. This work focuses on the establishment of a secret cryptographic key among a group of devices that are part of an ad hoc network. The main group key establishment protocols are analyzed and the two that present best performance are simulated. Simulations aim at evaluating the group key establishment success rate and the required time for the establishment of this key. Simulations are executed for two kinds of scenarios: individual and group mobility. Results indicate that device connectivity is this environment's greatest problem, requiring high densities of mobile devices to assure group key establishment. Scenarios with group mobility demand fewer messages, although they demand higher device densities in order to guarantee device connectivity.

Sumário

Lista de Figuras

Capítulo 1

Introdução

AS redes sem fio têm apresentado um grande crescimento nos últimos anos, em grande parte devido à sua maior facilidade de instalação, quando comparadas às redes tradicionais, e à possibilidade de movimentação dos dispositivos durante o uso da rede, permitindo assim maior praticidade e flexibilidade. As aplicações para redes sem fio compreendem desde comunicações a curtas distâncias com pouca mobilidade, como encontros em salas de reunião, a comunicações com maiores distâncias e com bastante mobilidade, como operações militares ou de resgate. Muitas destas aplicações seriam muito inconvenientes, ou até mesmo inviáveis, de serem realizadas em redes tradicionais.

A comunicação por este tipo de rede apresenta no entanto algumas limitações como reduzida banda-passante, altas taxas de erro e, em geral, limitados poder computacional e fornecimento de energia dos dispositivos portáteis. É desejável, portanto, uma melhor utilização da banda-passante e da capacidade computacional disponíveis, por meio da utilização de protocolos que minimizem o número de mensagens, a quantidade total de dados transmitidos e a quantidade de processamento realizado.

Devido à carência de mecanismos de segurança em redes ad hoc, este trabalho avalia a utilização dos principais protocolos para o estabelecimento de uma chave criptográfica secreta, ou chave de grupo, neste tipo de rede, de modo a prover comunicações seguras entre um grupo de dispositivos.

1.1 Redes sem fio

Uma possibilidade de rede sem fio consiste na comunicação de cada dispositivo com os demais por meio de um equipamento centralizador, denominado ponto de acesso. Neste tipo de rede, cada dispositivo somente comunica-se com algum ponto de acesso, podendo este ser sempre o mesmo ou não. O ponto de acesso é conectado a outros pontos de acesso ou a outras redes, exercendo as atividades de controle de acesso e de encaminhamento de mensagens de um dispositivo para outro, estejam eles localizados na mesma rede local ou em redes diferentes. Este tipo de rede necessita, portanto, de pelo menos um ponto de acesso para prover a comunicação entre os dispositivos. Por esta razão, este tipo de rede sem fio é denominado rede sem fio infra-estruturada. A área de cobertura deste tipo de rede é bem delimitada, sendo determinada pela área de cobertura dos pontos de acesso. Assim, todos os dispositivos capazes de estabelecer comunicação com algum ponto de acesso são capazes de se comunicar com todos os demais na mesma situação.

Outra possibilidade de rede sem fio, denominada rede sem fio ad hoc, é composta por um conjunto de dispositivos capazes de se comunicar diretamente, sem a necessidade de pontos de acesso. Assim, desde que os dispositivos estejam posicionados a uma distância suficiente para que os dados transmitidos pelo dispositivo fonte alcancem o dispositivo destino, eles são capazes de se comunicar diretamente, sem depender de outros dispositivos. Em situações nas quais estes dispositivos estão mais afastados, não sendo possível a comunicação direta entre eles, é necessário que haja outros dispositivos capazes de encaminhar mensagens da fonte até o destino, ocorrendo então uma comunicação por múltiplos saltos. Neste caso, os próprios dispositivos móveis assumem também a função de roteadores.

Alguns possíveis cenários de comunicações que podem ser viabilizadas por redes ad hoc consistem na comunicação entre um telefone celular, um fone de ouvido sem fio, um computador de mão, um computador portátil ou um relógio, de uma mesma pessoa; na comunicação entre os computadores portáteis e de mão de diferentes pessoas, durante uma reunião ou aula; na comunicação entre equipamentos médicos como termômetros, medidores de ritmo cardíaco e medidores de respiração e o computador de mão de um médico; na comunicação entre o computador de mão de um cliente e o computador de um

supermercado ou de um restaurante; na comunicação entre o computador de mão de um visitante e o computador de um museu, posicionado junto a um objeto em exposição; na comunicação entre os carros que percorrem uma rodovia e o computador que controla esta rodovia ou recolhe seu pedágio; na comunicação entre os membros de uma família que estão espalhados por um centro de compras ou por uma feira de evento, mas desejam se comunicar; na comunicação entre os organizadores de um evento; na comunicação entre grupos de turistas que estão visitando um museu ou uma cidade histórica, entre outros.

Outros possíveis cenários são aplicações militares, de policiamento ou de resgate, como a comunicação entre batalhões de um exército, entre grupos policiais durante uma operação de busca e apreensão; a comunicação entre grupos de resgate dos sobreviventes de uma avalanche de neve; a comunicação entre helicópteros de busca de um avião acidentado em alto mar; a comunicação entre grupos de busca de sobreviventes em uma selva.

Apesar de suas vantagens, como praticidade, mobilidade e flexibilidade, as redes sem fio apresentam problemas intrínsecos de segurança, devido à transmissão de dados pelo ar, pois qualquer dispositivo posicionado dentro do raio de alcance de um transmissor é capaz de receber os dados transmitidos. Ainda devido ao canal utilizado, a geração ou alteração indevida de mensagens é mais simples neste tipo de rede do que em redes tradicionais, onde o canal de transmissão de dados é um meio cujo acesso físico pode ser dificultado.

Em alguns dos cenários apresentados, a segurança das informações transmitidas pela rede sem fio é fundamental, como em operações de comércio, policiamento ou reuniões de negócios, havendo portanto a necessidade de mecanismos que proporcionem níveis adequados de segurança para cada tipo de aplicação.

1.2 Segurança em redes de computadores

A segurança para troca de mensagens por meio de redes de computadores pode atender a três requisitos:

- integridade – garantir que a mensagem recebida pelo destinatário é idêntica àquela que foi enviada pelo emissor;
- privacidade – garantir que somente o destinatário é capaz de compreender o conteúdo da mensagem;
- autenticação – garantir que uma entidade é realmente quem ela diz ser.

Estes requisitos são atendidos pelo uso de códigos de integridade de mensagem e de algoritmos criptográficos. Códigos de integridade de mensagem são utilizados de forma semelhante a um código detector de erro, para detectar alterações indevidas nas mensagens transmitidas, garantindo assim a integridade da informação.

Algoritmos criptográficos são responsáveis por codificar um conjunto de dados de modo a torná-lo incompreensível. Existem dois tipos de criptografia. O primeiro, denominado criptografia simétrica, ou de chave secreta, faz uso de uma única chave para encriptar e decriptar os dados. A chave criptográfica utilizada deve ser de conhecimento apenas das entidades que desejam trocar informações de forma segura, sendo mantida secreta de todas as demais. Assim é garantida a autenticação e a privacidade da comunicação.

O segundo tipo de criptografia, denominado criptografia assimétrica, ou de chave pública, utiliza um par de chaves criptográficas associado a cada entidade: uma chave privada que deve ser mantida em sigilo, e uma chave pública que pode ser livremente distribuída. Uma importante característica deste tipo de criptografia consiste no fato de que os dados encriptados com uma das chaves somente podem ser decriptados com a outra. Para garantir a privacidade da comunicação e a autenticação do destinatário, o emissor utiliza a chave pública do destinatário na proteção de dados, pois estes dados somente podem ser acessados pelo destinatário, que detém a chave privada. Para se garantir a autenticação do emissor, os dados são encriptados com a chave privada do emissor, de forma que somente podem ser acessados com o uso de sua chave pública, que é de conhecimento geral. O sucesso da decriptação com a chave pública garante que somente o detentor da chave privada pode ter gerado um conjunto válido de dados. Este tipo de criptografia requer que todos os dispositivos conheçam as chaves públicas de todos os dispositivos com

os quais desejem se comunicar. Isto é geralmente garantido utilizando-se servidores de chaves públicas.

A seção seguinte aborda a questão da segurança em redes sem fio ad hoc, sendo mencionados alguns trabalhos relacionados, apresentado o modelo de comunicação utilizado e avaliada a viabilidade de utilização dos dois tipos de criptografia para prover segurança a este modelo.

1.3 Segurança em redes sem fio ad hoc

Os aspectos de segurança em redes sem fio são de grande importância devido às vulnerabilidades intrínsecas ao processo de comunicação sem fio, como a facilidade de escuta passiva e de ataques ativos. Assim, são necessários mecanismos de segurança que garantam a integridade e a privacidade da comunicação, bem como a autenticação das entidades envolvidas. A implementação de mecanismos de segurança em redes sem fio infra-estruturadas é relativamente simples, devido à maior facilidade de disponibilidade de servidores de chave pública. É possível ainda a autenticação e o estabelecimento de uma chave criptográfica secreta entre cada dispositivo e o ponto de acesso com o qual está se comunicando. Assim, cada dispositivo somente precisa ser autenticado uma única vez, e o ponto de acesso, ao encaminhar uma mensagem de um dispositivo para outro, utiliza a chave compartilhada com o dispositivo fonte para decriptar a mensagem. Esta mensagem é então encriptada com a chave compartilhada com o dispositivo destino e encaminhada a este dispositivo.

Em redes ad hoc, devido à ausência de dispositivos que centralizem e coordenem a comunicação, a implementação de mecanismos de segurança é complexa, pois os mecanismos desenvolvidos para redes convencionais não são convenientes para utilização no ambiente ad hoc, devido às hipóteses geralmente adotadas como disponibilidade de servidores de autenticação e repositórios de chaves públicas. Em ambientes ad hoc estas hipóteses geralmente não são verdadeiras, cabendo aos próprios membros que compõem a rede o estabelecimento de uma relação de segurança entre si.

A maior parte dos estudos sobre segurança em redes ad hoc concentra-se na área de roteamento seguro [1, 2, 3]. Estes estudos supõem no entanto o compartilhamento de uma chave criptográfica entre os dispositivos móveis, ou seja, que o estabelecimento de uma chave de grupo já ocorreu. O estabelecimento de uma chave de grupo em redes ad hoc é abordado por Asokan e Ginzboorg [4], que propõem uma versão tolerante a falhas do protocolo para estabelecimento de chave de grupo Hipercubo [5] (Seção 2.4) e mecanismos de autenticação entre os membros de um grupo.

Ainda com relação à segurança em redes ad hoc, Haas e Zhou [6] abordam a questão de serviços de certificação utilizando criptografia assimétrica e apresentam um esquema de distribuição da responsabilidade de uma autoridade certificadora de chave pública entre um conjunto de dispositivos que fazem parte de uma rede ad hoc. Khalili *et al.* [7] baseiam-se nesta proposta, substituindo a autoridade certificadora por um serviço distribuído de geração de chaves privadas. A questão da autenticação é abordada por Stajano e Anderson [8], que apresentam um modelo de política de segurança baseado na autenticação de dispositivos ad hoc por meio do contato físico destes dispositivos com outros. Balfanz *et al.* [9] abordam a questão da segurança e da autenticação em redes ad hoc propondo a utilização de um canal privado de alcance restrito para autenticação, como o contato entre os dispositivos ou a utilização de raios infravermelhos ou de som.

Este trabalho visa o estabelecimento de comunicações seguras entre os dispositivos que compõem uma rede ad hoc, ou seja, um conjunto de usuários deseja que seus dispositivos eletrônicos sem fio sejam capazes de trocar informações entre si de forma autêntica, íntegra e com privacidade. Busca-se então que estes dispositivos estabeleçam uma relação de segurança entre si, compondo assim um grupo seguro. As mensagens enviadas entre membros deste grupo podem então ser protegidas de forma que somente membros do grupo tenham acesso aos seus conteúdos, que eventuais alterações destes conteúdos sejam detectadas e que dispositivos que não participem do grupo não sejam capazes de forjar mensagens como sendo do grupo.

Uma vez que o grupo como um todo atua como uma única entidade, a utilização de criptografia assimétrica, como proposto por Haas e Zhou [6] e por Khalili *et al.* [7], não se aplica a este modelo de comunicação, pois o conceito de chaves pública e privada implica

na comunicação entre duas entidades. A associação de um par de chaves pública e privada a um grupo faz sentido para a comunicação de membros deste grupo com dispositivos externos ao grupo, mas não para comunicações entre membros de um mesmo grupo.

Este trabalho analisa [10, 11, 12] os principais protocolos para o estabelecimento de uma chave de grupo e avalia por simulação [13, 14] os dois que melhor se adaptam às redes ad hoc. O estabelecimento deste tipo de chave é um dos primeiros passos em direção ao estabelecimento de uma comunicação segura entre os dispositivos que compõem a rede ad hoc. Com base nesta chave podem ser implementados diversos mecanismos seguros, como roteamento seguro e detecção de intrusão, sendo garantida autenticação, integridade e privacidade das mensagens transmitidas sob a proteção da chave de grupo.

Uma vez definidos os dispositivos que participarão do grupo seguro, estes dispositivos executam um protocolo e ao final da execução deste protocolo todos os membros do grupo, e apenas os membros do grupo, compartilham uma chave de grupo.

A autenticação dos membros do grupo deve ocorrer antes ou durante o estabelecimento da chave de grupo de modo a restringir quais dispositivos podem participar da geração desta chave e ter acesso a ela. Uma vez que um membro do grupo conhece a chave de grupo, sua autenticação perante os demais membros do grupo está implícita no conhecimento desta chave. A questão da autenticação não é abordada neste trabalho, existindo no entanto diversas propostas [4, 8, 9, 15, 16, 17] para autenticação entre os membros de um grupo.

Um dos desafios iniciais na utilização de criptografia simétrica era o estabelecimento de uma chave secreta entre duas entidades quaisquer, o que foi solucionado por Diffie e Hellman [18], que propuseram um algoritmo que ficou conhecido pelo nome de seus autores. Algumas extensões do algoritmo Diffie-Hellman para o caso de múltiplos participantes foram propostas [19, 20, 5, 21, 22, 16, 17, 23] e são apresentadas no Capítulo 2. Kim *et al.* [24] propõem um estabelecimento de chave de grupo baseado em árvores binárias.

Este trabalho está organizado da seguinte forma. O Capítulo 2 apresenta o algoritmo Diffie-Hellman e os principais protocolos para estabelecimento de chave de grupo. É re-

alizada também uma comparação analítica entre os desempenhos destes protocolos. No Capítulo 3 são apresentados os resultados obtidos por simulação destes protocolos e comparados seus desempenhos com base nestas simulações. É utilizado o modelo de mobilidade geralmente utilizado, no qual os dispositivos se movem de forma independente dos demais, e é proposto um modelo no qual grupos de dispositivos se movem em conjunto. O Capítulo 4 finaliza o trabalho expondo as conclusões finais obtidas.

Capítulo 2

Estabelecimento de Chave de Grupo

O estabelecimento de uma chave de grupo entre os membros que compõem uma rede ad hoc pode ocorrer em diversas situações. Em um cenário de uso no qual todos os dispositivos que compõem a rede estão localizados em uma área geograficamente restrita, como por exemplo uma sala de reuniões, uma casa, um apartamento, uma sala médica ou um restaurante, todos os dispositivos são capazes de se comunicar diretamente com todos os demais a todo instante, não havendo problema de conectividade entre eles. Neste tipo de cenário o estabelecimento de uma chave de grupo é mais simples, pois todos os dispositivos são mutuamente alcançáveis durante o estabelecimento da chave de grupo.

Outra possibilidade de cenário consiste de vários dispositivos movimentando-se por uma área maior que o raio de alcance de cada dispositivo. Cada dispositivo movimenta-se livremente, de forma independente dos demais. Nesta situação, a comunicação entre eles não pode ser garantida, pois pode haver dispositivos que não sejam capazes de se comunicar com os demais. Isto gera problemas, pois não é mais possível garantir a conectividade mútua de todos os pares de dispositivos. Não há, portanto, como garantir que todos os dispositivos estejam presentes durante o estabelecimento da chave de grupo.

Outra possibilidade é um cenário semelhante ao anterior, mas com os dispositivos movimentando-se em grupos. Neste cenário, pode ser utilizada a característica de grupo de forma que apenas um dispositivo de cada grupo participa do estabelecimento da chave em vez de todos os dispositivos participarem. Este procedimento reduz o custo da geração

da chave.

A segurança da comunicação entre os membros do grupo seguro estabelecido deve ser garantida por meio de mecanismos e políticas de gerenciamento da chave de grupo. Por gerenciamento da chave de grupo entende-se as atividades de estabelecimento desta chave entre os membros do grupo e a sua manutenção de modo a garantir que os requisitos de segurança estabelecidos sejam atendidos. As atividades de manutenção consistem nas trocas das chaves criptográficas utilizadas, seja devido à adição ou à exclusão de membros do grupo, de modo a atender aos requisitos de sigilo do futuro e de sigilo do passado[1], ou à utilização da chave por períodos longos de tempo, de modo a dificultar ataques por força-bruta. Uma boa política de gerenciamento de chave é fundamental para a prestação de serviços de segurança e deve definir quando e como a chave de grupo deve ser alterada.

O estabelecimento de uma chave de grupo pode ocorrer de forma centralizada, também denominada distributiva, onde uma entidade é responsável pela geração da chave e sua distribuição aos demais membros. Esta abordagem apresenta a vantagem de ser simples, mas seu uso em redes ad hoc não é conveniente devido aos seguintes fatores:

- segurança – a segurança de um sistema de gerenciamento de chave centralizado depende de apenas um dispositivo; caso este dispositivo seja comprometido, todo o sistema também fica comprometido, de forma que este dispositivo é um forte candidato a sofrer ataques;
- tolerância a falhas e disponibilidade – como no caso anterior, caso o dispositivo centralizador apresente falhas ou pare de funcionar, todo o sistema fica indisponível;
- conectividade – em redes ad hoc a conectividade entre os dispositivos nem sempre pode ser garantida. Assim, mesmo que o dispositivo centralizador esteja operando sem problemas, pode haver dispositivos incapazes de contactá-lo devido a problemas de interferência, congestionamento ou partição da rede.

Outra possibilidade é o estabelecimento da chave de grupo de forma contributiva, onde

[1] O sigilo do futuro garante que os membros que abandonam o grupo não conseguem acesso às futuras chaves de grupo e o sigilo do passado garante que novos membros do grupo não conseguem acesso às antigas chaves de grupo.

todos os membros do grupo contribuem para a geração da chave. Algumas vantagens desta abordagem consistem em ser tolerante a falhas, devido à distribuição da responsabilidade de geração da chave, em diminuir os riscos de vícios na geração de chaves por uma única entidade e na garantia, para cada dispositivo, da aleatoriedade da chave, desde que sua contribuição seja aleatória. A técnica contributiva permite variações quanto à definição do grupo responsável pelo estabelecimento da chave, que pode exigir a totalidade dos membros ou um subconjunto destes.

A abordagem contributiva é portanto a mais adequada para implementação em redes ad hoc. Uma vez estabelecida uma chave de grupo entre os membros deste grupo, sua utilização na encriptação das mensagens transmitidas entre os membros do grupo fornece autenticação, integridade e privacidade, pois somente dispositivos que possuem acesso à chave de grupo são capazes de gerar, alterar e compreender as mensagens protegidas com esta chave.

As seções seguintes apresentam o algoritmo Diffie-Hellman, que é o principal algoritmo para o estabelecimento de chave secreta entre duas entidades, e alguns dos principais protocolos para estabelecimento de chave de grupo. Estes protocolos são extensões naturais do algoritmo Diffie-Hellman para o caso de múltiplos participantes, conforme definido por Steiner *et al.* [21], herdando portanto todas as suas características de segurança, e proporcionam um estabelecimento contributivo da chave de grupo. É realizada na Seção 2.6 uma comparação entre estes protocolos de modo a determinar qual o mais adequado para utilização em redes ad hoc.

2.1 O Algoritmo Diffie-Hellman

Desenvolvido por Diffie e Hellman [18], este algoritmo permite o estabelecimento de uma chave criptográfica secreta entre duas entidades por meio da troca de dados utilizando um canal inseguro de comunicação. A execução do algoritmo entre duas entidades A e B segue os seguintes passos:

1. A e B concordam[2] na utilização de dois números p e g inteiros positivos escolhidos aleatoriamente, tais que p é primo e grande e $g < p$;
2. A escolhe um número aleatório secreto S_A e B escolhe um número aleatório secreto S_B;
3. A calcula um valor público $T_A = (g^{S_A} \bmod p)$ e B calcula um valor público $T_B = (g^{S_B} \bmod p)$;
4. A envia T_A para B e B envia T_B para A;
5. A calcula ${T_B}^{S_A} \bmod p = (g^{S_B})^{S_A} \bmod p$ e B calcula ${T_A}^{S_B} \bmod p = (g^{S_A})^{S_B} \bmod p$.

Como $(g^{S_A})^{S_B} \bmod p = (g^{S_B})^{S_A} \bmod p = K$, estas duas entidades compartilham a chave criptográfica secreta K.

Em outras palavras, duas entidades trocam informações por um meio onde qualquer um pode escutar e no final do processo as duas entidades, e só estas duas entidades, conseguem compartilhar uma mesma chave secreta.

A segurança deste algoritmo se baseia na dificuldade de se calcular a chave secreta $K = g^{S_A S_B} \bmod p$, mesmo conhecidos os valores públicos $g^{S_A} \bmod p$ e $g^{S_B} \bmod p$, quando o número primo p é suficientemente grande, da ordem de 128 a 256 bits para os padrões atuais.

Todas as operações matemáticas realizadas por este algoritmo se baseiam em aritmética modular, onde p é o módulo utilizado. Todos os protocolos apresentados a seguir também utilizam aritmética modular p, estando este conceito implícito nos valores apresentados.

2.2 O Protocolo de Ingemarsson et al.

Este protocolo, apresentado por Ingemarsson *et al.* [19], referido neste trabalho como ING, foi uma das primeiras tentativas de se estender o algoritmo Diffie-Hellman para o

[2]Todas as informações trocadas entre as entidades fazem uso de um canal inseguro, sendo portanto considerados de conhecimento público.

caso de múltiplos participantes. A execução do protocolo exige que os n membros do grupo estejam dispostos na forma de um anel lógico. Ao início da execução do protocolo cada participante M_i, $i \in [1, n]$, gera um valor aleatório secreto S_i, que é a sua contribuição para a chave de grupo, e envia g^{S_i} para o próximo participante (M_{i+1} para $i \in [1, n-1]$ e M_1 para $i = n$), conforme ilustrado pela Figura 2.1.

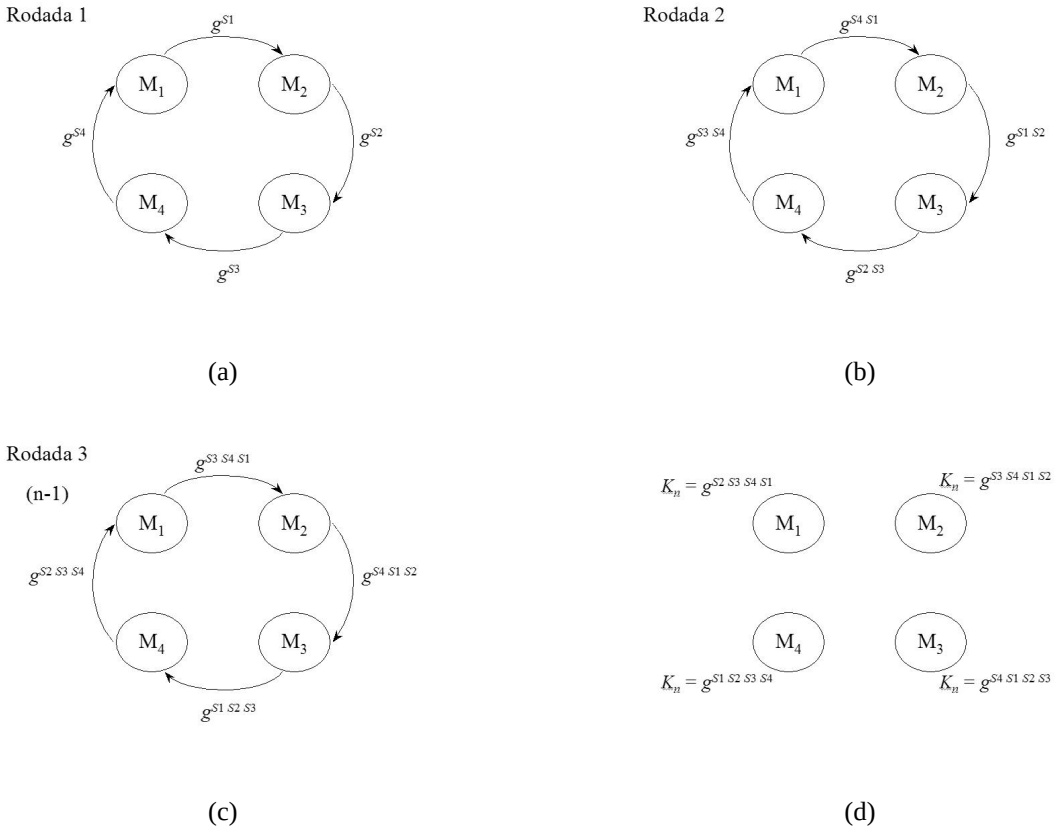


Figura 2.1: Protocolo de Ingemarsson *et al.* para n = 4.

A cada rodada do algoritmo, cada participante eleva o valor recebido na rodada anterior ao seu valor secreto S_i e envia o resultado ao próximo participante da seqüência. Todos os participantes enviam, portanto, uma mensagem para outro participante, ocorrendo, a cada rodada, a transmissão de n mensagens entre os n membros do grupo. Após $n - 1$ rodadas, todos os participantes terminam por calcular a mesma chave de grupo $K_n = g^{S_1 \cdot S_2 \cdot \ldots \cdot S_n}$. São transmitidas, portanto, n mensagens de tamanho fixo a cada uma das $n - 1$ rodadas do protocolo.

A principal desvantagem desta proposta consiste no elevado número de mensagens necessárias à sua execução, bem como no elevado número de operações de exponenciação,

conforme apresentado na Seção 2.6.

2.3 O Protocolo de Burmester e Desmedt

Este protocolo, apresentado por Burmester e Desmedt [20], referido neste trabalho como BD, é executado em três rodadas, que consistem das seguintes operações, executadas por cada participante M_i, $i \in [1, n]$:

1. geração de um valor aleatório secreto S_i, que é sua contribuição para a chave de grupo, e envio do valor $z_i = g^{S_i}$ aos demais participantes;
2. cálculo e transmissão por difusão aos demais participantes do valor $X_i = (\frac{z_{i+1}}{z_{i-1}})^{S_i}$ [3];
3. computação da chave de grupo $K_n = z_{i-1}^{nS_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdot \ldots \cdot X_{i-2}$.

A chave de grupo obtida é da forma $K_n = g^{S_1 \cdot S_2 + S_2 \cdot S_3 + \ldots + S_n \cdot S_1}$ e compartilha as características de segurança apresentadas pelo protocolo Diffie-Hellman. Este protocolo é eficiente quanto ao número total de rodadas, o que poderia proporcionar uma execução mais rápida. No entanto, estas rodadas requerem a execução de n transmissões simultâneas por difusão, o que geralmente não é possível, mesmo em redes sem fio, pois somente pode haver um dispositivo difundindo mensagens a cada instante. Devido a esta característica, a implementação deste protocolo deve ocorrer por meio do envio seqüencial de mensagens, o que anula a vantagem de serem necessárias poucas rodadas, pois o envio de cada mensagem comporta-se como uma rodada. Em cada uma das duas rodadas, cada um dos n participantes transmite, portanto, $n - 1$ mensagens de tamanho fixo. É necessário ainda um elevado número de operações de exponenciação.

2.4 O Protocolo Hipercubo

O protocolo Hipercubo, apresentado por Becker e Wille [5] procura contornar o elevado número de mensagens do protocolo ING por meio da disposição lógica dos dis-

[3] $z_0 = z_n$ e $z_{n+1} = z_1$

positivoss na forma de hipercubo. Para o caso de 4 dispositivoss dispostos em forma de quadrado é estabelecida uma chave ($g^{S_a S_b}$) entre A e B e outra ($g^{S_c S_d}$) entre C e D, que são utilizadas para estabelecer uma chave ($g^{(g^{S_a S_b})(g^{S_c S_d})}$) única entre as 4 entidades, conforme apresentado pela Figura 2.2. Este comportamento pode ser generalizado para cenários com um maior número de dispositivos, devendo o número de participantes ser igual a 2^d. O protocolo é executado ao longo de d rodadas, sendo transmitidas n mensagens de tamanho fixo a cada rodada.

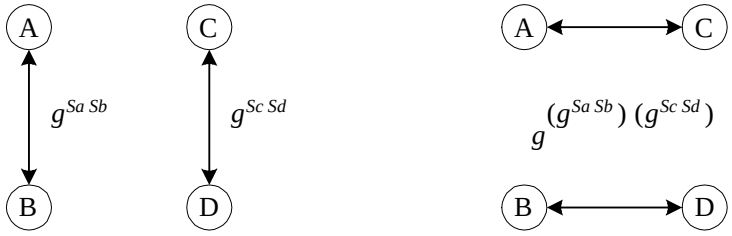


Figura 2.2: Protocolo Hipercubo para n = 4.

Em [5] é também apresentado o protocolo Octopus, que é uma extensão do protocolo Hipercubo para um número arbitrário de participantes. Os participantes da execução deste protocolo são divididos em dois grupos: participantes de núcleo, que devem estar dispostos na forma de um hipercubo, e de periferia. Cada um dos participantes de periferia associa-se a um dos participantes do núcleo e estabelece com ele uma chave criptográfica simétrica por meio do algoritmo Diffie-Hellman. Os participantes de núcleo executam então o protocolo Hipercubo. Cada participante de núcleo utiliza como contribuição o produto de um valor secreto gerado por ele com as chaves estabelecidas com os participantes da periferia aos quais se associou. A chave criptográfica estabelecida entre os participantes de núcleo é então distribuída a cada participante de periferia, protegida pela chave estabelecida com um dos participantes de núcleo no início da execução do protocolo.

2.5 A família de protocolos CLIQUES

Desenvolvida por Steiner *et al.* [21, 22, 16, 17, 23], a família de protocolos CLIQUES é composta por protocolos de gerenciamento de chave para grupos dinâmicos. Dois destes

protocolos, IKA.1 e IKA.2 (*Initial Key Agreement* 1 e 2), são definidos para o estabelecimento da chave de grupo. Os demais protocolos executam a adição e a exclusão de membros e subgrupos e a troca da chave de grupo utilizada, não sendo necessária a execução completa do procedimento de estabelecimento de chave, reduzindo assim os custos envolvidos com operações de troca da chave de grupo. São também propostas versões destes protocolos com suporte a autenticação. A seguir são apresentadas as versões básicas destes protocolos.

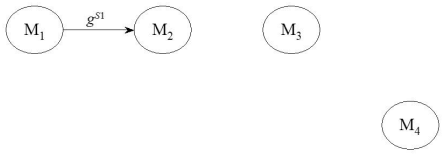
2.5.1 IKA.1

O protocolo IKA.1 é executado em duas etapas:

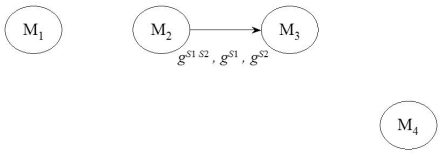
1. $M_i \Rightarrow M_{i+1}\ ,\ i \in [1, n-1]\ :$
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_i}{S_k}}\ |\ k \in [1, i]\},\ g^{S_1 \cdot S_2 \cdot \ldots \cdot S_i}$
2. $M_n \Rightarrow M_i\ ,\ i \in [1, n-1]\ :$
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_n}{S_i}}\ |\ i \in [1, n-1]\}$,

onde n é o número de participantes na execução do protocolo, ou seja, o número de membros do grupo, g é a base da exponenciação, M_i é o i-ésimo participante, S_i é o expoente aleatório secreto gerado por M_i, ou seja, sua contribuição para a chave de grupo.

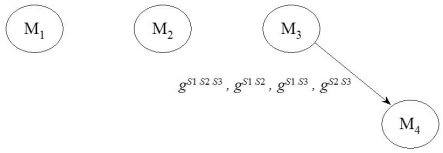
A execução deste protocolo é ilustrado pela Figura 2.3. Na primeira etapa são coletadas as contribuições dos $n-1$ primeiros membros do grupo, o que ocorre ao longo de $n-1$ rodadas. A cada rodada um dos participantes recebe um conjunto de dados do participante que o antecedeu na execução do protocolo. Este conjunto de dados é composto por um valor, denominado valor cardinal, que possui a contribuição de todos os membros que o antecedem na execução do protocolo e vários valores, denominados valores intermediários. Cada um destes valores intermediários possui a contribuição de todos os membros que o antecedem na execução do protocolo, exceto a de um deles. O membro adiciona sua contribuição a todos estes valores e repassa o novo conjunto de dados ao próximo participante.



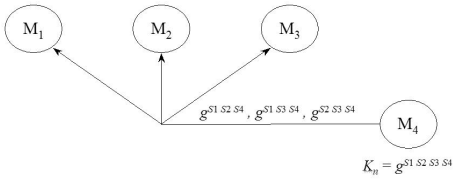
(a) 1^a etapa, 1^a rodada



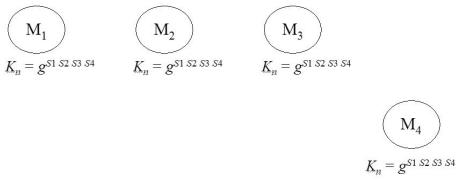
(b) 1^a etapa, 2^a rodada



(c) 1^a etapa, 3^a rodada



(d) 2^a etapa



(e) Finalização

Figura 2.3: Protocolo IKA.1 para n = 4.

O participante M_4, por exemplo, recebe de M_3 o conjunto $\{g^{S_1 \cdot S_2 \cdot S_3}$, $g^{S_1 \cdot S_2}$, $g^{S_1 \cdot S_3}$, $g^{S_2 \cdot S_3}\}$ e envia a M_5 o conjunto $\{g^{S_1 \cdot S_2 \cdot S_3 \cdot S_4}$, $g^{S_1 \cdot S_2 \cdot S_3}$, $g^{S_1 \cdot S_2 \cdot S_4}$, $g^{S_1 \cdot S_3 \cdot S_4}$, $g^{S_2 \cdot S_3 \cdot S_4}\}$. O conjunto enviado pelo i-ésimo participante é composto por i valores intermediários, cada um contendo $i - 1$ expoentes, e um valor cardinal contendo i expoentes, que corresponde à base da exponenciação elevada a todas as contribuições geradas até o momento.

O último participante (M_n) é denominado controlador do grupo e recebe um conjunto de dados cujo valor cardinal é $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}$. Com base neste valor é calculada a chave de grupo $K_n = g^{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1} \cdot S_n}$.

Na segunda etapa, o controlador do grupo acrescenta sua contribuição a cada um dos valores intermediários. Esta nova informação é então distribuída para todos os demais participantes. Cada participante M_i, calcula a chave de grupo utilizando o valor intermediário que lhe corresponde, ou seja, aquele que não possui sua contribuição. Este valor é

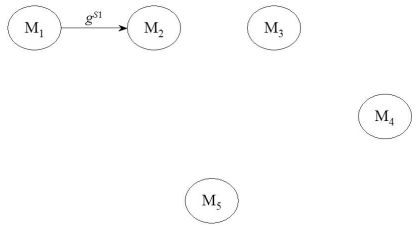
elevado à sua contribuição S_i e obtém-se $K_n = g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_n}{S_i} \cdot S_i}$.

2.5.2 IKA.2

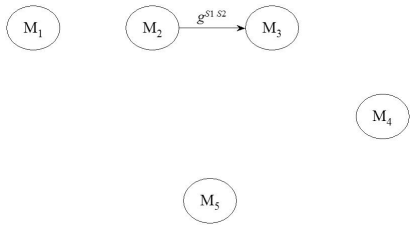
A execução do protocolo IKA.1 exige a realização pelo i-ésimo participante de $i + 1$ operações de exponenciação. Em alguns ambientes é desejável a minimização do esforço computacional exigido de cada participante para o estabelecimento da chave, como por exemplo em grupos com elevado número de participantes ou formados por equipamentos com limitado poder de processamento. Visando minimizar este esforço, foi proposto o protocolo IKA.2, que é conceitualmente similar, mas composto por quatro etapas:

1. $M_i \Rightarrow M_{i+1}\ ,\ i \in [1, n-2]\ :$
   - $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_i}$
2. $M_{n-1} \Rightarrow M_i\ ,\ i \in [1, n]\ :$
   - $g^{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}$
3. $M_i \Rightarrow M_n\ ,\ i \in [1, n-1]$:
   - $g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1}}{S_i}}$
4. $M_n \Rightarrow M_i\ ,\ i \in [1, n-1]$:
   - $\{g^{\frac{S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1} \cdot S_n}{S_i}} \mid i \in [1, n-1]\}$.

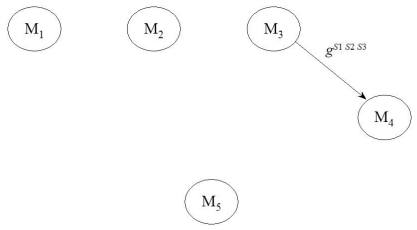
Na primeira etapa são coletadas as contribuições dos $n - 2$ primeiros membros do grupo, o que ocorre ao longo de $n - 2$ rodadas. A cada rodada um dos participantes recebe um conjunto de dados do participante que o antecedeu na execução do protocolo (Figura 2.4). Este conjunto de dados é composto apenas por um valor cardinal que possui a contribuição de todos os membros que o antecedem na execução do protocolo. O membro adiciona sua contribuição a este valor cardinal e repassa o novo valor ao próximo participante. Ao contrário do que ocorre durante a primeira etapa do protocolo IKA.1, o



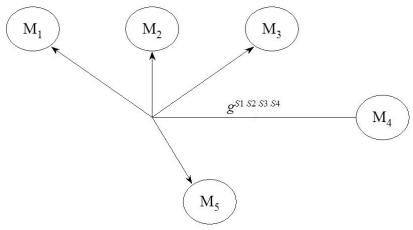
(a) 1^a etapa, 1^a rodada



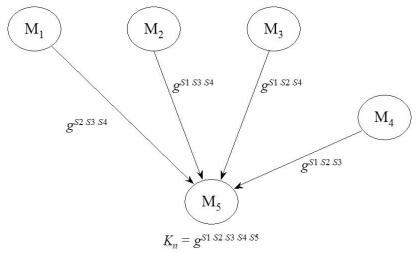
(b) 1^a etapa, 2^a rodada



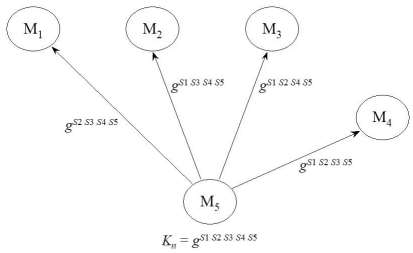
(c) 1^a etapa, 3^a rodada



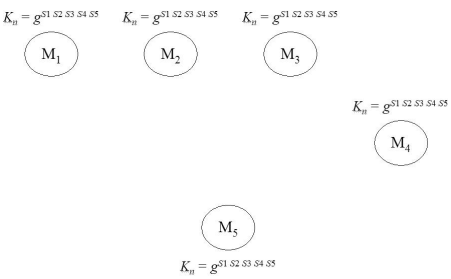
(d) 2^a etapa



(e) 3^a etapa



(f) 4^a etapa



(g) Finalização

Figura 2.4: Protocolo IKA.2 para n = 5.

conjunto de dados enviados possui tamanho fixo. O participante M_4, por exemplo, recebe o valor $g^{S_1 \cdot S_2 \cdot S_3}$ e envia a M_5 o valor $g^{S_1 \cdot S_2 \cdot S_3 \cdot S_4}$.

Na segunda etapa, o penúltimo participante (M_{n-1}) distribui a mensagem recebida, acrescida de sua colaboração, a todos os demais membros do grupo. O último membro, também denominado controlador do grupo, utiliza este valor para calcular a chave de grupo. Cada um dos $n-1$ primeiros membros retira então sua contribuição da mensagem recebida, por meio da elevação deste valor a S_i^{-1}, e envia este resultado para o controlador do grupo (terceira etapa). Para cada mensagem recebida, o controlador do grupo, eleva o valor recebido à sua colaboração S_n e envia o resultado de volta ao participante que o enviou (quarta etapa), permitindo assim que todos os participantes calculem a chave de grupo, elevando o valor recebido à sua contribuição.

Para os protocolos IKA.1 e IKA.2 a adição de membros ao grupo ocorre da seguinte forma: o participante a ser adicionado, denominado M_{n+1}, assume o papel de controlador do grupo, e é executada uma rodada da primeira etapa do protocolo por meio do envio de uma mensagem com as contribuições para a chave de grupo, mais uma contribuição aleatória, de M_n para M_{n+1}. São executadas então normalmente as demais etapas do protocolo utilizado, sendo assim gerada e distribuída uma nova chave de grupo.

Para a exclusão de membros do grupo, o controlador do grupo executa a última etapa do protocolo, acrescentando uma contribuição aleatória ao conjunto de dados previamente difundido e não difundindo desta vez o dado destinado ao membro excluído.

2.6 Comparação entre os protocolos

Dentre os protocolos apresentados, os protocolos BD, IKA.1 e IKA.2 necessitam distribuir dados a vários dispositivos. Não é especificado no entanto como estas distribuições devem ser realizadas. Duas possibilidades consistem na transmissão de dados por difusão natural (*broadcast*) ou por inundação (*flooding*). Estas transmissões, no entanto, normalmente utilizam protocolos de transporte não-confiáveis, não havendo portanto garantia de sucesso de entrega. Isto é crítico em redes ad hoc devido às suas características, que

incluem as maiores taxas de perda, a questão da conectividade dos dispositivos e a sobreposição dos sinais transmitidos por diferentes dispositivos, acarretando assim colisões, contenções e transmissões redundantes. Embora alguns trabalhos [25, 26] tenham sido desenvolvidos visando aliviar os problemas associados à difusão natural e à inundação de dados em redes sem fio ad hoc, nenhuma solução definitiva foi apresentada. Como em aplicações de segurança a confirmação da entrega dos dados transmitidos é fundamental, a distribuição destes dados deve ser realizada pela transmissão de várias mensagens do tipo ponto-a-ponto, entre o transmissor e cada um de seus receptores, utilizando um protocolo confiável de transporte.

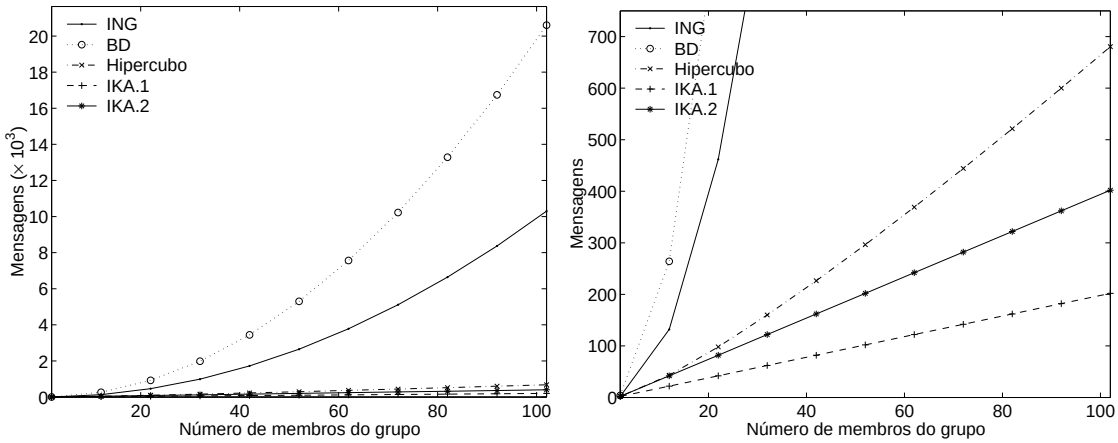
Calculou-se, para cada um dos protocolos de estabelecimento de chave de grupo apresentados, o número de mensagens ponto-a-ponto enviadas, a quantidade total de dados transmitidos, em função do tamanho da chave e o número total de operações de exponenciação efetuadas. A Tabela 2.1 apresenta estes valores e expõe se há necessidade de sincronismo entre os participantes no momento do envio de uma mensagem a outro participante. A Figura 2.5 expõe estes dados em forma gráfica.

	Mensagens	Dados transmitidos	Operações de exponenciação	Sincronismo
ING	$n^2 - n$	$n^2 - n$	n^2	Sim
BD	$2n^2 - 2n$	$2n^2 - 2n$	$n^2 - n$	Sim
Hipercubo	$n \cdot \log_2 n$	$n \cdot \log_2 n$	$2n \cdot \log_2 n$	Sim
IKA.1	$2n - 2$	$0.5n^2 + 1.5n - 3$	$0.5n^2 + 1.5n - 1$	Não
IKA.2	$4n - 5$	$4n - 5$	$5n - 6$	Não

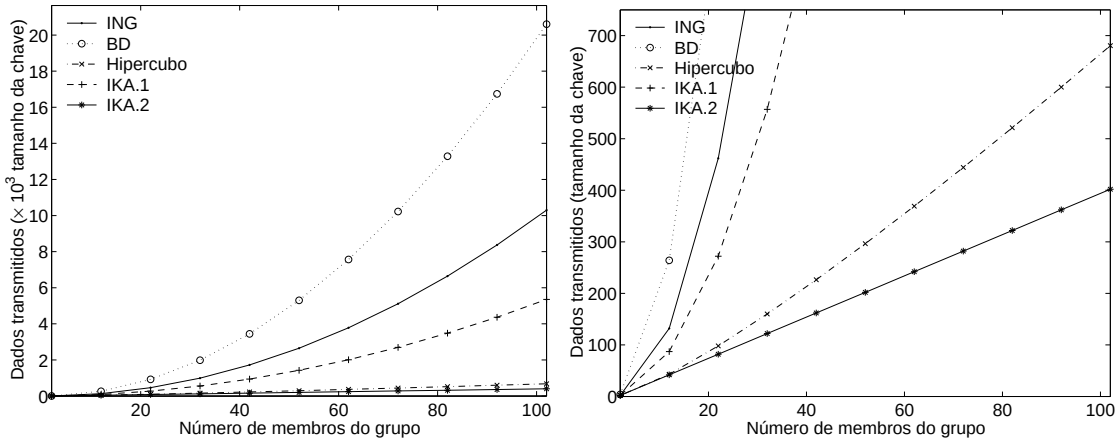
Tabela 2.1: Comparação entre os protocolos apresentados para estabelecimento de chave de grupo.

Os protocolos ING e BD são os mais custosos com relação às três métricas utilizadas, o que os torna pouco atraentes quando comparados aos demais protocolos apresentados.

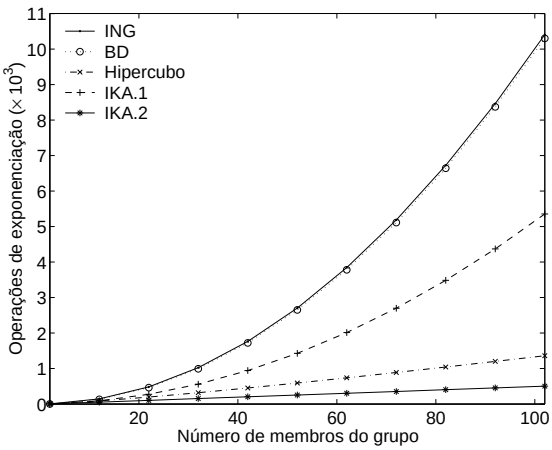
O protocolo Hipercubo necessita de sincronismo entre os participantes, de forma que uma rodada somente pode ser iniciada após a finalização da rodada anterior por todos os participantes. Isto implica na necessidade de um mecanismo sincronizador que garanta a



(a) Mensagens.



(b) Dados transmitidos.



(c) Operações de exponenciação.

Figura 2.5: Desempenho dos protocolos de estabelecimento de chave em função do número de participantes.

todos os participantes do estabelecimento da chave de grupo, a cada rodada, a informação de que todos os demais participantes receberam todas as mensagens enviadas a eles. A utilização deste tipo de mecanismo implica em uma sobrecarga a nível de tempo e de número de mensagens que varia em função do complexidade do mecanismo sincronizador utilizado.

Os protocolos IKA.1 e IKA.2 apresentam algumas vantagens, como a execução por um número arbitrário de participantes, o estabelecimento da seqüência em que ocorrem as contribuições durante a execução do protocolo e a possibilidade de adição e exclusão de membros do grupo sem a necessidade de execução de todo o protocolo de estabelecimento da chave.

A comparação entre os protocolos Hipercubo e IKA.2, com relação às três métricas apresentadas, permite perceber que o protocolo IKA.2 apresenta sempre o menor custo de execução. A inclusão de um mecanismo sincronizador, conforme mencionado, prejudicaria ainda mais o desempenho do protocolo Hipercubo. Este protocolo apresenta ainda o inconveniente de necessitar de um número específico de participantes, conforme exposto na Seção 2.4. A utilização de sua variante, o protocolo Octopus, resolve o problema do número de participantes, mas gera um atraso para o início da execução do estabelecimento da chave de grupo entre os participantes de núcleo.

O protocolo IKA.1 também apresenta algumas desvantagens como o crescimento quadrático da quantidade de dados enviados e do número de operações de exponenciação realizadas, prejudicando sua escalabilidade à medida que o número de participantes cresce. Esta característica torna seu desempenho pior com relação a estas métricas que os desempenhos dos protocolos Hipercubo e IKA.2, sendo mais vantajoso somente com relação ao número de mensagens transmitidas.

Com base nestas informações, o protocolo IKA.2 apresenta-se como o mais vantajoso dentre os protocolos apresentados. Embora o protocolo IKA.1 não seja tão eficiente com relação à quantidade de dados transmitidos e ao número de operações de exponenciação realizadas, sua utilização como uma alternativa ao IKA.2 pode ser interessante, uma vez que ele é mais eficiente com relação ao número de mensagens transmitidas e ambos pertencem à mesma família de protocolos, compartilhando a forma da chave criptográfica

utilizada. Assim, eventuais alterações da chave de grupo podem ocorrer ora por um protocolo ora pelo outro. Isto pode ser vantajoso, pois executar a etapa 2 do protocolo IKA.1 para acrescentar membros ao grupo é mais eficiente do que executar as etapas 2, 3 e 4 do protocolo IKA.2.

2.6.1 Algumas observações sobre os protocolos IKA.1 e IKA.2

Embora os protocolos IKA.1 e IKA.2 aparentem possuir um caráter centralizador, pois apenas o controlador do grupo é responsável pela distribuição das informações, isto não é verdadeiro, pois as funções do controlador do grupo são naturalmente designadas a outro dispositivo quando algum membro é adicionado ao grupo, ou caso o controlador do grupo torne-se indisponível.

A execução dos protocolos IKA.1 e IKA.2 pode ser dividida em dois estágios: um primeiro estágio de coleta de contribuições, que ocorre na primeira etapa de cada protocolo; e um segundo estágio no qual estas colaborações são distribuídas a todos os membros do grupo. Este segundo estágio corresponde à segunda etapa do protocolo IKA.1 e às segunda, terceira e quarta etapas do protocolo IKA.2.

Com relação ao número de mensagens transmitidas, o protocolo IKA.1 transmite $n-1$ mensagens no primeiro estágio, todas entre um dispositivo e o próximo da seqüência de contribuições, e $n-1$ mensagens no segundo estágio, entre o n-ésimo dispositivo e todos os demais. Já o protocolo IKA.2 necessita de cerca do dobro do número de mensagens, que são distribuídas da seguinte forma: $n-2$ mensagens no primeiro estágio, entre um dispositivo e o próximo da seqüência de contribuições e $3n-3$ mensagens no segundo estágio, entre os dois últimos membros do grupo e todos os demais, um número três vezes maior que o transmitido pelo protocolo IKA.1 no seu segundo estágio. Esta característica do protocolo IKA.2 pode prejudicar seu desempenho, com relação àquele do protocolo IKA.1, quando o custo de transmissão de mensagens for alto, devido aos fatores apresentados na seção seguinte.

Capítulo 3

Análise de desempenho

AS análises dos protocolos realizadas na Seção 2.6 não consideram importantes fatores que são encontrados em comunicações reais de redes de computadores. Um destes fatores é o encaminhamento das mensagens através de outros dispositivos da rede, realizando múltiplos saltos. A análise da Seção 2.6 considera a transmissão de apenas uma mensagem na transferência de uma informação de um dispositivo A para um dispositivo B. Em um um caso real, se esta transferência requerer s saltos, a quantidade total de dados transmitidos é s vezes maior que a inicialmente prevista. Um outro fator que é muito importante em redes ad hoc é a conectividade dos dispositivos, pois em redes ad hoc móveis alguns dispositivos podem estar momentaneamente indisponíveis, impedindo o estabelecimento da chave de grupo. Como a conectividade depende do número de dispositivos que compõem a rede, do tamanho da área sobre a qual estes dispositivos estão distribuídos e de sua mobilidade, uma das medidas de desempenho a ser obtida é a taxa de sucesso no estabelecimento da chave de grupo em função destes parâmetros. Além da conectividade, outros fatores que influenciam o desempenho do estabelecimento de chave de grupo em redes ad hoc são os protocolos de acesso ao meio e de roteamento. Visando considerar estes fatores, a análise do desempenho dos protocolos de estabelecimento de chave IKA.1 e IKA.2 foi realizada por simulação.

3.1 Ambiente de simulação

O ambiente de simulação utilizado foi o ns-2 (*Network Simulator* 2) [27], que é um simulador de serviços e de protocolos de rede. Esse simulador encontra-se em desenvolvimento dentro do projeto *Virtual InterNet Testbed* (VINT), uma colaboração entre a Universidade da Califórnia em Berkeley, o *Lawrence Berkeley National Laboratory* (LBL), o *Information Sciences Institute* (ISI) da Universidade da Califórnia do Sul (USC) e o laboratório Xerox PARC. O ns-2 utiliza as linguagens C++ e OTcl (*Object Tool Command Language*), sendo o seu núcleo implementado em C++, para permitir um melhor desempenho. As simulações executadas são configuradas através de *scripts* OTcl que descrevem, a topologia, o cenário de mobilidade, os protocolos e as aplicações a serem simuladas. A estrutura de um nó da rede no ns-2 é composta de agentes, um ponto de entrada no nó, um classificador de endereços e um classificador de portas. Os agentes são entidades produtoras ou consumidoras de pacotes e implementam determinados tipos de protocolos. Um pacote gerado por um agente é entregue ao nó ao qual o agente está ligado, através do ponto de entrada, que também recebe pacotes cujo destino é o próprio nó. Após passar pelo ponto de entrada, o pacote é recebido pelo classificador de endereços, que verifica se o pacote deve ser entregue a um agente pertencente ao nó ou deve ser transmitido para um enlace de saída. Caso o pacote seja destinado a um agente do próprio nó, o pacote é então repassado ao classificador de porta que, de acordo com o endereço de destino, entrega o pacote ao respectivo agente.

Os dispositivos sem fio simulam o padrão IEEE 802.11 e possuem um raio de alcance de 250 metros. O protocolo de roteamento DSR (*Dynamic Source Routing*) [28] é utilizado para prover as rotas entre os dispositivos. Este é um protocolo de roteamento sob demanda, de forma que as rotas entre os dispositivos somente são estabelecidas na medida em que há necessidade. Todas as simulações tiveram duração de 1000 segundos, por ser este valor bem maior que os maiores tempos de execução observados, conforme apresentado a seguir.

Foi realizada a implementação dos protocolos IKA.1 e IKA.2 no ns-2. As seqüências em que ocorrem as contribuições são definidas com base nos identificadores dos dispositivos, em ordem crescente a partir do dispositivo com menor identificador, até que o último

dispositivo do grupo seja alcançado. O tamanho estabelecido para a chave de grupo foi de 256 bits, por se tratar de um valor que proporciona um forte nível de segurança para os padrões atuais.

Devido a fatores como a alta probabilidade de perda de pacotes no ambiente sem fio e à possibilidade de indisponibilidade temporária dos dispositivos que compõem a rede, é necessário que as informações transmitidas entre os dispositivos utilizem um protocolo de transporte confiável. O protocolo mais utilizado em redes tradicionais que atende a este critério é o protocolo TCP (*Transmission Control Protocol*). No entanto, diversos estudos [29, 30, 31, 32] apontam o TCP como um protocolo inapropriado para utilização em redes sem fio. A principal razão consiste no fato de o TCP interpretar perdas de pacotes devido a erros de transmissão como perdas devido a congestionamento da rede. Isto ativa o mecanismo de controle de congestionamento do TCP e gera um comportamento instável de constante alteração do tamanho da janela de congestionamento, levando a grandes variações da vazão disponível e prejudicando assim o desempenho das transmissões. Embora alguns estudos [33, 34] apresentem propostas de adaptações do TCP para redes sem fio, não há ainda um padrão estabelecido.

Algumas simulações foram realizadas utilizando-se o protocolo TCP e foi possível constatar uma grande instabilidade no seu comportamento sobre o ambiente sem fio. Com o objetivo de avaliar os protocolos de estabelecimento de chave de grupos sem a influência dos problemas gerados pela utilização do protocolo TCP foi implementado um protocolo simples de transporte confiável. O funcionamento deste protocolo é o seguinte: os dados são enviados em pacotes de tamanho máximo de 1000 bytes, que é o tamanho máximo padrão de pacotes no ns-2. Caso seja solicitado o envio de um pacote que exceda este tamanho ele é fragmentado em pacotes menores. Ao receber um pacote, o dispositivo destino envia um pacote de reconhecimento de 5 bytes para o dispositivo fonte. O dispositivo fonte, ao receber o pacote de reconhecimento, tem a confirmação do sucesso da transmissão. O próximo pacote a ser transmitido é então enviado. Caso o pacote de reconhecimento não seja recebido em 5 segundos o pacote de dados é retransmitido. Este valor de 5 segundos foi observado como o tempo máximo para ida e volta para dispositivos capazes de estabelecer comunicação nos cenários simulados. Ao contrário do que ocorre com o protocolo TCP, não há transmissão adiantada de pacotes, não havendo por-

tanto a possibilidade de desordenação dos dados. Por se basear nos princípios básicos de um protocolo de transporte confiável, este protocolo pode ser utilizado sem perda de generalidade.

Foram calculadas margens de erro com intervalos de confiança de 95% relativos às médias das medidas. Estas margens de erro são representadas nos gráficos por barras verticais.

3.2 Dispositivos aleatoriamente distribuídos

Os cenários de movimentação dos dispositivos que compõem a rede ad hoc foram gerados utilizando-se a ferramenta "setdest", que se serve do modelo *Random Waypoint* de mobilidade. Neste modelo, todos os dispositivos móveis são posicionados aleatoriamente segundo uma distribuição uniforme em uma área especificada. Cada dispositivo escolhe então uma posição destino, também aleatória segundo uma distribuição uniforme, dentro da área de simulação e movimenta-se até esta posição em linha reta com uma velocidade constante de valor aleatoriamente distribuído entre zero e a velocidade máxima especificada. Ao alcançar o destino, o dispositivo permanece parado durante um tempo de pausa especificado e então se movimenta para outro destino. Este procedimento se repete para todos os dispositivos simulados até que o final da simulação seja alcançado. Visando avaliar a influência da movimentação dos dispositivos a determinada velocidade, foi feita uma modificação no modelo *Random Waypoint* de modo a ser especificada uma velocidade nominal, e não mais uma velocidade máxima. Assim, a velocidade dos dispositivos móveis é aproximadamente constante com uma tolerância, para mais ou para menos, de 10%. Esta mudança no modelo requeriu modificações na ferramenta setdest.

3.2.1 Área menor que o alcance de transmissão

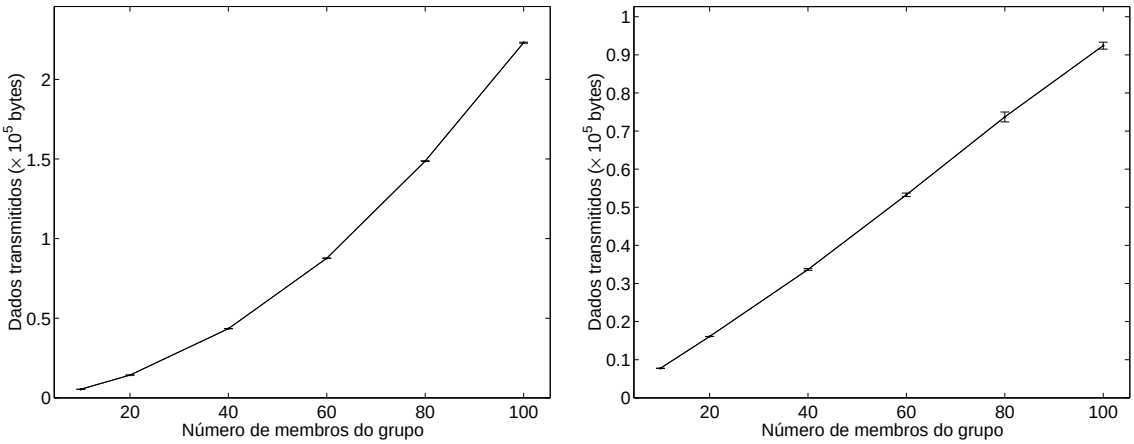
Com o objetivo de se avaliar o comportamento dos protocolos IKA.1 e IKA.2 em cenários sem problemas de conectividade, estes protocolos foram simulados em cenários com áreas quadradas com tamanho fixo de 150 metros de lado, de forma que todos os

dispositivos estivessem sempre dentro do alcance de transmissão de todos os demais, evitando assim problemas de conectividade. Este tipo de cenário representa dispositivos que estão contidos em um mesmo ambiente, como por exemplo, pessoas em uma reunião, uma palestra, ou uma festa.

Um dos parâmetros de desempenho avaliados é a taxa de sucesso no estabelecimento da chave de grupo. A taxa de sucesso é calculada dividindo-se o número de simulações que obtiveram sucesso no estabelecimento da chave de grupo pelo número total de simulações realizadas. Conforme esperado, a taxa de sucesso em todos os casos foi de 100% para ambos os protocolos. A total conectividade da rede permitiu, portanto, sucesso em todas as tentativas de estabelecimento da chave de grupo.

As simulações foram realizadas inicialmente para dispositivos parados. A Figura 3.1 expressa a quantidade de dados transmitidos durante a execução dos protocolos de estabelecimento de chave de grupo em função do número de membros do grupo. À medida que o número de membros do grupo cresce, aumenta a quantidade de dados transmitidos, conforme esperado (Tabela 2.1 e Figura 2.5(b)). A análise desta figura permite perceber, no entanto, que para um grupo de, por exemplo, 100 dispositivos, o protocolo IKA.1 necessitou transmitir uma quantidade de dados cerca de 2.4 vezes maior que o protocolo IKA.2, enquanto a diferença esperada era de cerca de 13 vezes. Foi observado que esta discrepância ocorreu devido aos cabeçalhos adicionados aos dados no momento de sua transmissão. Como no protocolo IKA.2 todas as mensagens possuem tamanho fixo, o percentual de sobrecarga (*overhead*) dos cabeçalhos nestas mensagens é o mesmo para todas as mensagens. Já para o protocolo IKA.1 este percentual diminui à medida que a primeira etapa do protocolo é executada, pois as mensagens crescem de tamanho com a execução do protocolo e os cabeçalhos apresentam tamanhos constantes. Assim, a diferença de desempenho entre os protocolos IKA.1 e IKA.2 segundo a métrica da quantidade de dados enviados é menor que a prevista analiticamente.

Este tipo de cenário foi também simulado com dispositivos movimentando-se a velocidades em torno de 1 m/s, de modo a avaliar a influência da mobilidade dos dispositivos. Os resultados foram iguais àqueles obtidos com os dispositivos parados. Percebe-se portanto que em cenários nos quais todos os dispositivos estão sob o alcance de transmissão



(a) IKA.1. (b) IKA.2.

Figura 3.1: Dados transmitidos pelo protocolo de estabelecimento de chave para dispositivos parados.

de todos os demais a mobilidade ou não destes dispositivos é indiferente, pois não há alteração da topologia da rede.

3.2.2 Múltiplos saltos

Visando avaliar a influência do espaçamento entre os dispositivos sobre o desempenho dos protocolos IKA.1 e IKA.2, foram realizadas simulações com diferentes densidades de dispositivos, representadas pelo número de dispositivos por área. A relação entre o número d de dispositivos, a área S sobre a qual estes dispositivos estão distribuídos e a densidade ρ de dispositivos é dada por $d = \rho \cdot S$. Diferentes valores de densidade poderiam portanto ser escolhidos variando-se o número de dispositivos presentes em uma área fixa ou o tamanho da área de simulação para um número fixo de dispositivos. A primeira abordagem apresenta um inconveniente, pois com a variação do número de dispositivos não é possível distinguir se os resultados observados são conseqüências da variação do número de dispositivos, conforme previsto pela Tabela 2.1 e pela Figura 2.5, ou da variação da densidade de dispositivos.

Para se obter diferentes densidades, utilizou-se portanto a segunda abordagem, variando-se a área quadrada de simulação em função do número de dispositivos. As densidades

utilizadas foram $(0,2\ R)^{-2}$, $(0,4\ R)^{-2}$, $(0,6\ R)^{-2}$, $(0,8\ R)^{-2}$ e R^{-2}, onde R é o raio de alcance dos dispositivos. Assim, para o raio de alcance utilizado nas simulações, de 250 metros, estas densidades correspondem respectivamente a 50^{-2}, 100^{-2}, 150^{-2}, 200^{-2} e 250^{-2} dispositivos por metro quadrado. A razão pela qual as densidades estão expressas nesta forma, por exemplo, 50^{-2} dispositivos por metro quadrado, é para transmitir a noção de que há, em média, uma área quadrada com 50 metros de lado para cada dispositivo. A representação desta densidade como 0,0004 dispositivos por metro quadrado não transmite esta noção.

A Tabela 3.1 apresenta as áreas de simulação utilizadas em função das densidades de dispositivos e do número de dispositivos.

Dens. \ Num. disp.	20	40	60	80	100
$(0,2\ R)^{-2}$	223	316	387	447	500
$(0,4\ R)^{-2}$	447	632	774	894	1000
$(0,6\ R)^{-2}$	670	948	1161	1341	1500
$(0,8\ R)^{-2}$	894	1264	1549	1788	2000
R^{-2}	1118	1581	1936	2236	2500

Tabela 3.1: Tamanho, em metros, dos lados das áreas quadradas de simulação utilizadas em função das densidades de dispositivos por área e do número de dispositivos simulados.

Os protocolos IKA.1 e IKA.2 foram simulados inicialmente para cenários sem movimentação. A Figura 3.2 apresenta as taxas de sucesso obtidas com a execução dos protocolos em função do número de membros que compõem o grupo, para diferentes densidades de dispositivos.

Percebe-se que à medida que a densidade de dispositivos diminui, aumentando o espaçamento entre estes dispositivos, há uma diminuição das taxas de sucesso obtidas devido à diminuição da conectividade da rede. Para as densidades de $(0,2\ R)^{-2}$ e $(0,4\ R)^{-2}$ a conectividade da rede é alta de forma que o estabelecimento da chave de grupo se dá sempre com sucesso. Para a densidade de $(0,6\ R)^{-2}$ a taxa de sucesso é mais baixa, mas este valor pode ser considerado aceitável em algumas aplicações. Para as densidades de $(0,7\ R)^{-2}$, $(0,8\ R)^{-2}$ e R^{-2}, as taxas de sucesso são muito baixas, tornando inviável a

execução dos protocolos.

A observação desta figura permite ainda perceber que, para uma dada densidade, à medida que o número de dispositivos aumenta, a taxa de sucesso no estabelecimento da chave de grupo diminui. Isto se deve ao aumento da área em função do aumento do número de dispositivos. Ainda que estas duas grandezas aumentem juntas, observa-se que em uma área maior aumenta a probabilidade de haver pelo menos um dispositivo incapaz de se comunicar com os demais, impedindo a finalização do protocolo e prejudicando assim o desempenho dos protocolos à medida que o número de participantes do grupo cresce.

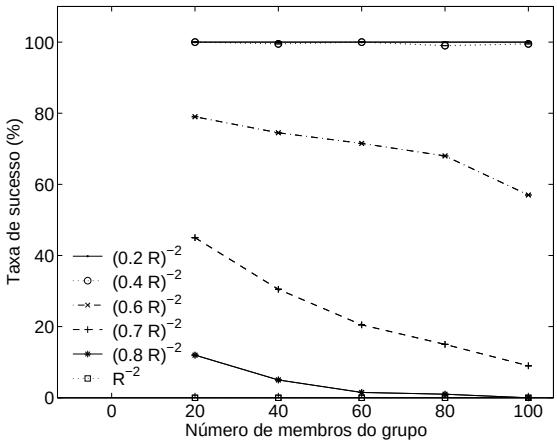
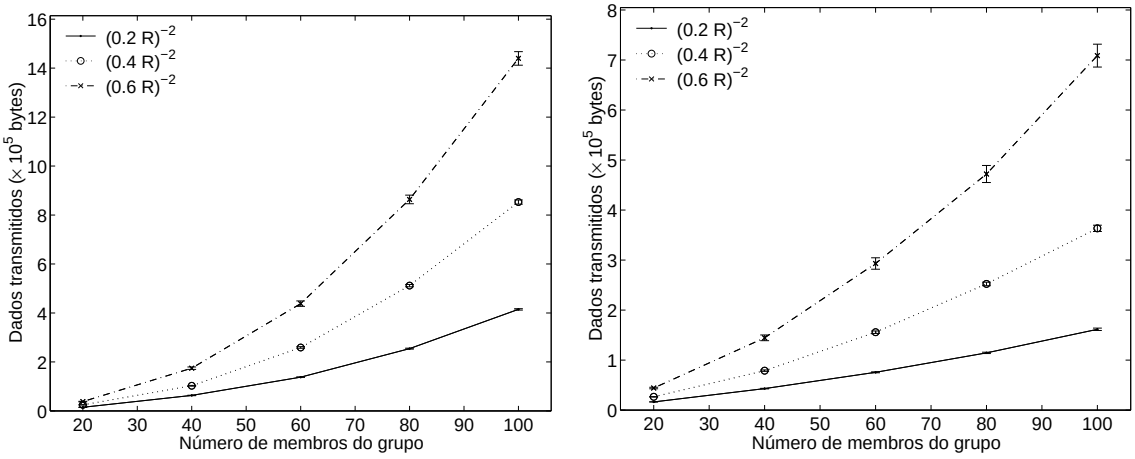


Figura 3.2: Taxa de sucesso para dispositivos parados (IKA.1 e IKA.2).

A Figura 3.3 expressa a quantidade de dados transmitidos pelos protocolos de estabelecimento de chave em função do número de membros do grupo, para diferentes densidades de dispositivos. São apresentados apenas os resultados referentes às densidades para as quais o estabelecimento da chave de grupo foi viável, ou seja, $(0,2\ R)^{-2}$, $(0,4\ R)^{-2}$ e $(0,6\ R)^{-2}$. Para uma dada densidade, à medida que o número de membros do grupo cresce, aumenta a quantidade de dados transmitidos, conforme esperado. Nota-se no entanto que para o protocolo IKA.2 este crescimento é mais acentuado que o crescimento linear previsto (Tabela 2.1 e Figura 2.5(b)) e que o crescimento observado para dispositivos dentro de uma área pequena (Figura 3.1). Isto se deve à transmissão dos dados por múltiplos saltos, de modo que a cada salto é gerada uma nova mensagem, que é encaminhada ao destino, elevando assim a quantidade de dados transmitidos na rede.

Percebe-se ainda que, à medida que a densidade de dispositivos diminui, há um aumento da quantidade de dados transmitidos. Isto se deve ao maior espaçamento entre os dispositivos, o que aumenta o número de saltos necessários para que uma mensagem transmitida alcance seu destino. Vale notar que a ordem em que os dispositivos participam do estabelecimento da chave de grupo no primeiro estágio de ambos os protocolos se baseia no identificador destes dispositivos, ou seja, o dispositivo 1 envia uma mensagem ao dispositivo 2, que envia ao 3, e assim por diante até que o dispositivo $n - 1$ envie ao n. Assim, devido à distribuição uniforme dos dispositivos pela área de simulação é provável que as mensagens sejam desordenadamente transmitidas pela rede, como ilustrado pela Figura 3.4. Se neste exemplo cada dispositivo está posicionado de forma a se comunicar diretamente apenas com seus vizinhos, então um total de 11 saltos é necessário, ao invés de apenas 5 como inicialmente esperado. Devido a esta ordem como ocorrem as contribuições, um aumento do número de saltos pode gerar portanto um total de dados transmitidos significativamente maior. Percebe-se que a diminuição da densidade de dispositivos de $(0,2\ R)^{-2}$ para $(0,4\ R)^{-2}$ levou à transmissão de cerca do dobro da quantidade de dados. Para uma densidade de $(0,6\ R)^{-2}$ a quantidade de dados transmitidos é um pouco maior que o triplo do necessário com uma densidade de $(0,2\ R)^{-2}$.



(a) IKA.1.

(b) IKA.2.

Figura 3.3: Dados transmitidos pelo protocolo de estabelecimento de chave para dispositivos parados.

Foi também observada a quantidade de dados de roteamento enviados durante a exe-

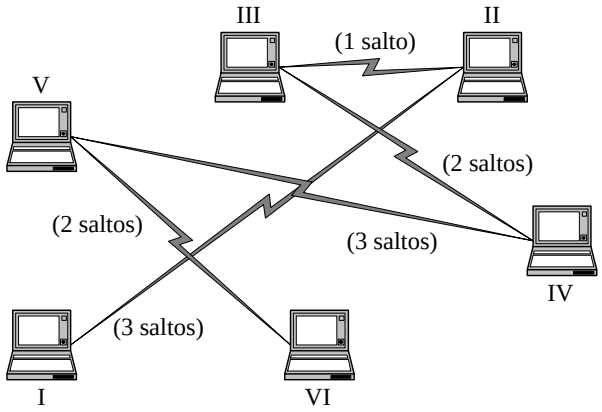
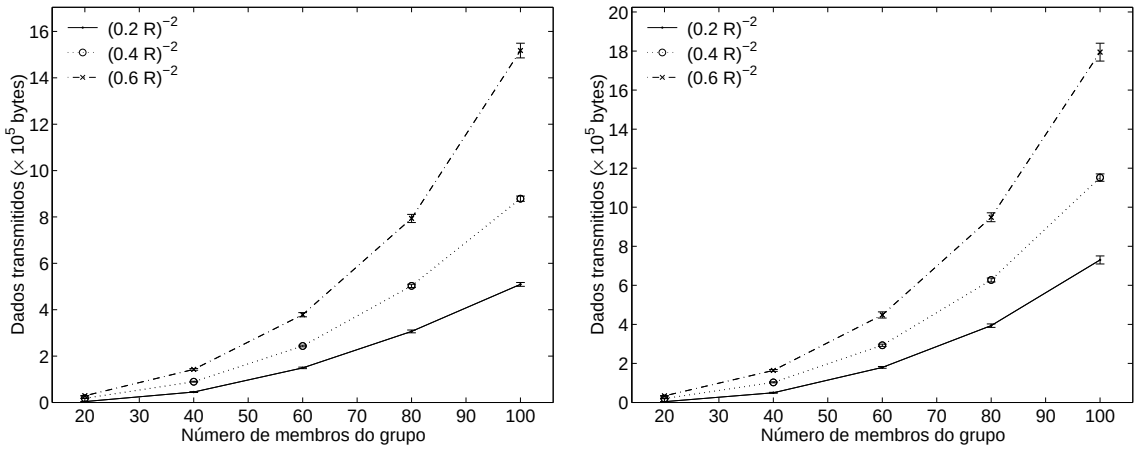


Figura 3.4: Exemplo de uma seqüência de contribuições que necessita de vários saltos.

cução dos protocolos de estabelecimento de chave, que é apresentada na Figura 3.5. Assim como ocorrido para as quantidades de dados transmitidos pelos protocolos IKA.1 e IKA.2, houve um aumento dos dados de roteamento em função da diminuição da densidade de dispositivos. Percebe-se que o protocolo IKA.2 gerou a transmissão de uma maior quantidade de informações de roteamento que o protocolo IKA.1, o que se deve ao maior número de conexões ponto-a-ponto realizadas durante o seu segundo estágio de execução. A quantidade de dados transmitidos pelos protocolos IKA.1 e IKA.2 em todas as situações foi menor que a quantidade de dados de roteamento transmitidos. Isto indica um custo relativamente baixo de execução dos protocolos IKA.1 e IKA.2, com relação à quantidade de dados transmitidos, pois é mais baixo que o custo do estabelecimento de rotas entre os dispositivos deste grupo, o que é uma tarefa indispensável ao funcionamento da rede.

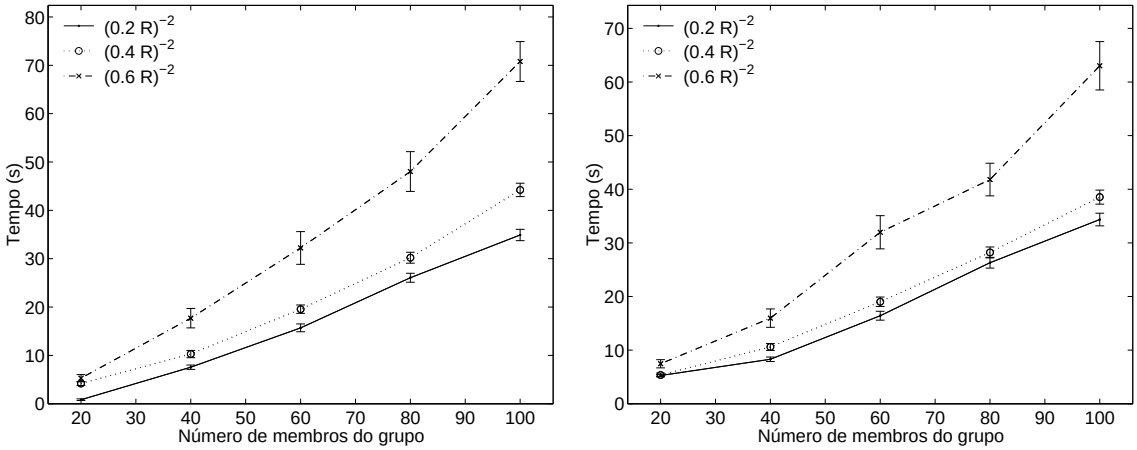
A Figura 3.6 expressa o tempo de execução dos protocolos de estabelecimento de chave em função do número de membros do grupo, para diferentes densidades de dispositivos. O tempo de execução é o tempo decorrido desde o início da execução do protocolo até o instante em que todos os participantes possuem a chave de grupo. Estes tempos também elevaram-se em função do aumento do número de membros do grupo e da diminuição da densidade de dispositivos por área. Percebe-se um aumento das barras de erro obtidas para a densidade de $(0,6\ R)^{-2}$ com relação às demais densidades, o que se deve ao menor número de amostras utilizadas no calculo da média e da margem de erro,



(a) IKA.1. (b) IKA.2.

Figura 3.5: Dados de roteamento transmitidos para dispositivos parados.

pois as taxas de sucesso alcançadas foram mais baixas.



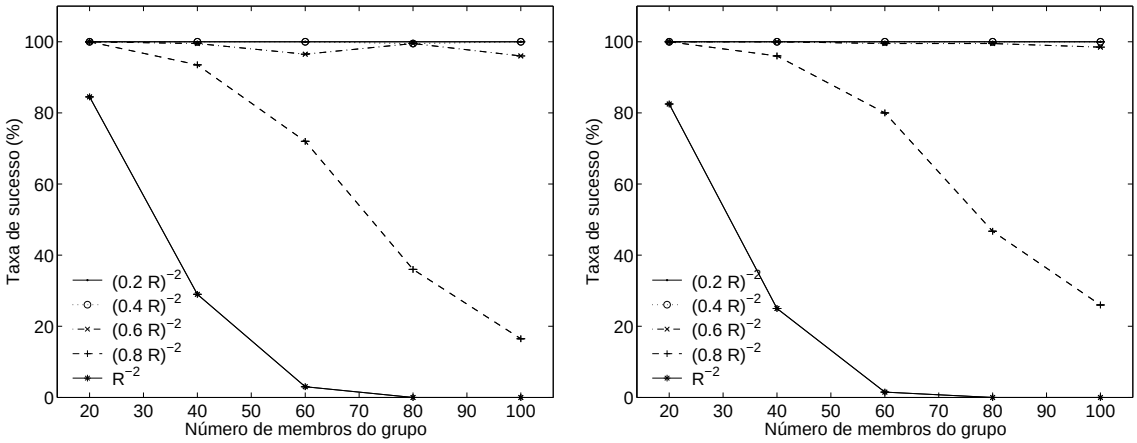
(a) IKA.1. (b) IKA.2.

Figura 3.6: Tempo de execução para dispositivos parados.

Com o objetivo de avaliar a influência da mobilidade sobre o desempenho dos protocolos IKA.1 e IKA.2, estes protocolos foram simulados em cenários com constante movimentação dos dispositivos a velocidades em torno de 1 m/s.

As taxas de sucesso alcançadas com ambos os protocolos são apresentadas na Figura 3.7. Houve uma melhora do desempenho com relação aos dispositivos parados. Para uma densidade de $(0,6\ R)^{-2}$ esta taxa elevou-se de valores entre 60% e 80% (Figura 3.2)

para próximo de 100%. Para densidades mais baixas, também houve melhora, mas o estabelecimento da chave de grupo ainda apresenta-se inviável para um maior número de dispositivos. A movimentação dos dispositivos favorece portanto a o estabelecimento da chave de grupo, pois a freqüente modificação da topologia, por meio da quebra e criação de enlaces, aumenta a probabilidade de que um dado dispositivo, que esteja afastado dos demais, seja eventualmente capaz de se comunicar com os outros. Ainda que a mobilidade leve alguns dispositivos se afastem dos demais, as dimensões restritas da área de simulação tende a fazer com que eles se reaproximem.

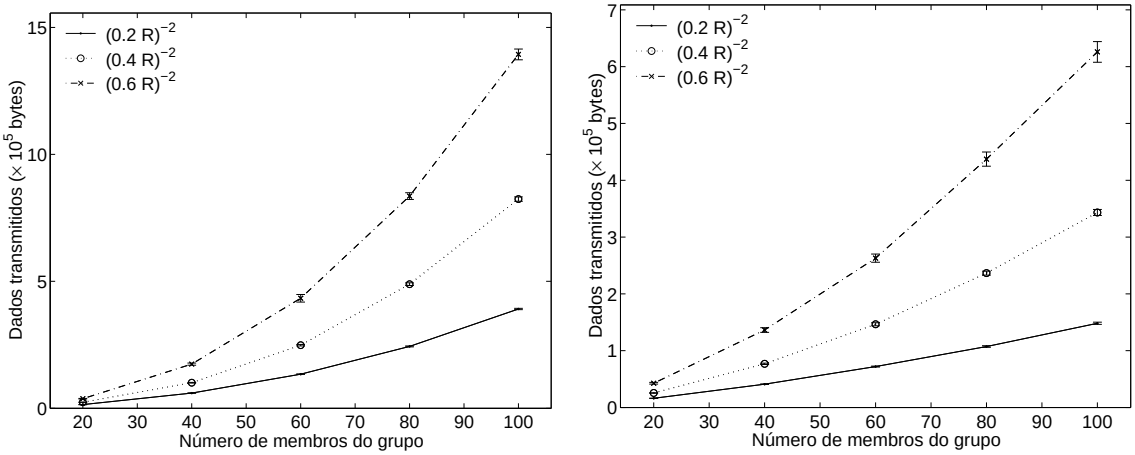


(a) IKA.1. (b) IKA.2.

Figura 3.7: Taxa de sucesso para dispositivos movimentando-se a 1 m/s.

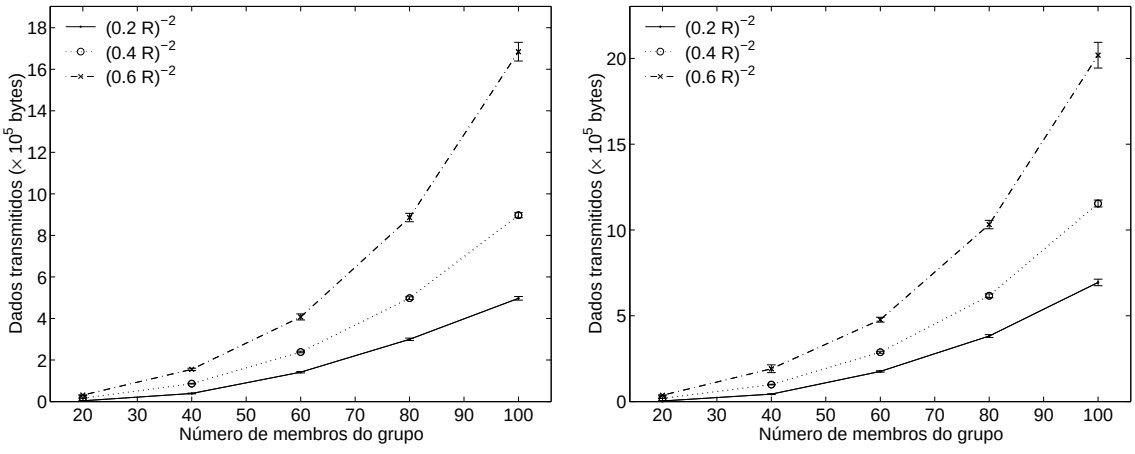
Na Figura 3.8 são expressas as quantidades de dados transmitidos por ambos os protocolos. A comparação com o desempenho obtido com dispositivos parados (Figura 3.3) permite perceber que os resultados foram equivalentes para ambas as situações. Com relação aos dados de roteamento transmitidos (Figura 3.9), para as densidades de $(0,4\ R)^{-2}$ e $(0,6\ R)^{-2}$ houve um aumento de cerca de 10%, com relação aos cenários com dispositivos parados, devido às alterações da topologia causadas pela mobilidade. Para a densidade de $(0,2\ R)^{-2}$ a quantidade de dados de roteamento transmitidos se manteve aproximadamente igual àquela transmitida para o caso de dispositivos parados, pois a mobilidade praticamente não causou alterações na topologia da rede.

A Figura 3.10 apresenta os tempos de execução dos protocolos sob estas condições. Para a densidade de $(0,6\ R)^{-2}$, o tempo de execução para ambos os protocolos é prati-



(a) IKA.1. (b) IKA.2.

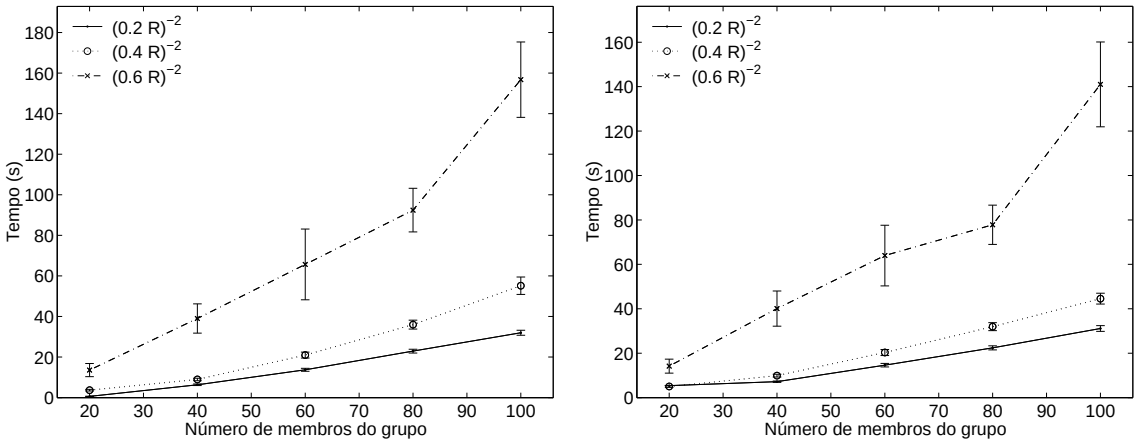
Figura 3.8: Dados transmitidos pelo protocolo de estabelecimento de chave para dispositivos movimentando-se a 1 m/s.



(a) IKA.1. (b) IKA.2.

Figura 3.9: Dados de roteamento transmitidos para dispositivos movimentando-se a 1 m/s.

camente duplicado. Isto se deve ao aumento dos casos de sucesso no estabelecimento da chave, ou seja, dispositivos que estavam afastados e assim impediriam a finalização do protocolo se movimentam, permitindo o estabelecimento da chave de grupo. Como conseqüência, o tempo de estabelecimento para estes casos é alto, levando a uma elevação da média obtida e ao aumento das barras de erro com relação aos cenários sem mobilidade. Para a densidade de $(0,4\ R)^{-2}$, o tempo necessário ao estabelecimento da chave de grupo também aumenta com relação aos cenários sem mobilidade, mas a um nível mais baixo. Como a conectividade da rede para este valor de densidade é alto mesmo sem mobilidade, o aumento do tempo de execução foi devido a fatores como a perda de alguns enlaces e a criação de novos enlaces, o que leva à execução dos procedimentos de descoberta de rota do protocolo de roteamento. Para uma densidade de $(0,2\ R)^{-2}$ as quebras de enlace são menos freqüentes, havendo manutenção dos tempos de execução.



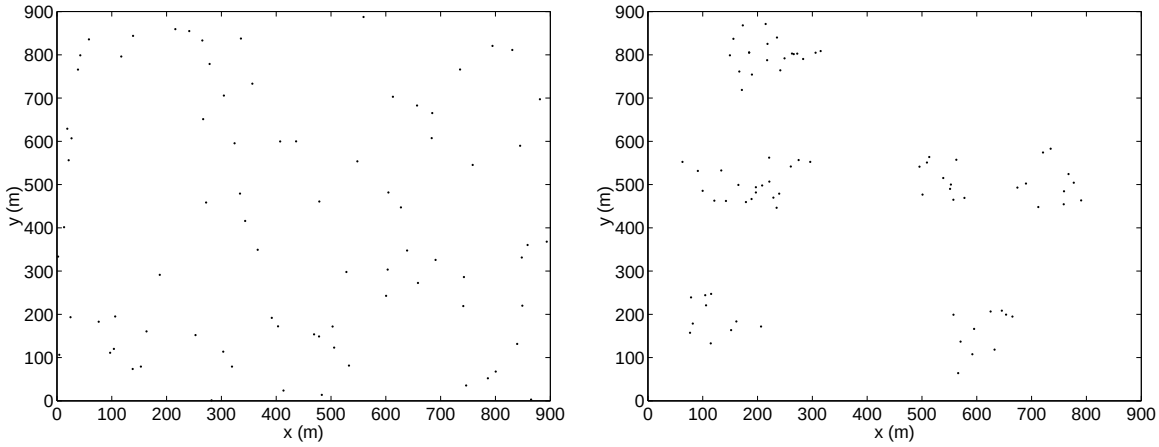
(a) IKA.1. (b) IKA.2.

Figura 3.10: Tempo de execução para dispositivos movimentando-se a 1 m/s.

3.3 Dispositivos aglomerados em subgrupos

O modelo de movimentação *Random Waypoint* é considerado muito genérico e distante de uma aplicação real. Isto deve-se em parte ao modo como ocorrem as movimentações, pois cada dispositivo se move de forma completamente independente dos demais. Assim, foi utilizada a ferramenta “scengen” [35], que gera padrões de movimentação em

grupos. Esta ferramenta possui alguns modelos de movimentação e permite especificar dentro da área de simulação áreas menores capazes de se mover segundo algum destes modelos. Assim, em vez de os dispositivos se movimentarem aleatoriamente, grupos de dispositivos se movem de forma aleatória. Os dispositivos contidos nestas áreas também seguem um dos modelos de mobilidade dentro da sua área. Este modelo de grupos é mais apropriado para representar determinadas aplicações como, por exemplo, uma operação militar onde os grupos seriam os pelotões. Nos cenários utilizados, tanto os grupos como um todo, bem como cada participante do grupo, movimentam-se segundo o modelo *Random Waypoint* e todos os grupos são compostos por 10 dispositivos. A área definida para cada um destes grupos é de 150 por 150 metros, de modo que todos os dispositivos que participam de um mesmo grupo são mutuamente alcançáveis. A Figura 3.11 expõe as diferenças entre os dois tipos de cenário para uma mesma quantidade de dispositivos móveis e uma mesma área. De forma a não causar equívoco com o grupo de dispositivos que busca estabelecer a chave criptográfica secreta, o termo "subgrupo" é utilizado para se referir aos conjuntos de dispositivos que se movimentam em grupos.



(a) Dispositivos aleatoriamente posicionados.

(b) Dispositivos aglomerados em subgrupos.

Figura 3.11: Exemplos dos dois modelos de movimentação adotados (80 dispositivos, densidade de $(0{,}4\ R)^{-2}$).

Os protocolos IKA.1 e IKA.2 foram simulados em cenários com aglomeração em subgrupos, estando inicialmente os dispositivos parados. Observa-se que as taxas de sucesso obtidas, apresentadas pela Figura 3.12, são mais baixas que aquelas obtidas nos cenários

sem subgrupos. Este pior desempenho deve-se à concentração dos dispositivos, conforme pode ser percebido observando a Figura 3.11. Isto, apesar de favorecer a conectividade entre dispositivos de um mesmo subgrupo, gera um maior espaçamento entre os subgrupos, prejudicando a conectividade entre os subgrupos.

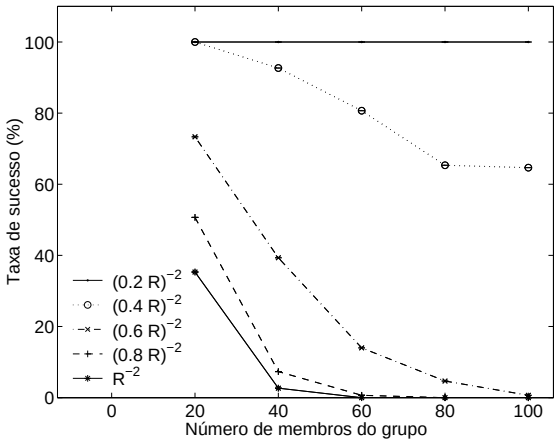
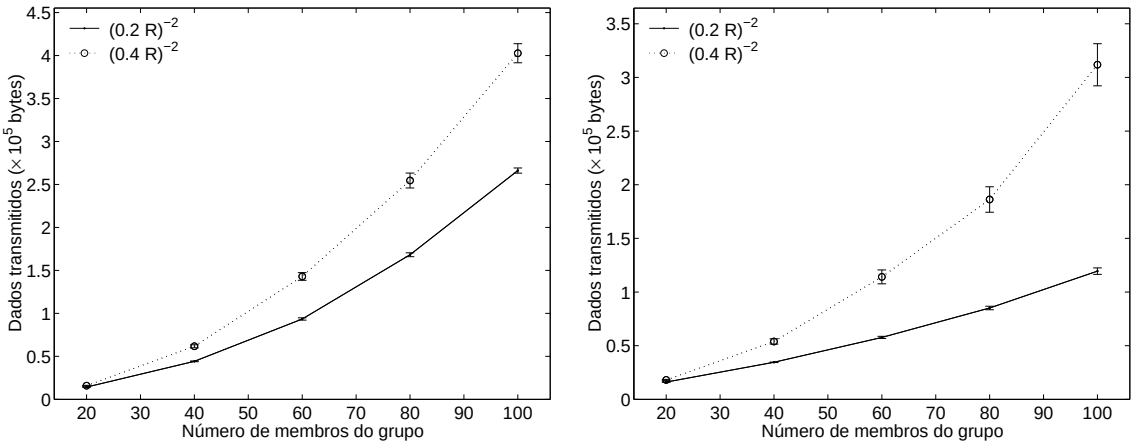


Figura 3.12: Taxa de sucesso para dispositivos parados aglomerados em subgrupo (IKA.1 e IKA.2).

A comparação das quantidades de dados transmitidos em cenários com aglomeração em subgrupos (Figura 3.13) com os valores obtidos em cenários com movimentações independentes (Figura 3.3) permite perceber uma redução das quantidades de dados transmitidos, para ambos os protocolos. Como os dispositivos são agrupados com base nos seus identificadores, esta redução se deve à proximidade entre os membros de um mesmo subgrupo, pois todos os dispositivos que participam de um mesmo subgrupo estão dentro do alcance de transmissão, não havendo, portanto, problemas de conectividade. Todas as mensagens enviadas entre estes dispositivos são então transmitidas sempre por um salto. Os problemas de conectividade só existem quando do envio da contribuição da chave de um subgrupo a outro.

Para uma densidade de $(0,2\ R)^{-2}$ a redução foi de cerca de 35% para ambos os protocolos. Para uma densidade de $(0,4\ R)^{-2}$ esta redução foi de cerca de 50% para o protocolo IKA.1 e cerca de 15% para o protocolo IKA.2. Percebe-se que para o protocolo IKA.1 a aglomeração dos dispositivos em subgrupo apresentou uma maior influência sobre os cenários com densidade $(0,4\ R)^{-2}$ do que sobre os cenários com densidade $(0,2\ R)^{-2}$. Assim, a aglomeração dos dispositivos, favorecendo a execução do primeiro estágio, di-

minuiu o custo para a menor densidade, onde o número de saltos era maior. Para o protocolo IKA.2 a aglomeração dos dispositivos apresentou uma menor influência sobre os cenários com densidade $(0,4\ R)^{-2}$ pois nesta situação o segundo estágio de execução é o mais custoso, transmitindo cerca de três vezes mais mensagens que o primeiro estágio.



(a) IKA.1.

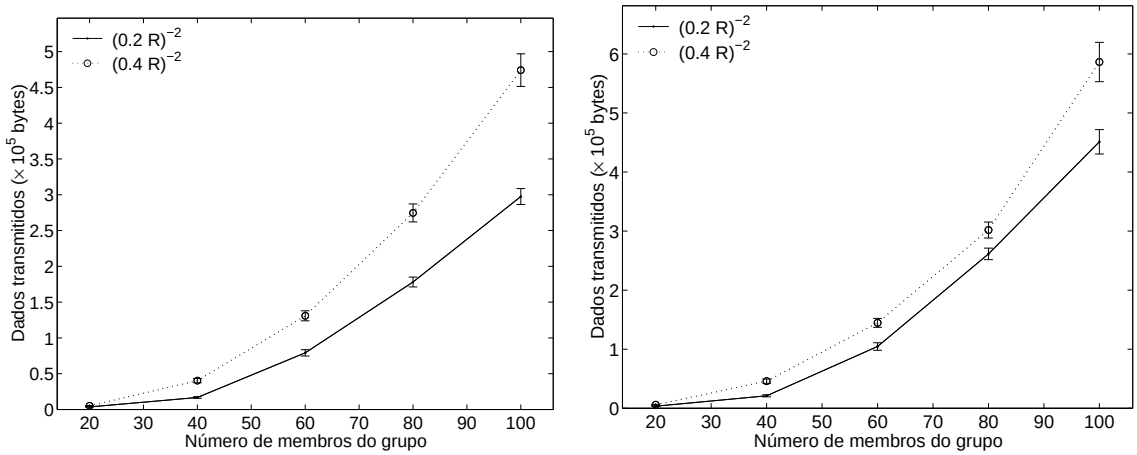
(b) IKA.2.

Figura 3.13: Dados transmitidos pelo protocolo de estabelecimento de chave para dispositivos parados aglomerados em subgrupo.

As quantidades de dados de roteamento transmitidos (Figura 3.14) também sofreram diminuição, chegando a cerca da metade.

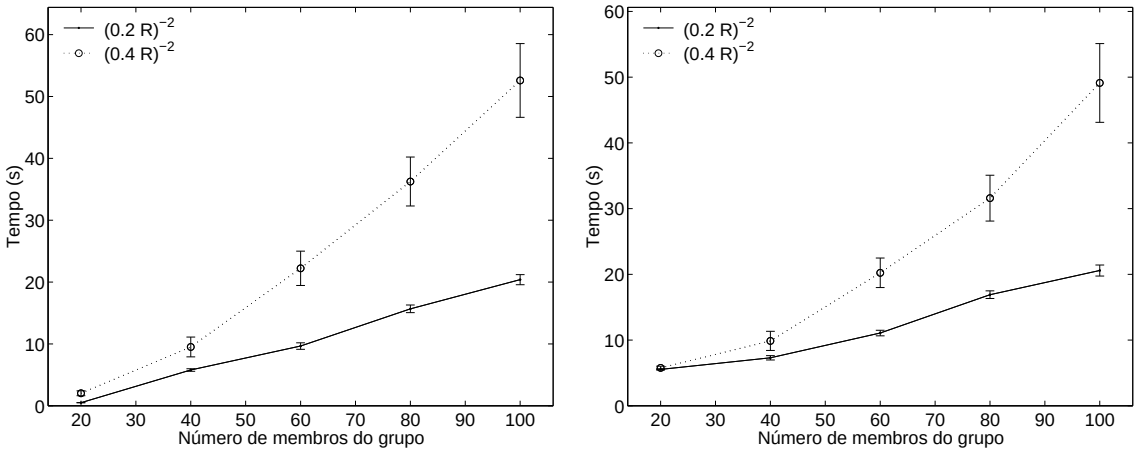
A Figura 3.15 apresenta o tempo de execução dos protocolos para dispositivos parados aglomerados em subgrupos. A comparação com a Figura 3.6 permite perceber que para uma densidade de $(0,2\ R)^{-2}$ o tempo de execução foi cerca de 40% mais baixo para cenários com aglomeração em subgrupos, para ambos os protocolos, o que se deve à comunicação por um salto entre dispositivos de um mesmo subgrupo. Para uma densidade de $(0,4\ R)^{-2}$ o tempo de execução é cerca de 20% a 25% maior em cenários com aglomeração em subgrupos, para ambos os protocolos. Como o tempo de troca das mensagens dentro de um mesmo subgrupo é praticamente constante, o excesso de tempo observado se deve às dificuldades de comunicação entre os subgrupos, devido à menor conectividade entre subgrupos.

Visando analisar o efeito da mobilidade sobre os comportamentos dos protocolos IKA.1 e IKA.2, estes protocolos foram simulados em cenários com aglomerações de dis-



(a) IKA.1. (b) IKA.2.

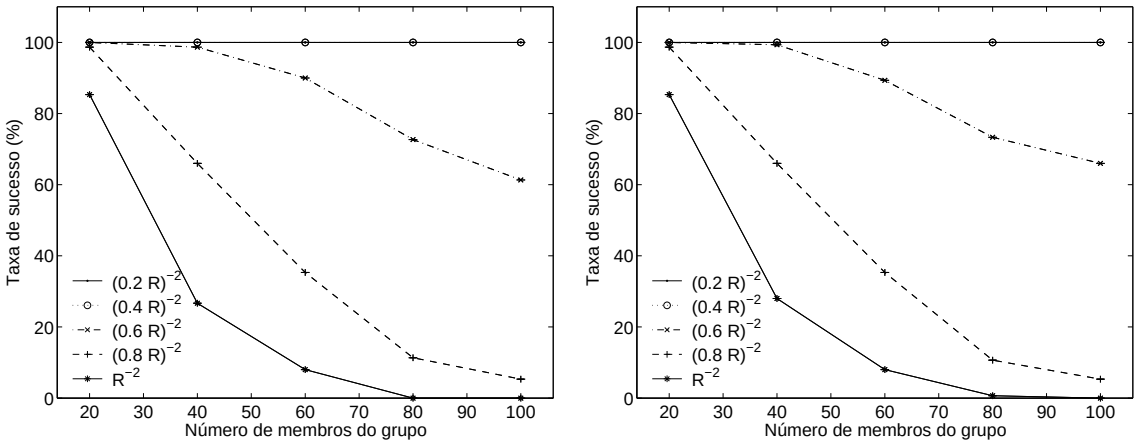
Figura 3.14: Dados de roteamento transmitidos para dispositivos parados aglomerados em subgrupo.



(a) IKA.1. (b) IKA.2.

Figura 3.15: Tempo de execução para dispositivos parados aglomerados em subgrupo.

positivos em subgrupos de 10 dispositivos e constante movimentação a velocidades em torno de 1 m/s. A Figura 3.16 apresenta as taxas de sucesso obtidas. Percebe-se uma tendência de melhora com relação ao comportamento sem mobilidade (Figura 3.12). Para uma densidade de $(0,4\ R)^{-2}$ as taxas de sucesso apresentam-se em torno de 100% e para uma densidade de $(0,6\ R)^{-2}$ a execução dos protocolos tornou-se viável.

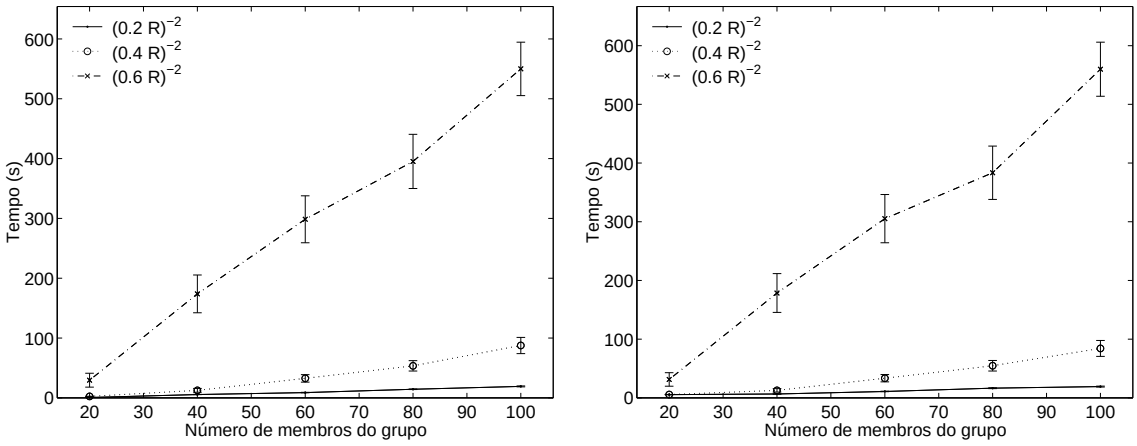


(a) IKA.1. (b) IKA.2.

Figura 3.16: Taxa de sucesso para dispositivos movimentando-se em subgrupos com velocidades em torno de 1 m/s.

Com relação à quantidade de dados transmitidos pelos protocolos IKA.1 e IKA.2 e à quantidade de dados de roteamento transmitidos, os desempenhos foram equivalentes àqueles obtidos com dispositivos parados aglomerados em subgrupos. Este resultado é consistente com o obtido comparando-se os cenários com dispositivos parados e em movimento, aleatoriamente distribuídos pela área de simulação.

A observação dos tempos de execução (Figura 3.17) permite perceber que para uma densidade de $(0,2\ R)^{-2}$ os desempenhos são semelhantes àqueles obtidos com os dispositivos parados e que para uma densidade de $(0,4\ R)^{-2}$ há aumento dos tempos de execução devido a quebras de enlaces e criação de novos enlaces, como verificado para cenários sem aglomeração em subgrupos.



(a) IKA.1. (b) IKA.2.

Figura 3.17: Tempo de execução para dispositivos movimentando-se em subgrupos com velocidades em torno de 1 m/s.

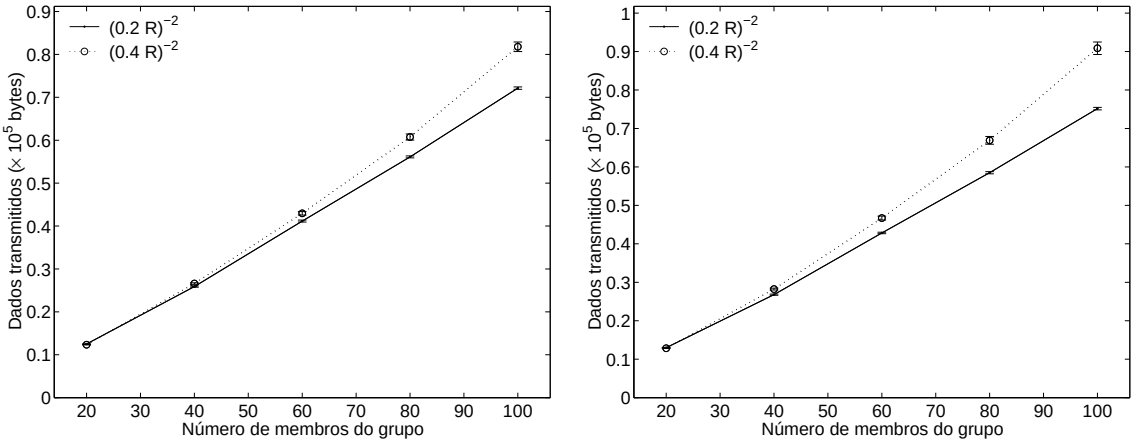
3.3.1 Dispositivos aglomerados em subgrupos com líderes

Com base na hipótese de movimentação em subgrupos, os protocolos IKA.1 e IKA.2 foram simulados em caráter parcialmente contributivo, de forma que cada subgrupo possui um líder, e apenas os líderes participam do estabelecimento da chave de grupo. Esta chave de grupo é então distribuída aos demais membros do subgrupo. Esta distribuição ocorre de forma segura, pois cada membro do subgrupo estabelece uma chave criptográfica secreta com seu líder utilizando o algoritmo Diffie-Hellman. Na simulação, os líderes são posicionados aleatoriamente dentro do subgrupo e são escolhidos pelo identificador mais baixo dentre os membros do subgrupo.

As taxas de sucesso obtidas foram idênticas àquelas obtidas com os dispositivos parados aglomerados em subgrupos com a participação de todos, pois a taxa de sucesso depende neste caso apenas da topologia, que é idêntica nos dois tipos de cenário. Para o caso de dispositivos em movimento as taxa de sucesso foram bastante semelhantes ao caso com aglomeração em subgrupo e estabelecimento completamente contributivo da chave de grupo.

As quantidades de dados transmitidos são apresentadas pela Figura 3.18. Percebe-se uma redução de cerca de 75% com relação aos cenários com estabelecimento completa-

mente contributivo da chave de grupo. Embora o número de participantes no estabelecimento da chave de grupo seja dez vezes menor, a quantidade de dados transmitidos não decai nesta proporção, pois são estabelecidas chaves criptográficas simétricas entre cada líder e cada um dos outros dispositivos que compõem o subgrupo.

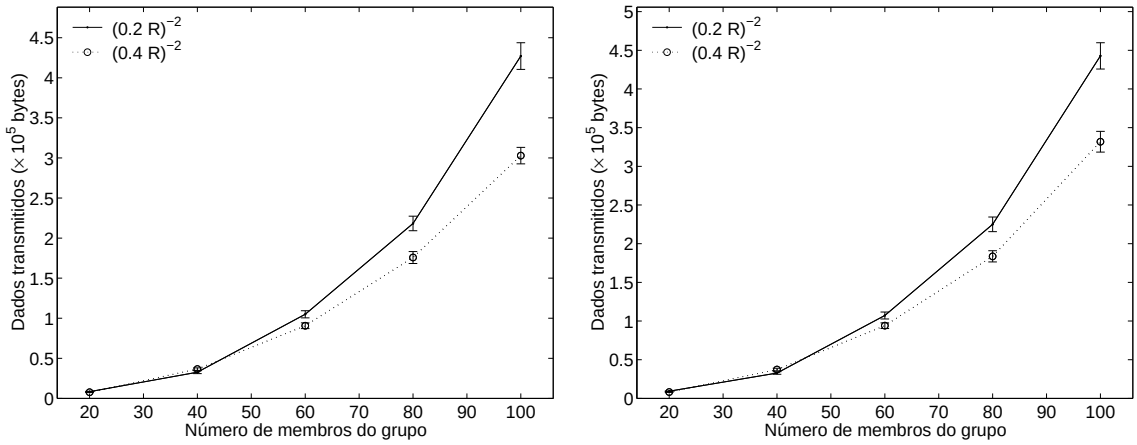


(a) IKA.1. (b) IKA.2.

Figura 3.18: Dados transmitidos pelo protocolo de estabelecimento de chave para dispositivos parados aglomerados em subgrupos com estabelecimento parcialmente contributivo da chave de grupo.

Ao contrário do que vinha sendo observado, a quantidade de dados de roteamento transmitidos por ambos os protocolos foi maior para a densidade mais alta. Isto se deu devido ao funcionamento dos protocolos na forma parcialmente contributiva. Enquanto é executado o estabelecimento da chave de grupo, são estabelecidas várias chaves criptográficas simétricas, entre o líder de cada subgrupo e os demais membros destes subgrupos, o que ocorre simultaneamente para todos os subgrupos. Como os pacotes de solicitação de rotas são transmitidos por difusão natural o protocolo de acesso ao meio não verifica a ocupação do canal no momento de transmiti-los. Isto gera colisão entre os pacotes de pedido de rota, o que gera a necessidade de retransmissão, elevando a quantidade de dados de roteamento transmitidos. Para cenários com maior espaçamento entre os subgrupos a quantidade de colisões é menor, gerando menos transmissões de dados de roteamento.

Os tempos de execução para os cenários com maior densidade foram maiores que para cenários com menor densidade, o que se deve à maior transmissão de dados de roteamento



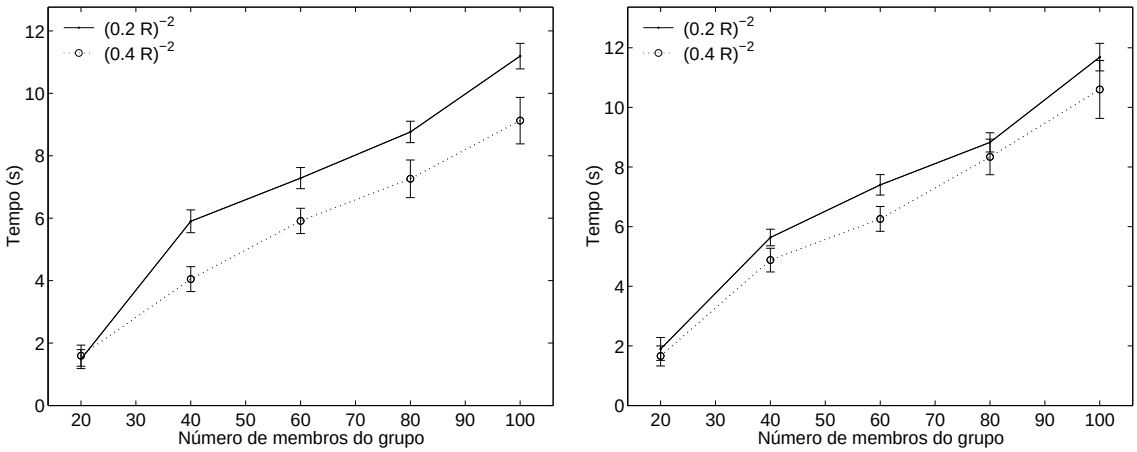
(a) IKA.1. (b) IKA.2.

Figura 3.19: Dados de roteamento transmitidos para dispositivos parados aglomerados em subgrupo com estabelecimento parcialmente contributivo da chave de grupo.

conforme explicado no parágrafo acima.

A mobilidade dos dispositivos a velocidades em torno de 1 m/s favoreceu a conectividade, sendo esta bastante similar à observada para o caso de estabelecimento totalmente contributivo da chave de grupo (Figura 3.16(a)). Os resultados obtidos para as quantidades de dados transmitidos, informações de roteamento transmitidas e tempos de execução foram semelhantes ao caso sem mobilidade.

A divisão do grupo em subgrupos com líder favorece o desempenho dos protocolos de estabelecimento de chave, pois o número de dispositivos envolvidos na execução dos protocolos é menor, diminuindo o tempo de execução, o número de mensagens e a quantidade de dados transmitidos. Com relação ao tempo de execução, o estabelecimento de chaves simétricas entre cada líder e os demais dispositivos de seu subgrupo pode ocorrer em paralelo à execução do protocolo de estabelecimento da chave de grupo e à execução deste mesmo procedimento para os demais subgrupos. A escalabilidade também é favorecida, pois o número de participantes no estabelecimento da chave de grupo pode ser maior ou menor em função do número de subgrupos e da quantidade de dispositivos por subgrupo.



(a) IKA.1.

(b) IKA.2.

Figura 3.20: Tempo de execução para dispositivos parados aglomerados em subgrupos com estabelecimento parcialmente contributivo da chave de grupo.

Capítulo 4

Conclusões

ESTE trabalho analisou e comparou os principais protocolos de estabelecimento de chave de grupo entre um conjunto de dispositivos que compõem uma rede ad hoc. Os protocolos IKA.1 e IKA.2 foram selecionados como os mais convenientes para execução neste ambiente por apresentarem bons desempenhos com relação ao número de mensagens transmitidas, à quantidade total de dados transmitidos e ao número de operações de exponenciação realizadas, por permitirem a descoberta de participantes durante o estabelecimento de chave de grupo e permitirem a alteração desta chave de grupo sem a necessidade de execução de todo o protocolo a partir do início. Estes protocolos foram avaliados por simulação de modo a considerar as características do ambiente ad hoc.

As simulações se basearam no modelo de mobilidade geralmente utilizado, que consiste de dispositivos aleatoriamente distribuídos pela área de simulação, e no modelo proposto, que consiste na aglomeração dos dispositivos em subgrupos.

Os resultados demonstram que o maior problema do estabelecimento de chave de grupo em redes ad hoc é a falta de conectividade entre os membros deste grupo, devido ao maior espalhamento dos dispositivos pela área de simulação quando se diminui a densidade de dispositivos. Este maior espalhamento leva ainda ao aumento do número de mensagens transmitidas, da quantidade de dados transmitidos e do tempo de execução dos protocolos.

As simulações demonstraram que a mobilidade dos dispositivos favorece o estabele-

cimento da chave de grupo pois aumenta as chances de comunicação devido a problemas de conectividade.

Foi observado que nos cenários com aglomeração dos dispositivos em subgrupos pode-se tirar proveito da proximidade entre os dispositivos de um mesmo subgrupo para se transmitir um menor número de mensagens. Em contra-partida, este cenário, quando comparado ao cenário de posicionamento aleatório, tem um maior problema de falta de conectividade devido à maior distância entre os dispositivos, para uma mesma densidade de dispositivos móveis.

Verificou-se que uma abordagem parcialmente contributiva favorece a escalabilidade do estabelecimento da chave de grupo pois diminui os custos relacionados a número de mensagens, quantidade de dados transmitidos e tempo de execução dos protocolos.

Os resultados indicam um baixo custo de execução dos protocolos IKA.1 e IKA.2 nos cenários utilizados.

Alguns trabalhos futuros incluem a ordenação das seqüências em que ocorrem as contribuições baseada na posição geográfica dos dispositivos, e não no identificador destes dispositivos, de modo a reduzir o número de saltos; a avaliação do comportamento dos protocolos IKA.1 e IKA.2 em cenários de movimentação com velocidades mais elevadas; a avaliação da adição e da exclusão de membros do grupo; e a estimação dos tempos relativos às computações necessárias ao estabelecimento da chave de grupo.

Referências Bibliográficas

[1] HU, Y.-C., PERRIG, A., E JOHNSON, D. B. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *The Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)* (setembro de 2002).

[2] PAPADIMITRATOS, P., E HAAS, Z. J. Secure routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)* (janeiro de 2002).

[3] HU, Y.-C., JOHNSON, D. B., E PERRIG, A. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications* (junho de 2002).

[4] ASOKAN, N., E GINZBOORG, P. Key agreement in ad hoc networks. *Computer Communications 23*, 17 (novembro de 2000), 1627–1637.

[5] BECKER, K., E WILLE, U. Communication complexity of group key distribution. In *5th ACM conference on Computer and Communication Security* (novembro de 1998).

[6] HAAS, Z. J., E ZHOU, L. Securing ad hoc networks. *IEEE Network Magazine 13*, 6 (novembro/dezembro de 1999), 24–30.

[7] KHALILI, A., KATZ, J., E ARBAUGH, W. A. Toward secure key distribution in truly ad-hoc networks. In *IEEE Workshop on Security and Assurance in Ad hoc Networks* (janeiro de 2003).

[8] STAJANO, F., E ANDERSON, R. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *3rd AT&T Software Symposium* (outubro de 1999).

[9] BALFANZ, D., SMETTERS, D. K., STEWART, P., E WONG, H. C. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium (NDSS '02)* (fevereiro de 2002).

[10] ANTON, E. R., E DUARTE, O. C. M. B. Estabelecimento de chave de grupo em redes ad hoc. In *Workshop em Segurança de Sistemas Computacionais (WSeg 2002)* (Búzios, RJ, maio de 2002), pp. 89–96.

[11] ANTON, E. R., E DUARTE, O. C. M. B. Segurança em redes sem fio ad hoc: Gerenciamento de chave de grupo. In *XIV Congresso Brasileiro de Automática* (Natal, RN, setembro de 2002).

[12] ANTON, E. R., E DUARTE, O. C. M. B. Group key establishment in wireless ad hoc networks. In *Workshop em Qualidade de Serviço e Mobilidade (WQoSM 2002)* (Angra dos Reis, RJ, novembro de 2002).

[13] ANTON, E. R., E DUARTE, O. C. M. B. Uma análise de protocolos para o estabelecimento de chave de grupo em redes ad hoc. Relatório técnico, março de 2003. GTA-03-01.

[14] ANTON, E. R., E DUARTE, O. C. M. B. Performance analysis of group key establishment protocols in ad hoc networks. Relatório técnico, março de 2003. GTA-03-06.

[15] OORSCHOT, P. C. V., E RUEPPEL, R. A. Modern key agreement techniques. *Computer Communications 17*, 7 (julho de 1994), 458–465.

[16] ATENIESE, G., STEINER, M., E TSUDIK, G. Authenticated group key agreement and friends. In *5th ACM Conference on Computer and Communications Security* (novembro de 1998).

[17] ATENIESE, G., STEINER, M., E TSUDIK, G. New multiparty authentication services and key agreement protocols. *IEEE Journal on Selected Areas in Communications 18*, 4 (abril de 2000).

[18] DIFFIE, W., E HELLMAN, M. E. New directions in cryptography. *IEEE Transactions on Information Theory IT-22*, 6 (novembro de 1976), 644–654.

[19] INGEMARSSON, I., TANG, D. T., E WONG, C. K. A conference key distribution system. *IEEE Transactions on Information Theory IT-28*, 5 (setembro de 1982), 714–720.

[20] BURMESTER, M., E DESMEDT, Y. A secure and efficient conference key distribution system. In *Advances in Cryptology (EUROCRYPT '94)* (maio de 1994), pp. 275–286.

[21] STEINER, M., TSUDIK, G., E WAIDNER, M. Diffie-Hellman key distribution extended to group communication. In *3rd ACM Conference on Computer and Communications Security* (março de 1996).

[22] STEINER, M., TSUDIK, G., E WAIDNER, M. CLIQUES: A new approach to group key agreement. In *18th International Conference on Distributed Computing Systems* (maio de 1998).

[23] STEINER, M., TSUDIK, G., E WAIDNER, M. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems 11*, 8 (agosto de 2000), 769–780.

[24] KIM, Y., PERRIG, A., E TSUDIK, G. Simple and fault-tolerant key agreement for dynamic collaborative groups. In *7th ACM Conference on Computer and Communications Security* (novembro de 2000), pp. 235–244.

[25] NI, S.-Y., TSENG, Y.-C., CHEN, Y.-S., E SHEU, J.-P. The broadcast storm problem in a mobile ad hoc network. In *5th annual ACM/IEEE International Conference on Mobile Computing and Networking* (agosto de 1999), pp. 151–162.

[26] SUN, M.-T., FENG, W., E LAI, T.-H. Location aided broadcast in wireless ad hoc networks. In *IEEE GLOBECOM 2001* (novembro de 2001), pp. 2842–2846.

[27] FALL, K., E VARADHAN, K. *The ns Manual*, abril de 2002.

[28] JOHNSON, D. B., MALTZ, D. A., HU, Y.-C., E JETCHEVA, J. G. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, fevereiro de 2003. Internet draft: draft-ietf-manet-dsr-08.txt.

[29] XU, S., E SAADAWI, T. Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? *IEEE Communications Magazine 39*, 6 (junho de 2001), 130–137.

[30] GERLA, M., TANG, K., E BAGRODIA, R. TCP performance in wireless multi-hop networks. In *2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99)* (fevereiro de 1999).

[31] BIAZ, S., E VAIDYA, N. H. Distinguishing congestion losses from wireless transmission losses: A negative result. In *International Conference on Computer Communications and Networks* (outubro de 1998).

[32] HOLLAND, G., E VAIDYA, N. Analysis of TCP performance over mobile ad hoc networks. In *5th annual ACM/IEEE International Conference on Mobile Computing and Networking* (agosto de 1999), pp. 219–230.

[33] PARSA, C., E GARCIA-LUNA-ACEVES, J. J. Improving TCP performance over wireless networks at the link layer. *ACM Mobile Networks and Applications 5*, 1 (março de 2000), 57–71.

[34] BALAKRISHNAN, H., PADMANABHAN, V. N., SESHAN, S., E KATZ, R. H. A comparison of mechanisms for improving TCP performance over wireless links. *IEEE/ACM Transactions on Networking 5*, 6 (dezembro de 1997), 756–769.

[35] QIMING, L. The Scenario Generator, 2001. `http://www.comp.nus.edu.sg/~liqm/scengen/`.