UM MODELO DE GERENCIAMENTO DE SEGURANÇA ADAPTATIVO PARA REDES DE EMERGÊNCIA

THIAGO RODRIGUES DE OLIVEIRA

UM MODELO DE GERENCIAMENTO DE SEGURANÇA ADAPTATIVO PARA REDES DE EMERGÊNCIA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

ORIENTADOR: JOSÉ MARCOS SILVA NOGUEIRA

Belo Horizonte

Fevereiro de 2010

Oliveira, Thiago Rodrigues de
O48m Um modelo de gerenciamento de segurança adaptativo para redes de emergência / Thiago Rodrigues de Oliveira. — Belo Horizonte, 2010
viii, 20 f. ; 29cm

Dissertação (mestrado) — Universidade Federal de Minas Gerais
Orientador: José Marcos da Silva Nogueira

1. Redes de computação - segurança - teses. 2. Redes de computação - medidas de segurança - teses. 3. Gerenciamento de redes - teses. 4. Segurança em DTN - teses. I. Título.

CDU 519.6*22(043)

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

Um modelo de gerenciamento de segurança adaptativo para redes de emergência

THIAGO RODRIGUES DE OLIVEIRA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

PROF. JOSÉ MARCOS SILVA NOGUEIRA - Orientador
Departamento de Ciência da Computação - UFMG

DR. DANIEL FERNANDES MACEDO
Bolsista de Pós-Doutorado - DCC-UFMG

PROF. DORGIVAL OLAVO GUEDES NETO
Departamento de Ciência da Computação - UFMG

PROF. SÉRGIO DE OLIVEIRA
Universidade Federal de São João Del-Rei - UFSJ

Belo Horizonte, 26 de fevereiro de 2010.

Agradecimentos

Agradeço primeiramente a Deus, é d'Ele a vitória alcançada em minha vida. O tempo de oração pode ter diminuído, mas não a fé.

A família é fundamental em cada conquista, pelo incentivo e confiança. Agradeço à minha mãe, que sempre nos transmitiu garra, vontade de estudar e transmitir conhecimento. Ao meu pai, que esteve muito próximo em um período difícil desse trabalho e não pode estar presente agora. Aos meus irmãos, sempre presentes como companheiros e exemplos para meus passos, tenho orgulho de me parecer um pouco com cada um deles. Também à minha madrinha, a quem ainda devo algumas visitas, mas nunca esquecerei.

Ao meu orientador José Marcos, por toda a atenção e auxílio antes e durante o mestrado. Aos amigos de laboratório ATM, que ajudaram na construção desse trabalho. Todos os amigos do DCC, especialmente do Synergia, companheiros de trabalho e de constante aprendizado.

Aos amigos de Lafaiete, que a tornam perfeita para combater o *stress* de toda semana. Aos amigos de república, superamos momentos difíceis. Ao Wellington, presente nas duas últimas citações e parceiro nos estudos. Todos que confiaram em mim e que tudo seria possível.

Resumo

Em casos de desastres e cenários de emergência, onde há carência de infra-estrutura de rede, equipes de resgate podem formar redes ad hoc móveis para envio de informações. Contudo, a comunicação nesses casos pode sofrer longas interrupções, o que deve ser considerado no aspecto de segurança da rede. Os requisitos de segurança podem variar de acordo com o cenário e situação da utilização da rede de emergência. É necessário prover adaptabilidade para equilibrar a relação entre o grau de segurança e o uso de recursos da rede. Esse trabalho propõe um modelo de gerenciamento de segurança para configurar dinâmica e autonomicamente redes de emergência, com objetivo de adaptar a utilização de mecanismos de segurança às informações de gerenciamento recebidas pelos nós responsáveis por tomada de decisões. O modelo de gerenciamento inclui a definição dos níveis de segurança, base de informações de gerenciamento, mensagens do protocolo e eventos. O gerenciamento permite a adaptação da rede durante sua execução, habilitando ou desabilitando componentes de segurança. As avaliações realizadas mostram o comportamento de uma rede de emergência com a ativação de mecanismos de segurança quando necessário. Os resultados indicam que o modelo de gerenciamento proposto não proporciona impacto na probabilidade de entrega de mensagens da rede. A análise desse modelo demonstra que as mensagens de gerenciamento enviadas alcançam todos os nós participantes e a ativação gradual de mecanismos à medida que forem detectadas ameaças para segurança da rede pode representar economia de recursos.

Palavras-chave: *segurança em DTN, gerenciamento de redes, adaptação, redes de emergência, redes DTN, mecanismos de segurança.*

Abstract

In cases of disasters and emergency scenarios, due to lack of network infrastructure, first-responders can build mobile ad hoc networks to send information. However, the communication in these situations can suffer long interruptions, which should be considered in the network security aspect. The security requirements can change according to the scenario and utilization of the network. It's necessary to provide adaptability to balance the relation between security degree and network resource utilization. This work proposes a security management framework to dynamically configure and reconfigure emergency networks, with goal to adapt the use of security mechanisms according to management information received by the entities responsible for decision-making. The security management model includes the definition of security levels, management information base, protocol messages and events. This management allows the network adaptation during its execution, activating or deactivating security components. The evaluations realized show an emergency network behavior with activation of security mechanisms if necessary. Results indicate that the proposed management model doesn't impact the delivery probability of network messages. The analysis of this model demonstrates that the management messages reach every participant node and the mechanisms' gradual activation due to threat detections for network security can provide resource savings.

Keywords: *DTN security, network management, adaptation, emergency networks, DTN, security mechanisms.*

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Grandes catástrofes recentes e situações de crise como o tsunami no fim de 2004 e o furacão Katrina em setembro de 2005 mostraram a importância da comunicação para evitar mortes de milhares de pessoas. Deve-se estar preparado para o aumento de fenômenos naturais de grande porte, visto que o aquecimento global é uma realidade e lidar com suas conseqüências não é tarefa trivial. Em situações de crise, diferentes situações adversas devem ser respondidas apropriadamente, considerando-se a maior quantidade possível de informações.

Se um desastre tem impacto em várias regiões ou países, é um grande desafio coordenar as atividades de diferentes autoridades (polícia, ambulância, bombeiros etc) na área do desastre. O idioma pode também ser um desafio, sendo que autoridades da mesma região podem utilizar linguagens profissionais diferentes. Redes de comunicação de dados podem ser utilizadas para dar suporte a equipes de resgate em diversos cenários de emergência como incêndios, enchentes, terremotos, atentados terroristas, etc [Mehrotra, 2008].

Inicialmente, é interessante observar o que realmente caracteriza um estado emergencial. Segundo o Dicionário da Língua Portuguesa, emergência é: "...situação crítica; acontecimento perigoso ou fortuito; incidente...". Evidentemente, esta é uma definição generalizada, que não contempla o aspecto técnico-operacional abordado nesse trabalho. Ou seja, emergência significa perigo iminente à vida.

Desastres são situações que rompem o funcionamento normal da sociedade e economia de uma região, que podem ter origens naturais,

tecnológicas ou humanas. Catástrofes são desastres em grandes proporções que acarretam grandes prejuízos, humanos e materiais. Após a ocorrência de um desastre de grandes proporções, é necessário o esforço coordenado de um grande número de pessoas para dar apoio às vítimas, atuar no controle das causas e efeitos do desastre e trabalhar com o intuito de reestabelecer as atividades econômicas e sociais da região afetada.

Em termos de rádio-comunicação, uma operação de emergência configura, normalmente, um conjunto de condições que determinam, por sua gravidade e urgência de atendimento, ações de socorro, suporte, resgate, auxílio, transporte e, em nosso caso, estabelecimento de comunicação alternativa entre o local do evento e as estruturas criadas em função do mesmo. Obviamente, o objetivo principal de tal mobilização é a proteção não só das possíveis vítimas, como também de todos os elementos humanos envolvidos na operação.

A partir da decretação do estado de emergência, por autoridade competente e nunca por iniciativa isolada, passam a vigorar procedimentos diferenciados de ação, que também atingem a comunicação. Entre os desafios, é necessário ter coordenação eficiente, fixação de tarefas, freqüências alternativas, revezamento de operadores etc.

Na maioria das vezes, várias entidades distintas atuam sobre a região afetada, cada uma com sua própria hierarquia de comando, mas trabalhando em conjunto, como é o caso dos bombeiros, das equipes de para-médicos, da defesa civil e de organizações não governamentais que podem auxiliar nos resgates na região em crise. Esses agentes necessitam do maior número de informações possível, tais como mapas, fotos aéreas e informações visuais (fotos e vídeos) que melhoram o entendimento dos problemas.

Um fator que favorece a montagem de redes de emergência é a popularização de dispositivos móveis como notebooks, PDAs, tablets e celulares com mais recursos disponíveis, que podem ser utilizados por agentes de equipes que atendem a situações de emergência. Porém, deve-

se considerar que as redes formadas por esses dispositivos possuem várias limitações, pois necessitam de certas condições que nem sempre são satisfeitas. Em redes de missões críticas, tais como situações de atendimento a desastres, a conectividade fim-a-fim é altamente suscetível à interrupção de comunicação.

As redes móveis ad hoc (MANETs) [Manet, 2008][Mota, 2009] se encaixam nesse tipo de cenário pela ausência de infra-estrutura e necessidade de conexões entre dispositivos móveis, com utilização de centros de controles com maiores recursos, roteadores sem fio, aparelhos móveis e nós sensores.

Deve ser considerada a necessidade de se trabalhar em redes com conectividade intermitente ou com longos atrasos, através da utilização da arquitetura de rede DTN (Disruption Tolerant Networks) [Fall, 2004]. Utilizando um esquema de comunicação assíncrona, uma rede DTN pode ter melhor alcançabilidade, especialmente em redes com nós esparsos devido às seguintes propriedades: comunicação baseada em mensagens assíncronas agregadas (*bundles*); não há necessidade de um caminho fim-a-fim, pois os agregados podem ficar armazenados nos nós até que seja estabelecida uma conexão; atrasos podem ser longos e variados; por fim, sua tolerância a altas taxas de erros.

Apesar do potencial e impacto na vida humana, redes DTN são motivo de preocupações em relação à segurança e privacidade, o que limita suas aplicações. Possuem vulnerabilidades similares a outras redes sem fio, tais como a possibilidade de intrusos manipularem ou injetarem mensagens, limitarem a disponibilidade do sistema, confidencialidade e integridade dos sistemas.

Além das técnicas tradicionais de prevenção, um gerenciamento confiável pode servir como base de segurança para cooperação dos nós e disseminação das informações. A arquitetura de segurança para essas redes deve ser baseada nas necessidades dos usuários finais e suas aplicações. O gerenciamento de segurança deve evitar a utilização da rede por agentes externos e manter o equilíbrio em relação ao consumo de recursos da rede de emergência.

Características específicas desse tipo de redes, como mobilidade imprevisível e latência variável, ainda tornam a segurança mais desafiadora. Devido à conectividade esporádica e grande possibilidade de atraso de transmissão de mensagens, é necessário eliminar mensagens expiradas e evitar vazamento de informações.

1.1. Motivação

Redes de computadores para suporte a emergência podem ser construídas em situações ocasionadas por desastres naturais, tecnológicos ou causados pelo homem nos quais é interrompido o funcionamento normal da economia e da sociedade. A utilização de redes de comunicação sem fio pode facilitar a coordenação de pessoas e equipes em regiões de desastres, para superar o desafio de comunicação nessas situações.

A motivação original dessas redes é social, objetivando a proteção não só das vítimas, como também de todos os elementos humanos envolvidos na operação. Em situações críticas e de emergência, como em regiões isoladas, desastres ecológicos ou conflitos urbanos, geralmente não existe uma infra-estrutura de rede ou a mesma foi destruída.

Com o aumento do número de dispositivos móveis vendidos, como celulares e PDA's, e levando-se em consideração que tais dispositivos possuem recursos cada vez mais poderosos, tanto em termos de processamento, capacidade de armazenamento e conexão com outros dispositivos, é esperado que, em pouco tempo, eles sejam utilizados em vários tipos de aplicações distribuídas.

Uma possível solução para a comunicação é a formação de redes *ad hoc*, com a utilização de dispositivos móveis que se auto-organizam para prover comunicação, compartilhamento de arquivos e processamento colaborativo [Mota, 2009]. Porém, este tipo de rede é muito menos confiável do que a Internet ou redes com fio estruturadas.

Existem várias possíveis causas de ataques às redes de emergência: informações sigilosas sobre vítimas de desastres podem ser interessantes à imprensa, terroristas podem tentar atrapalhar o resgate após atentados, ideais políticos podem levar pessoas a tentar atrapalhar o atendimento a incêndios em áreas ricas, alguma empresa concorrente pode ter interesse em dificultar o trabalho de bombeiros em uma empresa afetada por um desastre, entre outros.

Este trabalho se justifica pela expansão do uso de dispositivos móveis que podem ser utilizados pelos agentes em operações de resposta a situações críticas e de emergência. Nesse contexto, observa-se a necessidade de aumentar a segurança entre esses recursos durante a crise e prover soluções que se adaptem de acordo com a situação da rede durante sua utilização. Uma solução de gerenciamento pode permitir que uma rede de emergência apresente o grau de segurança necessário em cada cenário, evitando o consumo excessivo de recursos da rede.

1.2. Problema

Os requisitos de segurança em redes de emergência podem variar de acordo com as situações e cenários em que elas são utilizadas, pois pode haver várias motivações para que sejam realizados ataques às redes de emergência.

Um dos principais desafios é garantir requisitos mínimos de segurança no envio dos dados, pois essas redes são mais vulneráveis à ação de intrusos que as redes convencionais, uma vez que os recursos computacionais são limitados, o ambiente é hostil e a comunicação sem fio está mais sujeita a ataques. Mecanismos de segurança desenvolvidos para tais redes precisam levar em conta também restrições de recursos, como o uso de baterias como fonte de energia.

Questões de confiança, envolvendo segurança, privacidade e confiabilidade devem ser consideradas em cenários de desastres. Os

recursos de resposta a um desastre devem prover diferentes níveis de segurança, garantia e confiabilidade, baseados nas necessidades dos usuários finais e suas aplicações.

Prover comunicação móvel segura e com possível integração de redes de sensores a redes de emergência são aspectos importantes para o gerenciamento de crises futuras. Percebe-se a necessidade da utilização de mecanismos de segurança em redes de emergência, pois o atendimento a requisitos de segurança é essencial. Dados os aspectos particulares dessas redes, é importante que exista adaptabilidade da segurança utilizada na rede para considerar o compromisso grau de segurança versus uso de recursos da rede.

1.3. Objetivos

Os objetivos desse trabalho consistem no estudo de aspectos relacionados à segurança em redes de emergência, na identificação de requisitos e na concepção de uma arquitetura para o gerenciamento de segurança, observando as situações em que os mecanismos de segurança estabelecidos devem ser utilizados. Assim como outras redes, características como confiabilidade e disponibilidade são fundamentais.

De acordo com a utilização da rede de emergência, podem ser necessários vários mecanismos para prover segurança. Para manter o equilíbrio entre o grau de segurança e os recursos utilizados da rede ao longo do tempo, é interessante considerar soluções adaptativas para a segurança de redes de emergência.

Abordando o problema da segurança para redes DTN nesse contexto, esse trabalho tem por objetivo principal propor um modelo de gerenciamento de segurança adaptativo que habilita ou desabilita componentes de segurança e de roteamento em reação a ameaças representadas por intrusos em redes de emergência. Um modelo de gerenciamento deve ser composto por um modelo de informações,

incluindo definição dos componentes de segurança, situações onde cada componente deve ser utilizado e protocolos para negociação da utilização dos componentes.

Os mecanismos de segurança propostos para redes DTN podem ser utilizados como componentes de um gerenciamento de segurança. O estudo e compreensão desses componentes é um dos objetivos desse trabalho, bem como a avaliação das suas formas e situações de utilização, de maneira a possibilitar a utilização de forma isolada ou mista. O gerenciamento pode permitir a adaptação da rede durante sua execução, inserindo ou removendo componentes de segurança adicionais.

1.4. Contribuições

As contribuições desse trabalho podem ser destacadas no aumento da segurança em redes tolerantes a interrupções (DTN) e especificamente no cenário de redes de emergência, ao conceber um modelo de gerenciamento de segurança adaptativo que possibilite a reconfiguração da rede DTN, segundo a abordagem de redes autonômicas, e através do qual poderá ser obtido um nível maior de segurança para essas redes.

A utilização de mecanismos de segurança integrados e de maneira adaptável às necessidades da rede é uma proposta inovadora na abordagem de problemas relacionados à segurança em redes DTN. A concepção e a implementação dessa proposta podem ser referência para outros trabalhos.

A avaliação do modelo proposto através de simulações pode apresentar novos dados a respeito do impacto de gerenciamento na entrega de mensagens em redes de emergência e comprovar se os mecanismos de segurança são ativados somente se necessário.

1.5. Estrutura do documento

O conteúdo desse documento é apresentado em seis capítulos. Os dois primeiros capítulos são introdutórios. Este primeiro capítulo apresenta o problema a ser abordado e, inicialmente, a solução proposta. O capítulo seguinte apresenta os conceitos básicos necessários para o entendimento desse trabalho, descrevendo as características das redes de emergência e o modelo de rede abordado, juntamente com os trabalhos relacionados.

As principais contribuições deste trabalho são apresentadas a partir do terceiro capítulo, que apresenta um estudo sobre os requisitos de segurança para redes de emergência e ameaças existentes nesses ambientes. São apresentadas explicações sobre cada um dos mecanismos de segurança abordados no gerenciamento de segurança proposto. O quarto capítulo apresenta o modelo gerenciamento de segurança adaptativo proposto, bem como suas formas de configuração, aspectos para prover auto-gerenciamento e vantagens de utilização. No quinto capítulo, são apresentadas a discussão sobre o modelo e a análise dos resultados obtidos na avaliação. Por fim, o sexto capítulo apresenta as conclusões deste trabalho, contribuições e possíveis trabalhos futuros.

Capítulo 2

Redes Abordadas

2.1. Redes de Emergência

2.1.1. Definição

Em situações críticas e de emergência, como em regiões isoladas, desastres ecológicos ou conflitos urbanos, geralmente não existe uma infra-estrutura de rede ou a mesma foi destruída. Os agentes humanos que atendem a essas situações necessitam do maior número de informações possível, tais como mapas, fotos aéreas e informações visuais que melhoram o entendimento dos problemas.

Redes de computadores para suporte a emergência podem ser construídas em situações ocasionadas por desastres naturais, tecnológicos ou causados pelo homem nos quais é interrompido o funcionamento normal da economia e da sociedade. A utilização de redes de comunicação sem fio pode facilitar a coordenação de pessoas e equipes em regiões de desastres, para superar o desafio de comunicação nessas situações.

As redes formadas nessas situações são heterogêneas em *hardware*, com a utilização de *notebooks, palmtops, tablets, celulares* e *nós sensores* em sua composição e várias tecnologias de rede para comunicação entre os nós. Porém, deve-se considerar que as redes formadas por esses dispositivos possuem várias limitações, pois necessitam de certas condições que nem sempre são satisfeitas. Em redes de missões críticas, tais como situações de atendimento a desastres, a conectividade fim-a-fim é altamente suscetível à interrupção de comunicação.

Dispositivos móveis podem ser utilizados pelos agentes em operações de resposta a situações críticas e de emergência. Componentes típicos dessas redes são ambulâncias, hospitais, veículos de transporte e bombeiros, além de agentes humanos atuando nas áreas de desastre. Um equipamento sem restrição de recursos, denominado centro de controle, será o responsável pela tomada de decisões e poderá detectar ataques à rede.

O centro de controle pode ser um computador *desktop* ou um *laptop*, apresentando uma fonte de energia constante e grande capacidade de processamento e memória. Os centros de controle podem ser móveis ou fixos.

Várias podem ser as motivações para que sejam realizados ataques às redes de emergência: informações sigilosas sobre vítimas de desastres podem ser interessantes à imprensa, terroristas podem tentar atrapalhar o resgate após atentados, ideais políticos podem levar pessoas a tentar atrapalhar o atendimento a incêndios em áreas ricas, alguma empresa concorrente pode ter interesse em dificultar o trabalho de bombeiros em uma empresa afetada por um desastre, entre outros.

O interesse em segurança nessas situações depende do ambiente e da aplicação, embora autenticação e privacidade sejam geralmente críticos [Portmann, 2008]. Os requisitos de segurança em redes de emergência podem variar de acordo com as situações e cenários em que elas são utilizadas, pois há várias motivações para que sejam realizados ataques a essas redes. Os diversos componentes de segurança devem ser usados de acordo com o objetivo da rede em cada situação.

A conectividade da rede no cenário de uma emergência não pode ser considerada constante, pois o ambiente considerado hostil pode gerar várias interrupções. Portanto, as redes devem ser tolerantes a atrasos e interrupções, devendo ser consideradas *Disruption Tolerant Networks* (DTN) compostas por diversos nós. Os nós em redes DTN carregam os pacotes enquanto se movem, e então encaminham os pacotes quando uma conexão sem fio estiver disponível entre eles.

2.1.2.Modelo de rede

Redes formadas em situações de emergência são heterogêneas em hardware, com a utilização de notebooks, palmtops, celulares e nós sensores em sua composição e com várias tecnologias de rede para comunicação entre os nós. Alguns dos nós estão conectados, enquanto os demais podem não ter conectividade. Tais conexões podem cair a qualquer momento, devido a falhas, deslocamentos ou outros tipos de eventos.

Redes de emergência possibilitam uma variedade muito grande de configurações. A ampla diversidade de nós participantes, que vão desde nós sensores a robustos centros de controle, a mobilidade e as aplicações impedem que a caracterização do problema de provimento de segurança seja feita de forma única, o que pode dificultar a proposta de uma solução aplicável a todos os casos.

Os nós da rede podem representar equipes de resgate, nós sensores para o monitoramento, pontos de acesso fixos que provêem conexão externa ao local do incidente e computadores gerenciadores (centros de controle). Sensores podem ser utilizados para monitoramento e sensoriamento de regiões em risco, como na monitoração de proximidades de um incêndio e envio dessas informações.

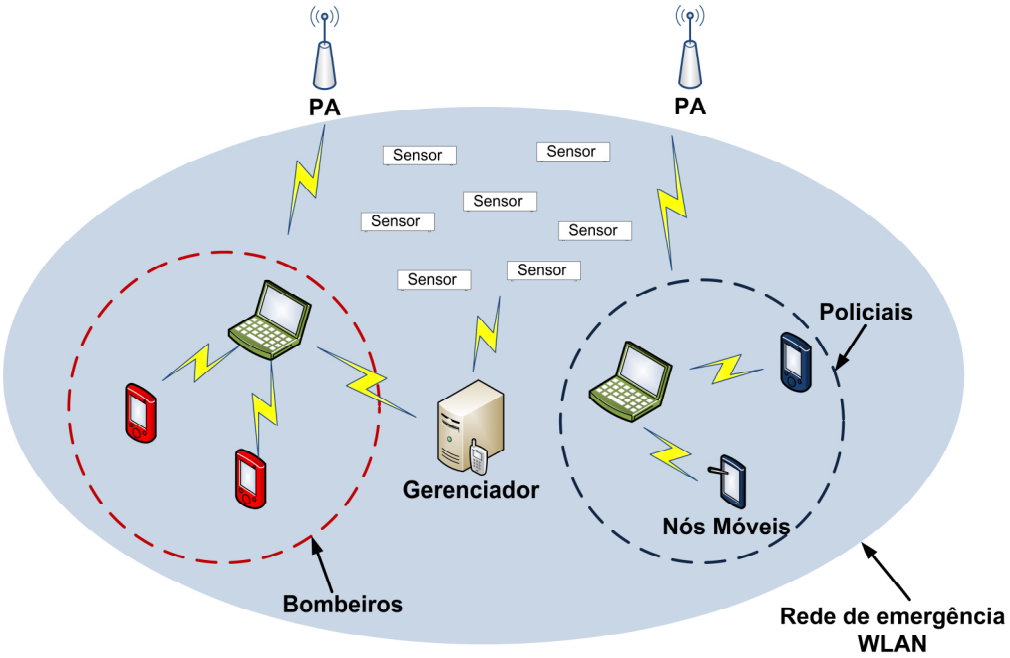

Figura 2.1. Exemplo do modelo de uma rede de emergência.

A Figura 2.1 ilustra os componentes da infra-estrutura da rede de emergência. Os nós se comunicam de modo ad hoc entre si e podem trocar dados. O acesso externo à Internet pode ser provido por pontos de acesso fixos com maior alcance de rádio (PA), utilizando tecnologias comerciais como wi-fi ou wimax [Mota, 2009].

As redes móveis *ad hoc* (MANETs) se encaixam no cenário pela ausência de infra-estrutura e necessidade de conexões entre dispositivos móveis, com utilização de um centro de controle com melhores recursos, roteadores sem fio, aparelhos móveis e nós sensores.

Dados cruciais e aplicações transmitidas em redes móveis sem fio devem possuir um alto grau de segurança. Principalmente devido à ausência de estações fixas e infra-estrutura pré-estabelecida, essas redes diferem consideravelmente das redes hierárquicas tradicionais. MANETs por exemplo, permitem que nós participem ou deixem a rede dinamicamente, algumas vezes sem deixar nenhum rastro.

Apesar das consequências de impedir a entrada de participantes sem autenticação, é válido evitar os efeitos negativos da inclusão de possíveis intrusos. Como participantes da rede, pode-se ter: ambulâncias, bombeiros, hospitais, veículos de transporte e agentes atuando nas áreas de desastre.

Objetiva-se neste trabalho propor soluções de segurança para redes de emergência com as seguintes características: *planas*, não há hierarquia de nós; *heterogênea*, com diversos tipos de dispositivos; *móveis*, com nós se deslocando na região abrangida pela rede; *com conectividade intermitente*, podendo haver perda de dados e atrasos na entrega de mensagens.

Para tratar o problema de segurança em redes de emergência, é necessário restringi-lo, considerando algumas premissas básicas:

- O centro de controle é confiável, ou seja, não está sujeito a ataques, e não apresenta restrições de recursos como os demais nós participantes da rede;

- O centro de controle é origem ou destino de todas as mensagens de gerenciamento da rede;
- Todos os participantes da rede são autorizados;
- É possível a captura de nós e inserção de nós adulterados, devido ao ambiente aberto e hostil;
- São possíveis a escuta e a criação de interferência, pois a comunicação é sem fio;
- Não existe conhecimento prévio de topologia de roteamento e localização, devido à distribuição aleatória dos nós;
- A rede é de larga escala, considerando redes de emergência com dezenas ou centenas de nós.

2.2. Redes Tolerantes a Interrupções (DTN)

2.2.1. Definição

Essas redes têm o objetivo de prover conexões entre dispositivos em áreas que não são bem dotadas da atual tecnologia de rede. Os protocolos de roteamento atuais necessitam da existência de um caminho fim-a-fim entre a origem e o destino. Além disto, o desempenho degrada consideravelmente com o aumento do número de saltos em uma comunicação sem fio [Ott, 2006].

Apesar de o termo DTN ser o mais utilizado na literatura, também podem ser encontradas outras terminologias, tais como: redes com conectividade eventual, redes móveis parcialmente conectadas, redes desconectadas, redes com conectividade transiente, redes incomuns, redes extremas e, mais recentemente, redes com desafios (CHAllenged NeTworkS - CHANTS) [Chen, 2006].

Características como baixa densidade de nós, altas taxas de erros de comunicação, alta latência, limitações de banda e longevidade de nós criam cenários desafiadores de rede, que na literatura são chamados de

Challenged Networks [Fall, 2003]. Essas características das redes fazem com que as aplicações nesses cenários tenham um comportamento diferente do que teriam em uma rede tradicional.

O conceito de DTN originalmente tem objetivo de dar suporte a comunicações intermitentes e com longos atrasos em redes que interligam pontos a longas distâncias, como no caso das redes interplanetárias. Para isso, Cerf et al. [2001] propuseram uma arquitetura capaz de suportar interrupções de comunicação utilizando armazenamento temporário de mensagens e reencaminhamento quando do retorno de conectividade. Foi definida uma nova camada de agregação (denominada *bundle*) para a arquitetura de rede.

Somente alguns dos nós podem estar conectados, enquanto os demais podem não ter conectividade. As possibilidades de comunicação podem se alterar a qualquer momento, devido a falhas, deslocamentos ou outros tipos de eventos.

Quando há conectividade entre nós, um nó tem oportunidade de enviar dados pela rede em direção a seus destinos finais. Tal oportunidade é chamada “contato” [Fall, 2003]. Um par de nós pode ter, ao mesmo tempo, vários contatos disponíveis, estabelecidos através de *links* físicos diferentes (*Wi-Fi*, *Bluetooh*, etc). A qualidade de cada um desses contatos pode oscilar devido a obstáculos e variações na distância entre os nós.

O RFC 4838 [Cerf, 2007] define a arquitetura de uma rede DTN como uma composição da pilha de camadas definida para a Internet (modelo OSI), acrescida de uma nova camada de agregação, denominada *bundle*, sobreposta à camada de transporte. A existência dessa camada comum permite que redes DTN sejam compostas por várias subredes heterogêneas, nas quais os protocolos de comunicação das camadas inferiores podem ser inteiramente distintos.

A Figura 2.2 apresenta as pilhas de protocolos da Internet e de uma rede DTN. Pode-se observar que os protocolos de comunicação da rede são específicos para cada sub-rede, que variam de acordo com o ambiente tecnológico em que estão operando, mas todas as sub-redes precisam

possuir a camada *bundle*, que irá fazer a interface entre a aplicação e as diversas tecnologias de comunicação entre as sub-redes.

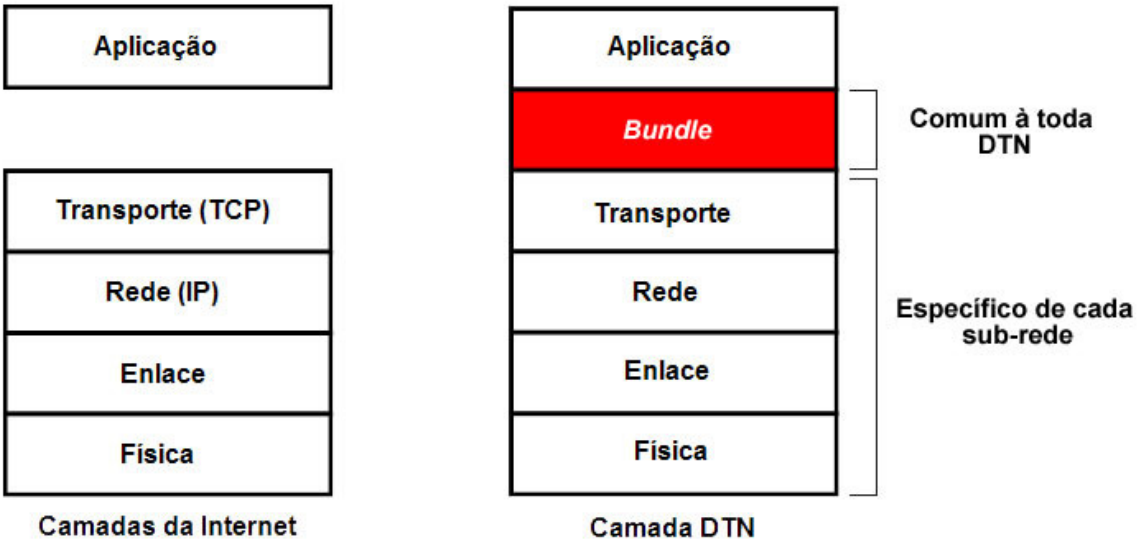

Figura 2.2. Pilha de protocolos da Internet e de uma DTN.

A arquitetura DTN propõe utilizar esse tipo de rede para encaminhar mensagens completas a cada salto. O roteamento da rede é feito da forma armazenar-carregar-repassar, ou seja, utiliza o paradigma *store-and-forward* [Fall, 2004]. Esse procedimento define que cada nó intermediário no caminho de uma mensagem deve armazená-la até que seja possível o estabelecimento de um contato com outro nó e o encaminhamento dessa mensagem armazenada, o que pode levar um longo tempo.

Um exemplo de ambiente onde os protocolos convencionais da Internet não funcionam são as redes ad hoc móveis (Mobile Ad hoc NETworks - MANETs) [Manet, 2008], onde a topologia da rede pode mudar constantemente quando a mobilidade dos nós é muito alta, provocando frequentes desconexões [Fall, 2005]. Outro exemplo são as redes de sensores sem fio, onde os nós precisam economizar energia e por isso permanecem desligados periodicamente, causando o particionamento da rede e conectividade intermitente. Assim, o caminho entre a origem e o destino pode não existir durante um período ou, ainda, pode ser que um caminho entre a origem e o destino nunca chegue a ficar completamente conectado. As características destes e de outros novos ambientes de rede

conduzem a uma série de desafios que precisam ser vencidos: freqüentes desconexões, atrasos longos e/ou variáveis (da ordem de horas ou dias), conectividade intermitente, recursos limitados dos dispositivos de comunicação, alta taxa de erros etc.

Segundo resumo de Oliveira et. al. [2007], as principais características encontradas nas Redes DTN são:

–atrasos longos e/ou variáveis: uma DTN pode chegar a ter atrasos da ordem de horas e, até mesmo, dias. O atraso fim-a-fim é determinado através da soma dos tempos de atraso salto-a-salto. Basicamente, é formado por quatro componentes: tempo de espera, atraso nas filas, atraso de transmissão e atraso de propagação [Jones, 2005]. A primeira componente corresponde ao tempo de espera de cada nó pelo nó de destino ou pela chegada de um nó intermediário que possa encaminhar as suas mensagens. O atraso nas filas corresponde aos atrasos variáveis que ocorrem nas filas dos nós antes de uma mensagem corrente ser entregue. Em seguida, existem o atraso de transmissão da mensagem e o atraso correspondente ao tempo de propagação do sinal (latência) a cada contato entre dois nós;

–freqüentes desconexões: desconexões podem ocorrer pela mobilidade que provoca constantes mudanças na topologia da rede, por péssimas condições de comunicação (desvanecimentos), por economia de recursos como em sensores sem fio onde sensores dormem para poupar energia, por negação de serviço como o ato do inimigo sujar a freqüência (jamming) em operações militares. Estes eventos podem resultar em uma conectividade intermitente da rede, ou seja, na inexistência de um caminho fim-a-fim entre um nó fonte e um nó de destino.

2.2.2. Protocolos de roteamento

Um desafio comum a todas as categorias de DTN é o roteamento, pois é preciso projetar protocolos capazes de superar os problemas dos atrasos

extremamente longos e das frequentes desconexões, já que os protocolos convencionais não estão aptos a manipular eficientemente a transmissão de dados em DTN [Mota, 2009]. É importante observar que é comum em DTN a necessidade de determinar rotas na rede sem que exista um caminho fim-a-fim entre a fonte e o destino no momento do envio.

A camada de agregação suporta a intermitência na comunicação ao isolar o atraso através da técnica de armazenagem-e-repasse, ou seja, um nó armazena uma mensagem até que seja possível repassá-la a outro nó. Há diferentes tipos de protocolos de roteamento DTN que definem o repasse da mensagem. Esses protocolos têm variações na política utilizada para escolher para quais nós vão repassar a mensagem para que essa chegue ao destino, de acordo com as características da aplicação e o modelo de mobilidade envolvido [Chaintreau, 2006].

Como existem vários tipos de DTN, diferentes soluções foram propostas na literatura. A seguir, são descritas as principais características, segundo Oliveira [2007], dos protocolos de roteamento mais reconhecidos para essas redes.

Protocolo Direct Delivery

Todos os demais protocolos transferem mensagens para outros nós com objetivo de atingir o destinatário final. O protocolo Direct Delivery não transfere nenhuma mensagem para outro nó, a menos que esse seja o destinatário final da mensagem. Esse pode ser considerado o algoritmo mais simples possível, pois um nó A envia uma mensagem para um nó B somente se esse for o destinatário da mensagem. Assim, esse esquema não possui limite para o atraso da entrega. A vantagem de sua utilização é que apenas uma única transmissão por mensagem é necessária.

Protocolo Spray and Wait

Esse protocolo cria somente um certo número de cópias de cada mensagem para serem transferidas para os outros nós. Normalmente, o

número de cópias é reduzido de 1 a cada transferência e, no modo binário, o número é dividido por 2. Somente mensagens que possuem mais de uma cópia restante são repassadas para outros nós que não são destinatários. Esse algoritmo limita o número de cópias e transmissões por mensagem sem comprometer o desempenho. Na primeira fase, é distribuído um número L de cópias da mensagem para L destinatários distintos. Se o destinatário não é encontrado nessa fase, cada um dos L nós que possuem a mensagem tentará uma entrega direta (Direct Delivery), enviando a mensagem somente se encontrar o nó destinatário. É um esquema simples, produz um número limitado de cópias de mensagens e proporciona uma boa taxa de entrega.

Protocolo Epidemic

O roteamento epidêmico é considerado a primeira proposta para redes caracterizadas por freqüentes desconexões e conectividade intermitente. É um protocolo de roteamento estocástico porque suporta a entrega eventual de mensagens a destinos arbitrários com suposições mínimas relativas ao conhecimento da topologia de rede. O trabalho propõe técnicas eficientes que garantem a entrega de mensagens até mesmo quando não existe um caminho totalmente conectado entre a fonte e o destino. Assim, esse protocolo pressupõe que um nó fonte não conhece onde o nó de destino está localizado e nem mesmo sabe qual a melhor rota para alcançá-lo. A idéia é que a mobilidade dos nós na rede possibilite que eles entrem no alcance de transmissão uns dos outros periodicamente e, o mais importante, de maneira aleatória. Logo, a mobilidade dos nós é utilizada como solução para a entrega de mensagens, ao invés de ser tratada como um problema que precisa ser superado na rede.

Somente a conectividade periódica par-a-par é necessária para assegurar a entrega de mensagens eventuais. Quando dois nós iniciam um contato, são trocadas listas com informações que identificam as mensagens armazenadas em cada nó. Essa troca é realizada para que o nó determine quais as mensagens existentes no buffer do nó vizinho que ele

ainda não possui. Depois que as mensagens são identificadas, cada nó solicita o envio das cópias das mensagens que ainda não possui. O processo de troca de mensagens se repete toda vez que um nó entra em contato com um novo vizinho, o que permite que as mensagens sejam rapidamente distribuídas pelas partes conectadas da rede. Assim, quanto mais cópias de uma mesma mensagem forem encaminhadas na rede, maior será a probabilidade da mensagem ser entregue e menor será o atraso.

Quanto mais nós existirem na DTN, maior é a probabilidade do destino ser alcançado em um menor tempo. As principais desvantagens são alto custo em termos do número de retransmissões e consumo dos recursos dos nós. De acordo com o limite do buffer, a replicação de mensagens pode diminuir a taxa de entrega.

Protocolo PRopHet

Protocolo de roteamento probabilístico utilizando históricos de encontros e transitividade (Probabilistic Routing Protocol using History of Encounters and Transitivity - PROPHET). Assim como acontece no roteamento epidêmico, quando dois nós iniciam um contato são trocadas as listas com informações que identificam as mensagens armazenadas em cada nó. A diferença é que agora existe uma informação extra para cada mensagem indicada na lista. Essa informação corresponde à probabilidade de cada nó a entregar mensagens para um destino conhecido b ($P(a,b) \in [0,1]$). O valor de P(a,b) aumenta sempre que a e b se encontram. Se a e b deixam de se encontrar freqüentemente, P(a,b) diminui à proporção que o tempo transcorre. [Oliveira, 2007].

Esse tempo é controlado por uma constante k denominada constante de envelhecimento, que corresponde ao número de unidades de tempo transcorridas desde a última vez que a métrica foi atualizada. A probabilidade de entrega também possui uma propriedade transitiva, que se baseia na seguinte observação: se um nó a encontra um nó b freqüentemente, e o nó b encontra freqüentemente um nó c, logo o nó c

provavelmente é um bom nó para encaminhar mensagens destinadas para a. Uma constante β (β ∈ [0,1]) é utilizada para definir o impacto da transitividade na entrega. Quando um nó recebe a lista do vizinho, ele calcula a probabilidade de entrega para cada uma das mensagens que ainda não possui armazenada. Em seguida, para cada mensagem, o nó compara a probabilidade indicada na sua lista com a probabilidade indicada na lista recebida do vizinho. Essa comparação é realizada para verificar qual dos dois nós possui a maior probabilidade de entrega. Feita essa comparação, devem ser realizados três procedimentos. Primeiro, o nó deve enviar um pedido das mensagens não armazenadas que possuem uma maior probabilidade de serem entregues através dele. Segundo, recebe o pedido de mensagens do vizinho e as envia.

Terceiro, apaga do buffer todas as mensagens que o vizinho tem maior probabilidade de entregar. No final, cada nó só ficará com as mensagens cujas probabilidades de entrega sejam maiores através dele. Os resultados das simulações demonstram que o PROPHET é capaz de entregar mais mensagens do que o roteamento epidêmico e com uma sobrecarga de comunicação menor, especialmente quando o alcance de comunicação dos nós é pequeno. Isso se deve ao fato do PROPHET enviar mensagens somente para os melhores nós, enquanto o epidêmico envia mensagens para todos os nós que encontra. Estratégias de descarte de mensagens baseadas na estimativa da probabilidade de entrega também podem ser utilizadas para aumentar o desempenho da rede quando os nós possuem buffers limitados.

2.3. Trabalhos relacionados

Existem vários exemplos na literatura da importância da utilização de recursos de comunicação para resposta a desastres, como em Mehrotra [2008]. Já foram propostas várias aplicações para redes de emergência [Chitumalla, 2008]. O Sahana [Currion, 2007] é comumente citado por ser

um sistema de gerenciamento de desastres de código aberto, ainda em desenvolvimento.

Uma arquitetura para redes de emergência e alguns requisitos de segurança foram propostos em Portmann & Pirzada [2008]. Segundo o estudo, muitos dos protocolos de segurança existentes não funcionarão bem se colocados para operar em redes de emergência. Muitas vezes será impossível entrar em contato com o servidor de interesse ou ter conectividade por um período suficientemente longo para transferir o material para a autenticação necessária.

Adicionar aspectos de segurança tem sido um foco maior na camada de agregação das redes DTN [Fall, 2004]. O interesse em segurança varia dependendo do ambiente e aplicação, embora autenticação e privacidade sejam geralmente críticos [Portmann, 2008]. Essas garantias de segurança são difíceis de serem estabelecidas em uma rede sem conectividade persistente porque a rede utilizaria protocolos de criptografia complexos, troca de chaves, e cada nó teria de identificar outros nós esporadicamente visíveis.

O modelo de segurança para a arquitetura DTN difere das redes tradicionais, pois o conjunto de participantes inclui os próprios roteadores [Fall, 2003]. A maior parte das técnicas de segurança envolve a autenticação mútua e a troca de dados restrita entre dois usuários da rede, deixando o restante da rede sem participação nesse processo. No caso de redes DTN, há maior interesse em verificar o acesso para o encaminhamento do tráfego para uma classe particular de serviço e espera-se evitar o encaminhamento por longas distâncias de tráfego que depois será considerado proibido.

Várias das propostas de segurança existentes requerem numerosas trocas de informações entre partes e envolvimento de um terceiro elemento confiável, ou requerem que sejam trocadas credenciais de autenticação relativamente grandes antes de se iniciar a comunicação [Seth, 2005].

Em geral, soluções de redes móveis *ad hoc* vêm sendo alteradas para adaptação a redes DTN e existem pesquisas de segurança distribuída,

como o uso de autoridades certificadas distribuídas [Burgess, 2007]. Soluções originais da comunidade de pesquisa de redes tolerantes a atrasos e desconexões incluem o uso da encriptação baseada na identidade [Seth, 2005] [Kate, 2007], que permite aos nós receber informação criptografada com seu identificador público.

Entre as propostas que têm sido publicadas relativas à segurança em redes DTN, em Symington et al. [2009] foram apresentadas algumas idéias preliminares sobre a distribuição e gerenciamento de chaves para DTN, mas percebe-se que ainda são questões abertas.

Em Durst et al. [2002], sugere-se que o usuário DTN apresente sua chave pública para uma autoridade certificadora DTN para obter uma cópia assinada daquela chave e um conjunto de credenciais assinado para autorizar o usuário a utilizar serviços específicos, o que seria necessário apresentar para um roteador antes de poder utilizar o seu serviço.

Assim como Lorincz [2004], este trabalho considera também a integração de redes de sensores sem fio (RSSF) a redes de emergência. Para tanto, propõe que os nós sensores utilizem o modelo de gerenciamento de segurança proposto para RSSF em Oliveira et al. [2008], bem como suas definições para os sensores.

As características e desafios do cenário de redes de emergência são apresentados em Asplund [2008], bem como a possível utilização dos mecanismos de segurança de DTN após análise em redes de emergência. Tanto quanto podemos saber, não existe na literatura alguma proposta específica para segurança em redes de emergência.

Em Walle [2008], apresenta-se a necessidade de gerenciamento para possibilitar a melhor utilização de recursos de redes de emergência. Porém, não foi encontrada uma abordagem de provimento de segurança que seja dinâmica e considere os objetivos ou restrições de recursos das redes de emergência.

Capítulo 3

Segurança em Redes de Emergência

Este trabalho propõe um modelo para o gerenciamento de segurança adaptativo para redes de emergência. Para tanto, é necessário um estudo sobre os requisitos de segurança, os mecanismos já existentes e a sua possível integração, o que é apresentado nesse capítulo.

O uso de mecanismos de segurança em redes de emergência se justifica na quase totalidade das aplicações, especialmente as militares ou aquelas nas quais as informações pessoais são tratadas, sendo necessário manter a privacidade das pessoas monitoradas.

Um intruso é considerado como uma entidade interna (nó malicioso) ou externa à rede [Burgess, 2007], que age sobre a rede de forma ativa, modificando, suprimindo ou inserindo pacotes de mensagens trafegadas, impedindo assim o funcionamento correto desta rede. Esta entidade também pode agir de forma passiva, obtendo sem autorização informações sigilosas das mensagens trafegadas em uma determinada rede.

O intruso passivo pode ser um analisador de pacotes sigilosos que trafegam em uma determinada rede. O ativo, ao contrário, poderia injetar falsos pacotes na rede. Já um intruso interno poderia ser um nó da rede capturado que sofreu modificação em seu hardware ou software. De maneira oposta, o intruso externo é um indivíduo que não tem permissão de acesso, contudo pode conseguir esta permissão através de falhas nos sistemas.

A detecção de intrusos é normalmente acompanhada da revogação do nó intruso. A revogação representa a exclusão do nó da rede, eliminando as possibilidades de comunicação desse nó com seus vizinhos. Esse processo deve ser autenticado, para evitar que nós intrusos promovam a revogação dos nós autênticos. Como os nós não são protegidos contra *tampering* (violação física) no modelo utilizado, é bem mais seguro permitir que apenas o centro de controle promova a revogação de nós. Do contrário, um nó intruso que possa ser autenticado pela rede, provavelmente originado numa ação de *tampering*, poderia agir revogando nós autênticos, promovendo assim outro ataque do tipo *negação de serviço*.

A segurança em redes de emergência é uma tarefa mais árdua que a segurança de redes sem fio tradicionais. A limitação de recursos conjugada com outras características das redes tolerantes a interrupções faz com que a segurança nessas redes possua características peculiares.

Segundo o RFC 4838 [Cerf, 2007], mecanismos propostos para essas redes devem objetivar o atendimento dos seguintes requisitos:

–Prevenção contra o envio e armazenamento, pelos membros da rede, de dados de aplicações não autorizadas;

–Prevenção contra o envio de dados e a alocação de recursos maiores que os permitidos por aplicações autorizadas;

–Descarte de pacotes modificados de maneira maliciosa durante seu roteamento;

–Detecção e remoção de membros maliciosos.

Portanto, os requisitos de segurança são essenciais às redes de emergência, uma vez que garantem a privacidade entre os nós que fazem parte da rede, além de impedirem o uso indevido e o acesso não autorizado às informações.

3.1. Requisitos de segurança

Questões de confiança, envolvendo segurança, privacidade e confiabilidade devem ser consideradas no cenário de desastres. Os recursos de resposta a desastres devem prover diferentes níveis de segurança, garantia e confiabilidade baseados nas necessidades dos usuários finais e suas aplicações como transmissões de dados médicos e privacidade de pacientes na rede. Devem ser considerados os aspectos [Asplund, 2008]:

- **Heterogeneidade das partes envolvidas:** um grande desastre envolverá várias entidades governamentais (locais, estaduais e federais), empresas e cidadãos. Redes de emergência têm de reagir a diferentes políticas de segurança e confiança que podem não ser compatíveis e esconder dados compartilhados e outros recursos. Esse problema pode ser mais complexo se outros países são envolvidos.
- **Flexibilidade:** respostas aos desastres podem requerer modificações flexíveis no tempo ou violação de políticas de segurança e confiança. Por exemplo, uma equipe médica de emergência pode precisar de acesso às informações de um paciente que não estariam disponíveis sem autorização.
- **Reutilização de tecnologias:** tecnologias podem ser projetadas para realizar ações em crises que não são suas funções primárias. Pode haver necessidade de elas serem projetadas então para não serem suscetíveis a invasões de terceiros durante o tempo de operação da rede de emergência.
- **Alarmes falsos:** deve ser considerada a detecção de um alarme falso por um intruso e a rede deve ser capaz de identificar tal intruso.

Em redes avançadas nas quais a comunicação foge dos padrões, a capacidade das conexões é um recurso precioso e o acesso ao serviço de encaminhamento de dados deve ser protegido por alguns mecanismos de controle de acesso, pelo menos em pontos críticos da topologia.

Os requisitos de segurança para uma rede de emergência dependem da sua aplicação. Redes de missão crítica podem necessitar de confidencialidade, autenticidade, integridade, frescor e disponibilidade. Dada a diversidade de hardware possivelmente atuante, eles não podem contar com resistência contra captura e adulteração. Assim, a captura de um nó pode comprometer a segurança da rede, revelando informações como chaves, ou mesmo permitindo a reprogramação do nó, tornando-o uma ferramenta de ataque de um inimigo.

Muitos ataques são facilitados se o intruso conseguir influenciar o estabelecimento de rotas na rede, manipulando a comunicação entre nós legítimos. Essa manipulação inclui injeção de mensagens maliciosas na rede, replicação de mensagens antigas e modificação do conteúdo de mensagens válidas. Um objetivo do intruso, nesse caso, pode ser obter informações destinadas ao centro de controle.

Pode-se proteger as redes de emergência contra alguns tipos de ataques, utilizando-se mecanismos preventivos. Para prevenir que nós adversários se façam passar por membros legítimos de uma rede, por exemplo, podem ser utilizados mecanismos de identificação baseados em métodos criptográficos. Existem, entretanto, ataques para os quais não são conhecidos mecanismos de prevenção. Para esses casos, a rede precisaria de um sistema de detecção de intrusos. Mesmo para ataques para os quais já existam mecanismos de prevenção, a necessidade desse sistema se justifica porque mesmo os mecanismos mais eficazes de prevenção podem falhar.

Enquanto vários protocolos de segurança têm sido propostos na literatura para prover autenticação e controle de acesso em pontos múltiplos da rede, a maior parte deles não é tolerante a longas latências. Em particular, protocolos que requerem múltiplas trocas de informações ou múltiplas interações entre cliente e servidor para alcançar a segurança objetivada não serão apropriados para redes avançadas com freqüentes e longas desconexões [Seth, 2005].

Os problemas de segurança podem estar presentes na forma de acesso, especialmente sem fio, em falhas nos protocolos de comunicação,

em falhas no software ou no hardware dos mecanismos de coleta e envio de dados, ou na adulteração de nós da rede.

A resposta da rede deve ser diferente quando ocorrer uma falha ou uma invasão. No caso de uma falha, a rede deve tentar contornar o problema identificando outro nó que possa assumir a função do nó com falha. Uma atualização na árvore de roteamento pode resolver o problema, ocasionado por uma falha, em relação ao roteamento. No caso de uma intrusão, a rede deve isolar o nó intruso. A execução da atualização do roteamento não elimina o intruso, pois ele está preparado para participar dessa atualização. Assim, faz parte dos objetivos deste trabalho permitir que as redes de emergência continuem funcionando normalmente, mesmo sob a ação de um ataque.

Permitir aos usuários que expressem aspectos da importância das mensagens da rede pode ser um benefício considerável, tanto para os usuários quanto para a infra-estrutura da rede que os suporta [Fall, 2004]. Dois aspectos que caracterizam a preferência dos usuários são uma noção de vida útil e uma relação de prioridade entre as mensagens, de forma que uma mensagem deve ser entregue antes de outra, se possível. Num caso de determinada mensagem ser útil somente para os próximos minutos, ela poderia ser descartada sem problemas caso não seja possível entregá-la nesse tempo.

Na maior parte dos sistemas de mensagens atuais, nenhum desses aspectos é tratado eficientemente. No caso da prioridade, indicadores relativos são tipicamente usados somente para sinalizar o destinatário (exclamações vermelhas, por exemplo), e o tempo restante pode ser especificado somente em um dos extremos (destinatários decidem quando descartar e-mails, por exemplo, enquanto mensagens instantâneas são descartadas se o destinatário não estiver disponível imediatamente).

Percebe-se que os requisitos de segurança para uma rede de emergência podem variar de acordo com as situações e cenários em que ela é utilizada, logo é necessário prover confiabilidade, garantia e flexibilidade nos aspectos de segurança, baseados nas necessidades dos usuários finais e suas aplicações. Os recursos de resposta a um desastre

devem ser auto-gerenciáveis, de forma que evitem sua utilização por agentes externos à rede.

3.2. Mecanismos de segurança

Diversos mecanismos podem ser usados para evitar a ação de um inimigo em uma rede de emergência. O *controle de acesso* à rede pode impedir a entrada de nós intrusos, a *detecção de intrusos* pode apontar os nós intrusos em ação na rede e, finalmente, *mecanismos de revogação* de nós podem isolar os nós intrusos, de forma que sua ação não tenha mais efeito. Através da detecção de intrusão, é possível verificar que um mecanismo de defesa foi violado, possibilitando a reação automática.

A sobreposição de mecanismos de segurança é necessária porque nenhum desses mecanismos consegue garantir eficácia total. Mecanismos de segurança usados em redes convencionais, como criptografia, só podem ser usados em redes de emergência se observadas às restrições de comunicação, energia e processamento.

Para redes tolerantes a interrupções (DTN) com recursos de conexão preciosos, uma técnica fim-a-fim para segurança não é muito atrativa, elevando o interesse por alternativas salto-a-salto. Primeiramente, técnicas fim-a-fim tipicamente requerem alguma troca de chaves ou informações, o que seria indesejável.

Além disso, é indesejável transportar tráfego inesperado por todo o caminho para seu destino sem realizar autenticação e checagem de controle de acesso. Esse continua como um problema da Internet, que pode ser visto pela grande coleção de técnicas que tentam determinar o problema de tráfego por todo o caminho de volta à sua origem.

Adicionar aspectos de segurança tem sido um foco maior no protocolo *bundle* para redes DTN. O interesse em segurança varia dependendo do ambiente e aplicação, embora autenticação e privacidade sejam geralmente críticos. Essas garantias de segurança são difíceis de

estabelecer em uma rede sem conectividade persistente porque a rede utilizaria protocolos de criptografia complexos, troca de chaves, e cada nó teria de identificar outros nós esporadicamente visíveis.

O modelo de segurança para a arquitetura DTN difere das redes tradicionais, pois o conjunto de princípios inclui os próprios roteadores. A maior parte das técnicas de segurança envolve a autenticação mútua e a troca de dados restrita entre dois usuários da rede, deixando o restante da rede sem participação. No caso de redes DTN, há maior interesse em verificar o acesso para o encaminhamento do tráfego para uma classe particular de serviço e espera-se evitar o encaminhamento por longas distâncias de tráfego que depois será considerado indevido.

Em geral, soluções de redes móveis *ad hoc* vêm sendo alteradas para adaptação a redes DTN e existem pesquisas de segurança distribuída, como o uso de autoridades certificadoras distribuídas [Burgess, 2007]. Soluções originais da comunidade de pesquisa de redes tolerantes a atrasos e desconexões incluem o uso da encriptação baseada na identidade [Seth, 2005] [Kate, 2007], que permite aos nós receberem informação criptografada com seu identificador público.

A escassez de recursos em redes avançadas indica que alguma forma de autenticação e controle de acesso é necessária, e que essa utilização deve ser aplicada o quanto antes possível ao longo da cadeia de roteadores usada para entregar a mensagem [Fall, 2004]. De outra forma, recursos preciosos podem ser utilizados para carregar mensagens que serão descartadas futuramente, quando alcançarem o seu destinatário.

Várias propostas de segurança existentes requerem numerosas trocas *round-trip* entre partes e algum terceiro confiável, ou requerem que sejam trocadas credenciais de autenticação relativamente grandes antes de iniciar a comunicação [Seth, 2005]. Muitos desses protocolos não funcionarão bem se colocados para operar em redes de emergência. Muitas vezes será impossível entrar em contato com o servidor de interesse ou ter conectividade por um período suficientemente longo para transferir o material para a autenticação necessária [Portmann, 2008].

Em redes de emergência, espera-se não somente limitações de recursos de rede e conectividade, mas também altas taxas de erros. Quando as taxas de erro são suficientes para causar perda de pacotes, dois métodos são comumente usados para corrigir o problema: retransmissão e técnicas de codificação [Fall, 2004]. Para redes em que essas taxas são altas, é improvável que retransmissão fim-a-fim seja eficaz e deve então ser implementada utilizando alguma técnica salto-a-salto.

Um salto refere a um salto entre agentes responsáveis pelo encaminhamento da mensagem, em qualquer camada que isso seja implementado. Isso é válido para os agentes de roteamento de e-mails atual, por exemplo, quando mensagens são retransmitidas um número máximo de vezes antes de ser declarada uma falha.

3.3. Detecção de intrusos

Diversos mecanismos podem ser usados para evitar a ação de um inimigo. O controle de acesso à rede pode impedir a entrada de nós intrusos, a detecção de intrusos pode apontar os nós intrusos em ação na rede e, finalmente, mecanismos de revogação de nós podem isolar os nós intrusos, de forma que sua ação não tenha mais efeito. Através da detecção de intrusão [Burgess, 2007], é possível verificar que um mecanismo de defesa foi violado, possibilitando a reação automática.

Os problemas de segurança podem estar presentes na forma de acesso, especialmente sem fio, em falhas nos protocolos de comunicação, em falhas no software ou no hardware dos mecanismos de coleta e envio de dados, ou na adulteração de nós. Porém, o requisito de segurança mais difícil de ser atendido é a disponibilidade. Ataques contra a disponibilidade podem estar presentes nas diversas camadas de protocolos, especialmente pela facilidade de execução e pelo impacto sobre a aplicação, que pode ser parcial ou totalmente inutilizada. Estes

ataques são conhecidos por negação de serviço ou *Denial of Service* (DoS) [Hu, 2003].

A detecção de ataques em uma rede depende da distinção entre normalidade e anormalidade, de forma a distinguir os padrões de ataque previstos. Também é necessário identificar o tráfego esperado e a demanda da rede como uma base para avaliação de novos protocolos de roteamento e descobertas de nós ou perdas de conexões.

Assim como ataques de negação de serviço distribuídos são ameaça para a Internet, a proteção e o controle de acesso à infra-estrutura da rede é crítico em redes DTN, que tipicamente apresentam desafios em termos de recursos, sendo extremamente necessária a capacidade de manter a comunicação sofrendo esses ataques. Como essas redes sofrem impacto de altos tempos de resposta, baixa taxa de conexões e freqüentes partições, eficiência é um fator importante em qualquer solução de segurança.

As reações de uma rede a um ataque podem ser muito diferentes. Por exemplo, na presença de um ataque de negação de serviço no roteamento, a rede pode se comportar de diversas formas: pode continuar funcionando normalmente, sem permitir o acesso do intruso à rede, tampouco sofrer os efeitos da sua presença; pode reduzir a produção da rede, silenciando alguns nós, ou até mesmo interromper o funcionamento de toda rede, inutilizando seu uso. Assim, faz parte dos objetivos deste trabalho permitir que as redes de emergência continuem funcionando normalmente, mesmo sob a ação de um ataque.

Pode-se proteger as redes contra alguns tipos de ataques utilizando-se mecanismos preventivos. Para prevenir que nós adversários se façam passar por membros legítimos de uma rede, por exemplo, podem ser utilizados mecanismos de identificação baseados em métodos criptográficos. Entretanto, existem ataques para os quais não são conhecidos mecanismos de prevenção, um exemplo é o ataque de canalização (*wormhole*). Para esses casos, a rede precisaria de um sistema de detecção de intrusos (IDS). Mesmo para ataques para os quais já

existam mecanismos de prevenção, a necessidade de um IDS se justifica porque mesmo os mecanismos mais eficazes de prevenção podem falhar.

Uma mensagem de presença de intruso deve colocar a rede em estado de alerta e pode ser usada também pelo intruso na tentativa de confundir a rede. Como é impossível decidir sobre qual é o nó intruso, a rede deve reduzir as possibilidades de comunicação.

3.3.1. Tipos de ataques

Diversas formas de intrusão vêm sendo documentadas na literatura [Engel, 2006] para redes móveis *ad-hoc* e podem ser consideradas no contexto de redes de emergência. Como o intruso pode ter acesso físico aos nós, eles podem ser violados fisicamente. A violação física (*tampering*) pode visar modificação, substituição ou destruição de hardware ou software. Assim, o intruso pode ter o intuito de obter informações secretas, como chaves criptográficas, ou de levar os protocolos a um comportamento anômalo, prejudicando a aplicação. Outra classe de ataques consiste na exaustão dos recursos da rede. Num ataque de exaustão (*exhaustion*), o intruso poderia, por exemplo, levar um nó a fazer um número elevado de transmissões, desperdiçando sua energia.

Geralmente, dois tipos de ataques podem ser lançados contra a segurança de redes *ad-hoc* móveis sem fio, passivos e ativos. O adversário descansa sem ser notado na rede enquanto promove um ataque passivo, sem perturbar as funções do protocolo, e escutando toda a informação útil sobre a rede e os nós participantes. Em ataques ativos, o intruso perturba o correto funcionamento do protocolo de roteamento modificando alguma informação ou promovendo ataques de negação de serviço. É importante utilizar mecanismos que permitam isolar esses nós maliciosos através da detecção do comportamento indevido. Os ataques ativos podem ser divididos em três categorias [Engel, 2006].

Ao promover um ataque de integridade, o nó malicioso perde mensagens, redireciona tráfego para um destino diferente, ou informa longas rotas com objetivo de aumentar o atraso na comunicação. O ataque

mais famoso nessa categoria é a criação de um *blackhole*, onde um intruso absorve todos os pacotes que passam por ele. As rotas podem ser influenciadas pelo intruso, sendo um nó invasor ou um nó legítimo, já violado, no ataque buraco negro (*blackhole* ou *sinkhole*). Nesse caso, o intruso deseja obter informações da rede ou aplicar o ataque de negligência. Como uma forma de extensão, o intruso pode promover um ataque *greyhole*, permitindo alternar entre encaminhar pacotes ou descartá-los.

Uma mensagem disponível num ponto da rede pode ser enviada para outro ponto distante, com o estabelecimento de um túnel na rede entre dois ou mais nós que colaboram de forma que os intrusos sejam ligados por uma rede privada, assim o *wormhole* permite ao intruso interferir no fluxo normal dos pacotes. Essa canalização é uma manipulação de comunicação, pois pode levar uma mensagem a um ponto da rede aonde ela não chegaria, ou chegaria com uma latência maior. Assim, o intruso conseguiria influenciar rotas, e, em conjunto com outros ataques, omitir informações, prejudicando a aplicação. Após redirecionar os pacotes para outro ponto da rede móvel *ad-hoc* sem fio, o intruso replica ele na rede.

Muitos ataques são facilitados se o intruso conseguir influenciar o estabelecimento de rotas na rede, manipulando a comunicação entre nós legítimos com replicação de mensagens antigas, injeção de mensagens maliciosas na rede ou modificação do conteúdo de mensagens válidas.

Ataques do tipo *tampering* são baseados na distribuição de mensagens de roteamento falsas e são difíceis de identificar e rastrear. O ataque *rushing* é um exemplo de ação como um ataque efetivo de negação de serviço contra todos os protocolos de roteamento de redes *ad-hoc* sob demanda propostos atualmente. Promovendo esse ataque, o adversário rapidamente espalha mensagens de roteamento por toda a rede, desabilitando mensagens de roteamento autorizadas com a conseqüência que outros nós as deletam como cópias replicadas. Obviamente, rotas computacionais para algum destino também podem ser canceladas pela montagem de mensagens de erro de roteamento, afirmando que o vizinho não pode ser alcançado. Logo, como difusão é mecanismo mais comum

usado por protocolos de roteamento sob demanda para estabelecer rotas, perturbar a difusão é um ataque eficiente contra esse tipo de protocolo.

Outro tipo de ataque é promovido quando o adversário tem objetivo de adotar alguma outra identidade na rede para parecer confiável. Consequentemente, ele pode operar como um nó da rede e divulgar informações incorretas de roteamento por exemplo. Um ataque perigoso é conhecido como *sybil* onde nós maliciosos podem não somente representar outros nós como multiplicar identidades falsas. Redes móveis que utilizam algum modelo de confiança são particularmente vulneráveis a esse ataque, pois o intruso pode gerar recomendações falsas sobre a confiabilidade de um nó específico para atrair mais tráfego da rede para ele, o que oferece um ponto de partida ideal para ataques *wormhole*.

Ao simular várias identidades através de ataques de *sybil*, seria possível atrapalhar os protocolos de roteamento e, assim, prejudicar o envio de mensagens. Outras formas de ataques são possíveis se o intruso conseguir inserir-se na rede, fazendo se passar por um nó legítimo. Seria possível, por exemplo, comprometer o roteamento das mensagens através de ataques de negligência (*neglect and greed*) ou retransmissão seletiva (*selective forwarding*). O intruso ignoraria seu papel de roteador, deixando de retransmitir algumas mensagens.

Caso o inimigo descubra as informações secretas da rede e insira estas informações em um nó estranho à rede, sendo aceito como membro da rede, é caracterizado um ataque interno. Já um ataque realizado por um computador portátil estranho à rede, é considerado um ataque externo. Nesse caso, ele não possui informações que são importantes para o funcionamento da rede, como as chaves e não consegue provar que é membro da rede.

Alguns desses ataques podem ser prevenidos. Pode-se prevenir injeção de mensagens maliciosas, replicação de mensagens antigas e modificação do conteúdo de mensagens válidas, através do uso de protocolos criptográficos bem projetados. Entretanto, existem ataques que são difíceis de serem prevenidos; para estes casos e para os casos onde os

mecanismos de prevenção forem comprometidos, a utilização de um sistema de detecção de intrusos torna-se primordial.

3.3.2. Revogação de nós

A detecção de intrusos é normalmente seguida da revogação dos nós com comportamento indevido. A revogação é a exclusão do nó da rede, tornando impossível para ele a comunicação com seus vizinhos. Esse processo deve ser autenticado para evitar a revogação de nós autênticos por intrusos. Como os nós não são protegidos contra violação física no modelo utilizado nesse trabalho, é mais seguro permitir somente ao centro de controle promover a revogação de nós. De outra forma, um nó intruso autenticado pela rede, provavelmente originado de uma violação física, poderia isolar nós autênticos, promovendo outros tipos de ataques de negação de serviço.

3.4. Roteamento dinâmico seguro

O roteamento é uma tarefa crítica porque um inimigo pode se inserir na rede para promover um ataque de negação de serviço. A maior parte dos protocolos de roteamento propostos para redes DTN não considera o aspecto da segurança como um dos objetivos principais. Consequentemente, esses protocolos são mais suscetíveis a ataques que redes *ad hoc* em geral. Assim, torna-se importante considerar o roteamento como um dos mecanismos principais para garantir a segurança da rede.

Os protocolos de roteamento mais reconhecidos para redes DTN foram considerados, conforme descritos anteriormente [Oliveira, 2007]: *Direct Delivery*, repasse de mensagens somente ao destinatário; *PRopHet*, repasse das mensagens para nós com maior probabilidade de entrega; *Epidemic*, distribuição de cópias das mensagens para toda a rede; *Spray*

and Wait, distribuição de um número determinado de cópias para cada mensagem, que é dividido por dois a cada salto no modo binário [Mota, 2009].

O ataque mais simples consiste em descartar todos os pacotes que um nó recebe. Para protocolos de repasse, cada descarte é um pacote perdido, pois não há cópia em outros nós. A melhor defesa em redes DTN contra ataques de perda maliciosa de pacotes é o uso de caminhos múltiplos.

Um intruso pode inundar continuamente a rede com envio de pacotes para qualquer nó e nunca repassar qualquer pacote recebido de outros nós. O uso de *flags* para indicar replicação de maior prioridade pode auxiliar nesse caso. Indicadores podem ser utilizados para caracterizar urgência e conseqüente tempo de vida (TTL) das mensagens, pois há mensagens que perdem o sentido se não forem entregues em certo espaço de tempo.

Dentro de um contexto emergencial, acontecem situações de urgência e de prioridade nas comunicações. Assim, temos:

- **Urgência:** situação em que o contato em que a rapidez é imprescindível.
- **Prioridade:** quando o contato é preferencial, numa série ou ordem, só superado por uma urgência.

As aplicações que utilizam a rede de emergência podem obrigar a definição de prioridade das mensagens, por exemplo: Baixa, Média, Alta ou Urgente. Mensagens definidas como urgentes possuirão um tempo de vida determinado pelo centro de controle e inferior ao das demais, para descarte após término desse tempo.

Confirmações de recebimento (*acknowledgments*) representam um mecanismo muito eficiente para entrega de pacotes em protocolos de roteamento replicativos e, por conseguinte, podem ser utilizados como um método efetivo de sabotagem. O uso de criptografia pode impedir um intruso de propagar uma falsa confirmação.

Em alguns protocolos de roteamento, tabelas de frequências de contato dos nós são propagadas em uma forma replicada de cada nó para

todos os outros [Mota, 2009]. Sem autenticação, intrusos podem propagar informações incorretas sobre as tabelas de roteamento de qualquer nó.

3.5. Mecanismos de prevenção de acesso

O uso de criptografia com gerenciamento adequado de chaves é necessário para obter vários requisitos de segurança. A criptografia pode ser usada de forma a ocultar as informações do inimigo, garantir a autenticidade da informação ou ainda garantir a integridade e o frescor dos dados. As informações podem ser criptografadas para serem transmitidas por um meio não seguro ou então para serem armazenadas em um sistema cujo acesso tem segurança duvidosa.

Em algumas aplicações, a encriptação e a assinatura dos dados fim-a-fim podem ser suficientes para garantir os requisitos de segurança. A encriptação e a assinatura de dados fim-a-fim não podem ser usadas para mensagens enviadas em difusão, ou mensagens que devem ser tratadas a cada passo do roteamento, como as mensagens de estabelecimento de rotas.

Quando os métodos criptográficos fim-a-fim não podem ser usados, uma alternativa é usá-los a cada passo do roteamento, através de encriptação e assinatura salto-a-salto. Nesse caso, é necessário um compartilhamento de chaves entre os vários nós que precisam se comunicar diretamente para a execução do roteamento. Essa abordagem pode evitar a entrada de intrusos no roteamento, caso eles não possuam as chaves necessárias para a realização dos processos criptográficos.

3.5.1. Encriptação

Protocolos DTN devem prover um meio de encriptar elementos de forma que mensagens em trânsito não possam ser lidas por terceiros. O protocolo de agregação não provê nenhuma confidencialidade para a

origem ou destino [Fall, 2003]. Similarmente, protocolos DTN devem possibilitar a aplicação de uma verificação de integridade de maneira que a identidade do nó origem seja provada e alterações em partes específicas da mensagem possam ser detectadas.

A criptografia pode ser usada para garantir privacidade, através da encriptação dos dados. Durante muito tempo, o termo criptografia referiu-se exclusivamente a encriptação, que é o processo de converter uma informação comum (texto plano) em algo não-inteligível, o qual se nomeia texto cifrado e é utilizado para prevenir a leitura e o entendimento do dado por um usuário não autorizado. A decriptação é a tarefa contrária, dado uma informação não-inteligível convertê-la em texto plano.

A encriptação é feita com o uso de um algoritmo e uma chave. O algoritmo, usando a chave, converte um documento normal em um documento cifrado. Quando o emissor cifra um documento, o documento só pode ser decifrado pelo receptor que possuir o algoritmo de deciframento e a chave. Este processo é conhecido como criptografia simétrica porque a mesma chave deve ser utilizada pelo emissor e receptor. Assim, a chave deve ser compartilhada e, se uma das partes, por descuido ou não, divulgar a chave, o sigilo estará comprometido. Outro problema da criptografia simétrica é a multiplicação das chaves, uma vez que por motivo de segurança, para cada par emissor/receptor deve existir uma chave diferente.

Para resolver os problemas do compartilhamento e multiplicação das chaves, utiliza-se a criptografia assimétrica onde são geradas duas chaves, uma pública e uma privada. Estas chaves são matematicamente relacionadas de forma que qualquer uma pode cifrar um documento, mas somente outra pode decifrar, ou seja, se um documento foi cifrado com a chave privada, somente a chave pública correspondente poderá decifrá-lo e vice-versa. Assim, cada pessoa que necessite realizar transações eletrônicas terá uma única chave pública e uma única chave privada onde só a chave pública deve ser compartilhada.

Na criptografia assimétrica, o custo relacionado à geração de chaves públicas e privadas é alto. Dessa forma, por consumir menos recursos, a

criptografia simétrica é mais adequada para prover segurança em redes de emergência, uma vez que estas redes são compostas por dispositivos que possuem limitações.

Em redes DTN, o tempo de expiração das credenciais provê um mecanismo para lidar com sistemas de compromisso. Melhor que tentar revogar um conjunto de credenciais, elas apenas não são renovadas. Esse tempo deve ser grande suficiente para que os atrasos envolvidos na propagação da renovação e resposta não resultem em revogações indevidas de credenciais, e também não ocorra uma inundação contínua da rede com mensagens de requisição de renovação.

3.5.2. Assinatura Digital

Um ou mais nós maliciosos podem se apresentar com identidades múltiplas ou a identidade de outros nós da rede, podendo assim controlar a maior parte da rede. Este ataque também é capaz de unir e separar as redes, podendo, assim, significar uma grande ameaça para protocolos de roteamento geográfico [Kate, 2007].

Algumas contramedidas podem ser adotadas para evitar ou minimizar este tipo de ataque, como a assinatura digital, que pode ocorrer de duas formas: fim-a-fim, com o uso de uma assinatura nos dados enviados para evitar a inserção de dados falsos por nós intrusos, ou salto-a-salto, com uso de uma assinatura a cada salto do roteamento, para evitar a entrada de um nó intruso no roteamento.

Admite-se que um ataque interno não pode ser prevenido por uma rede, já que este intruso apresenta as mesmas características dos demais nós. Contudo, a rede pode fazer o uso de identificadores para os nós legítimos desta rede. A utilização de uma chave compartilhada global não impede que um invasor se disfarce de algum nó da rede. Assim, há necessidade que esta chave seja verificada, o que pode ser feito com uso de uma chave pública cifrada.

Uma das diferenças das redes DTN, quando uma mensagem é autenticada usando uma assinatura digital, a princípio qualquer elemento

da rede no caminho pode fazer alguma checagem dessa assinatura. Se a mensagem contém informação suficiente, então qualquer nó pode pelo menos verificar a exatidão criptográfica da assinatura [Burgess, 2007]. Apesar de útil, isso é tipicamente insuficiente para decidir como processar a mensagem, pois em vários ambientes é possível que qualquer um insira uma chave pública e uma assinatura, produzindo uma mensagem que passaria no teste.

Na maioria dos casos reais, existem algumas verificações adicionais se o assinante é autorizado, explicitamente ao verificar se o nome ou chave são autorizados para aquele propósito, ou implicitamente pelo uso da infra-estrutura de chave pública. Isso mostra que todos os caminhos práticos para promover essa verificação são problemáticos em redes DTN devido também à falta de um servidor de autorização ou até pelas restrições específicas de recursos dos nós.

3.5.3. Gerenciamento de chaves

O estabelecimento de chaves entre os vizinhos permite a autenticação no enlace. Na comunicação entre os nós, a autenticação pode ser verificada salto a salto, em toda a rota percorrida pelos pacotes. A autenticação salto-a-salto permite eliminar os pacotes não autenticados, resultando em um controle de acesso, onde apenas os nós da rede podem enviar mensagens, evitando assim a presença de nós intrusos.

Os processos de criptografia têm como objetivo comum impedir que uma determinada entidade denominada intruso obtenha informações sigilosas. Um esquema de distribuição de chaves seguro e eficiente permite a autenticação dos nós da rede. A captura e adulteração de um nó pode permitir ao inimigo utilizar as chaves armazenadas nesse nó. É necessário prever quais chaves podem ser descobertas a partir dessa adulteração.

O controle de acesso à rede pode impedir e eliminar diversos tipos de ataques, a menos que o inimigo comprometa nós legítimos da rede. Uma forma de efetuar o controle de acesso à rede é implementando autenticação ponto-a-ponto das mensagens enviadas. Para implementar

autenticação ponto-a-ponto, um nó deve ser capaz de autenticar os nós vizinhos, não importando o tipo de comunicação, ponto-a-ponto ou em modo difusão. Faz-se necessário, então, um esquema de distribuição de chaves seguro e eficiente que permita a autenticação em diferentes tipos de comunicação.

Os sistemas de chaves simétricas consistem, basicamente, na substituição de uma determinada informação por outra calculada e cifrada. A inversão desta informação cifrada para uma forma compreensível necessita a aplicação de chaves que são idênticas, secretas e de conhecimento apenas para os seus donos (remetente e destinatário). Assim, a passagem desta chave entre eles deve ser feita através de um canal seguro.

Para se comunicar em sistemas de chave pública, primeiramente, uma determinada entidade A deverá utilizar a chave pública de outra entidade B para cifrar sua mensagem usando um algoritmo de criptografia também conhecido ou padronizado. Logo a entidade B decifra esta mensagem enviada pela entidade A usando a sua chave secreta e com o algoritmo de inversão conhecido ou padronizado. Assim, nesta comunicação não houve a necessidade de troca de nenhuma chave, logo não há a necessidade de um canal seguro. Um exemplo de criptografia por chave pública é a RSA (Rivest Shamir Adleman, nome dos inventores), que utiliza aritmética modular para cifrar e decifrar a mensagem transmitida [Kurose, 2003].

As características das redes de emergência exigem novas abordagens para que seja possível atender os requisitos de segurança necessários a algumas aplicações [Symington, 2009]. Atualmente, nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes DTN, devido às características específicas dessas redes. Os protocolos atuais necessitam de serviço de distribuição de chaves ou checagem on-line, impraticável nos ambientes de conectividade intermitente.

A maior parte dos métodos de segurança em redes procura autenticar a identidade e integridade das mensagens, mas não tentam autenticar os roteadores que encaminham as informações. Em redes DTN, nós encaminhadores (roteadores e *gateways*) também são autenticados

[Warthman, 2003] e a informação enviada também é autenticada por eles, logo os recursos da rede podem ser conservados ao prevenir o transporte de tráfego proibido na primeira oportunidade.

Na criptografia de chave pública, por exemplo, cada usuário tem um par de chaves privada e pública. Um certificado é um arquivo, assinado digitalmente por uma autoridade certificadora (CA) confiável, confirmando a identidade do usuário e contendo uma cópia confirmada da chave pública do usuário.

Em redes DTN, ambos usuários e nós encaminhadores possuem pares de chaves e certificados, e os certificados dos usuários também indicam a classe de serviço [Durst, 2002]. Nós podem enviar seus pacotes com assinatura com sua chave privada, o que produz uma assinatura digital para o agregado específico. A assinatura permite aos recebedores confirmar a autenticidade do nó origem, a integridade da mensagem e os direitos relativos à classe de serviço, através do uso da chave pública do nó que enviou.

Segundo Fall [2003], a utilização dos pares de chaves e certificados poderia ocorrer da seguinte forma:

- Nó origem envia seu pacote, juntamente com assinatura específica, para um nó adjacente que pode encaminhá-la. Se esse nó ainda não possui uma cópia do certificado do nó origem, ele obtém uma do próprio nó ou de uma CA.
- O primeiro nó que recebe o pacote para encaminhá-lo verifica a identidade da origem e direitos da classe de serviço, utilizando suas cópias armazenadas de certificados dos nós adjacentes e chaves públicas da autoridade certificadora. Então substitui a assinatura do nó origem pela sua própria assinatura e encaminha a informação.
- Cada nó subseqüente no encaminhamento verifica somente a identidade do nó anterior, usando suas cópias armazenadas de certificados de roteadores adjacentes e chaves públicas de uma CA. Então realiza o mesmo processo de substituição da assinatura pela sua própria e encaminha o pacote. Isso ocorre até que a informação alcance o destino.

3.5.4. Criptografia Baseada na Identidade

Como uma área recente de pesquisa, os mecanismos que utilizam criptografia baseada na identidade [Seth, 2005] fornecem muitos dos benefícios da criptografia de chave pública e reduzem o *overhead* envolvido na obtenção e verificação de chaves públicas. Há várias vantagens em relação à criptografia de chave pública convencional, em que certificados de chave pública não precisam ser obtidos e transmitidos. Embora esse esquema convencionalmente sofra alguns inconvenientes por requerer que os destinatários comuniquem com um servidor, afirma-se que simplesmente pré-estabelecer chaves para alguns nós com suas chaves privadas pode oferecer operações razoavelmente eficientes em redes com atrasos e interrupções, com um risco aceitável de segurança [Seth, 2005].

Para implementar essa técnica, cada mensagem deve incluir um campo inalterável contendo a identidade verificada da origem (nó que enviou a mensagem), uma recomendação (e autoridade responsável pela aprovação) e outros materiais criptográficos para realizar a autenticação da mensagem. Roteadores verificam as credenciais em cada salto e descartam o tráfego o mais cedo possível se a autenticação falhar. Essa técnica também apresenta o benefício de evitar que ataques de negação de serviço prejudiquem o desempenho da rede [Kate, 2007].

Pode-se utilizar criptografia de chave pública como o ponto de partida para a geração de chaves. Roteadores e usuários finais recebem pares de chaves pública/privada, e um usuário tem de obter uma cópia assinada dessa chave pública de uma autoridade certificada da rede DTN. Todos os roteadores são considerados como pré-equipados com cópias de uma ou mais chaves públicas certificadas por uma autoridade DTN.

O usuário então apresenta a chave assinada com a mensagem a ser encaminhada. No primeiro roteador DTN, a chave pública é usada para validar o remetente e a classe de serviço requisitada. Mensagens válidas são então assinadas novamente com a chave do roteador para o encaminhamento. Utilizando essa técnica, somente no primeiro salto

roteadores necessitam de certificados para usuários. Os demais roteadores podem confiar na autenticação dos roteadores anteriores para verificar a autenticidade das mensagens.

Essa técnica pode aumentar a escalabilidade do gerenciamento de chaves para essas redes, limitando o número de certificados de chaves públicas armazenadas para uma função do número de roteadores adjacentes em preferência ao número de usuários finais. Isso provê vantagens óbvias de economia de espaço, mas também uma melhoria no sistema de gerenciamento, esperando-se que as chaves dos roteadores sejam trocadas menos frequentemente que chaves de usuários finais.

Como roteadores DTN são comumente utilizados em áreas remotas, operações de restabelecimento de chaves podem ser tarefas difíceis, limitando o número e a freqüência de atualizações certificadas para prover segurança adicional.

3.6. Conclusão

Nesse capítulo, foram apresentados os aspectos relativos à segurança em redes DTN, no contexto de redes de emergência. Baseado em uma revisão da literatura, foi possível listar os principais requisitos de segurança, que foram considerados no modelo de gerenciamento proposto. Também foram identificados os principais mecanismos de segurança para essas redes e as possibilidades de utilização conjunta desses componentes no modelo proposto nesse trabalho.

Como os requisitos de segurança para uma rede de emergência podem variar de acordo com as situações e cenários em que ela é utilizada, a arquitetura de segurança para essas redes deve ser baseada nas necessidades dos usuários finais e suas aplicações. Logo, as redes devem ser auto-gerenciáveis no aspecto da segurança, de forma a evitar sua utilização por agentes externos à rede e manter o equilíbrio em relação ao consumo de recursos.

Capítulo 4

Modelo de Gerenciamento de Segurança em Redes de Emergência

Esse capítulo apresenta o modelo de gerenciamento de segurança proposto neste trabalho, bem como seus aspectos abordados e características definidas. Um modelo de gerenciamento deve agregar as informações de modelos já existentes e considerá-las em seu domínio, o que requer não só o entendimento sintático, mas também entendimento semântico de cada modelo e/ou proposta relacionada. Existem algumas pesquisas nessa área, mas ainda em fase inicial.

A maioria das pesquisas relacionadas à segurança em redes DTN está direcionada à modificação de soluções já existentes de redes móveis *ad hoc* e pesquisas de segurança distribuída, como o uso de autoridades certificadas distribuídas [Seth, 2005] [Kate, 2007]. Embora estes protocolos sejam comumente estudados isoladamente, pouca atenção tem sido dada ao gerenciamento de segurança.

Estudos relacionados a mecanismos de segurança e à análise do impacto causado por estes mecanismos nas taxas de entrega das mensagens ainda estão em aberto, tendo em vista os requisitos de segurança das aplicações e as restrições das redes DTN. Trabalhos relativos à segurança normalmente restringem-se a simulações baseadas em modelos estatísticos e análises matemáticas da implantação de novos algoritmos [Burgess, 2007]. No entanto, são encontrados poucos trabalhos voltados a cenários reais nesta área.

Em cenários de resposta a desastres, onde pelo menos um grupo de agentes de resgate foi treinado para esse propósito, considerando a

tendência de normalização da terminologia de emergência e troca de formatos [Shank, 2008], a detecção de intrusos é um problema mais simples que solucionar o problema geral das comunicações baseadas na Internet. Entretanto, existe um desafio técnico ao avaliar uma tecnologia nova, por isso representar falta de dados coletados por longos períodos de tempo e em cenários reais.

Nesse cenário de resposta a desastres, a infra-estrutura possuirá muito menos recursos e precisará prover auto-configuração e auto-cura para ser eficiente. Por outro lado, os ataques contra essas redes também tendem a ser menos sofisticados e menores em escala [Asplund, 2008]. Deve existir uma arquitetura de segurança que se adapte a um possível interesse de terceiros pelas informações da rede.

Existem também outros desafios, que não existiam ou pelo menos não nessa escala em infra-estruturas tradicionais, como a mobilidade, desconexão, escassez de recursos e heterogeneidade.

Entre os ataques que a rede pode sofrer, pode-se destacar: perda de dados, inundação da rede com mensagens extras, corrupção das tabelas de roteamento, falsificação de acks na rede ou informação falsa sobre probabilidades de encontro.

A utilização de replicações no roteamento é crucial para conseguir a tolerância a ataques. Avaliar como protocolos de roteamento em DTN se comportam sob ação de ataques requer hipóteses sobre o tamanho, conectividade e mobilidade. Deve-se considerar que tabelas de roteamento são baseadas em oportunidades de transferência de sucesso, em vez de sucesso na entrega.

Pode-se deduzir que os protocolos replicativos são amplamente mais resistentes a ataques. A inundação da rede com confirmações mostra-se como o mais devastador método de ataque, pois os pacotes são perdidos após alcançar um intruso e esse pode inundar a rede com *acks* enviados para provocar a exclusão de qualquer outra cópia do pacote existente na rede.

A escolha por restringir uma DTN somente a participantes autorizados implica uma perda de oportunidade, de maneira que os nós

perdidos poderiam ter voluntariado a participar caso houvesse um esquema mais simples sendo usado. Em cenários não militares, uma baixa porcentagem de nós intrusos é esperada, mas redes DTN de sucesso incentivarão a participação no caso de ausência de restrições de autenticação.

Alguns dos usuários poderiam ser adversários de outros, no intuito de interromper ou escutar a comunicação. Caso detectados, os comportamentos negativos ou egoístas devem ser punidos, não se permitindo a esses nós participarem da rede. O conhecimento sobre nós com esse tipo de comportamento pode também ser dividido com outros nós através da utilização de sistemas baseados em reputação. Mas esses sistemas criam novos problemas com falsas acusações e identidades fraudadas.

Pode ser necessária a detecção de intrusos distribuída contrapondo-se soluções propostas em infra-estruturas existentes, que são organizadas com a hierarquia de detectores bem-localizados e agentes relacionados.

Em particular, devido às desconexões frequentes entre os nós em DTN, autoridades certificadoras distribuídas são mais desejáveis do que as centralizadas, enquanto a frequente distribuição de uma grande quantidade de certificados deveria ser evitada devido ao alto tempo demandado. As credenciais dos usuários deveriam ser atualizadas periodicamente ao invés da confiança em mensagens de revogação.

Mesmo assim, utilizam-se técnicas de segurança aceitas como criptografia de chave pública comum e assinatura digital, que não são precisas por causa da dependência de entidades de acesso contínuo para gerenciar a distribuição de chaves de forma confiável, por exemplo. É, sem dúvidas, muito importante prover serviços de segurança como autenticação, confidencialidade, e privacidade se requerido.

Este trabalho propõe um modelo de gerenciamento de segurança adaptativo que habilita ou desabilita componentes de segurança e de roteamento em reação a ameaças representadas por intrusos em redes de emergência. O modelo inclui seleção de componentes de segurança, descrição de informação de gerenciamento, descrição de mensagens e

definição de eventos de segurança. De modo autonômico, componentes de segurança foram agrupados em níveis, que podem ser alterados em resposta a eventos de detecção de intrusos. O objetivo é evitar o efeito de ataques e economizar recursos com a ativação dos serviços de segurança somente quando for necessário.

4.1. Gerenciamento de segurança

O atendimento a requisitos de segurança é essencial em redes de emergência. Aplicações públicas, por exemplo, devem garantir aos cidadãos a privacidade a que têm direito. A operação incorreta de uma rede pode levar a situações que não foram previstas, como, por exemplo, sistemas podem ser usados para facilitar assaltos e fugas de criminosos ou podem ser adulterados para enviar informações incorretas que prejudiquem o atendimento às pessoas. Várias outras aplicações de redes tolerantes a interrupções estão sujeitas à ação de invasores caso não estejam protegidas por rigorosos mecanismos.

Os requisitos de segurança para uma rede de emergência dependem da sua aplicação. Redes de missão crítica podem necessitar de confidencialidade, autenticidade, integridade, frescor e disponibilidade. A captura de um nó pode comprometer a segurança da rede, revelando informações como chaves, ou mesmo permitindo a reprogramação do nó, tornando-o uma ferramenta de ataque de um inimigo.

Em relação à detecção de intrusos, propõe-se a utilizar preferencialmente o centro de controle para prover a segurança em redes de emergência, por apresentar maior quantidade de recursos computacionais que os demais nós.

É difícil conceber aplicações que não demandem um nível mínimo de segurança. A presença de invasores pode ser detectada em diversos tipos de aplicações de rede. Aplicações simples de monitoramento ambiental

podem despertar interesse de empresas que exploram o ambiente como madeireiras e garimpeiros.

A sobreposição de mecanismos de segurança é necessária porque nenhum desses mecanismos consegue garantir eficácia total. Mecanismos de segurança usados em redes convencionais, como criptografia, só podem ser usados em redes de emergência se observadas as restrições de comunicação, energia e processamento.

Diversas abordagens de segurança foram propostas para redes DTN, incluindo desde algoritmos de identificação baseados na identidade até mecanismos de detecção de intrusos. Essas abordagens podem ser vistas como componentes de uma arquitetura de segurança que podem ser usados de forma isolada ou mista, embora alguns componentes se excluam mutuamente ou somente possam ser usados em condições específicas.

Nesse sentido, cada componente pode ser usado isoladamente, de forma independente, ou em conjunto, complementando a ação de outro componente. Abordamos nesse trabalho a função de gerenciamento de segurança, que pode permitir a adaptação da rede durante sua execução, inserindo ou removendo componentes de segurança adicionais.

O gerenciamento de segurança trata de questões como:

- geração, distribuição e armazenamento de chaves de criptografia;
- manutenção e distribuição de senhas e informações de controle de acesso;
- monitoração e controle de acesso à rede ou parte da rede e às informações obtidas dos nós da rede;
- coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades.

As funções de gerenciamento de segurança podem ser agrupadas em três categorias:

- manutenção da informação de segurança;
- controle de acesso aos recursos;
- controle do processo de criptografia.

4.2. Controle de acesso

O controle de acesso é uma função crítica em redes de emergência e, portanto, deve estar sempre habilitado de acordo com o modelo proposto. Se qualquer nó tiver permissão para participar da rede, um nó malicioso pode se inserir na rede, e efetuar todo tipo de ataque.

O controle de acesso é tipicamente implementado através de mecanismo criptográfico e distribuição adequada de chaves. Um mecanismo de controle de acesso efetivo deve suportar comunicação autenticada para possibilitar a um nó reconhecer o transmissor de uma mensagem recebida como sendo um nó legítimo. Por esse motivo, deve existir um mecanismo de chaves que suporta o padrão de comunicação das redes DTN.

O maior problema em aberto em segurança para redes DTN é a ausência de um método de gerenciamento de chaves tolerante a interrupções. Os protocolos atuais necessitam de serviço de distribuição de chaves ou checagem on-line, impraticável nos ambientes de redes de emergência.

Esquemas de criptografia baseada na identidade foram propostos, mas ainda não considerados como soluções para o problema. As propostas existentes atuam efetivamente apenas como uma forma de certificado de grupo, onde todos os nós utilizam um dado gerador de chaves privadas e podem utilizar um único certificado, ainda restando o problema da validade desse certificado.

Redes DTN são robustas mesmo sem utilizar autenticação para restringir a participação a nós honestos [Fall, 2004]. Existe um pequeno custo de desempenho para a defesa quando todos os nós são bem comportados, mas a defesa é efetiva. Apesar dos custos da oportunidade de excluir participantes sem autenticação, é válido evitar os efeitos negativos da inclusão de possíveis intrusos.

Porém o impacto de um intruso na rede é imprevisível, visto que Holme et al. [2002] mostra que o tamanho do maior componente conectado no grafo que representa a visão no nível do roteador da Internet será reduzida a menos da metade do tamanho original após a remoção de somente 0,03% dos nós com maiores graus.

O controle de acesso, através da autenticação ponto-a-ponto, elimina a possibilidade de diversos ataques promovidos por nós externos, como escuta, inserção de dados incorretos, adulteração dos dados, alteração da origem, e também os ataques de negação de serviço no roteamento, como *black hole, selective forwarding, wormhole,* entre outros. A possibilidade de ataques internos, porém, deve ser verificada.

A inserção de novos nós é um problema em esquemas de autenticação ponto-a-ponto. Um inimigo pode utilizar a inserção de nós para inserir também os seus nós maliciosos. Para evitar a inserção de nós inimigos, deve ser garantido o controle de acesso à rede durante a inserção de novos nós. Para tanto, os nós antigos devem ser capazes de reconhecerem novos nós autênticos e também os nós novos devem reconhecer os nós antigos autênticos. E devem também ser capazes de estabelecer chaves entre eles.

Três requisitos devem ser garantidos durante a inserção dos novos nós: a autenticidade dos novos nós junto aos antigos, a autenticidade dos nós antigos junto aos novos e a confidencialidade do processo de troca de chaves entre esses nós. Todos esses requisitos poderiam ser alcançados apenas pelo compartilhamento de uma chave global entre os nós antigos e os novos, caso não existissem nós intrusos na rede. Mas, como a possibilidade de existência de intrusos existe, é necessário o uso de outros mecanismos para minimizar o efeito da presença de um nó malicioso na rede.

4.3. Componentes do modelo de gerenciamento

O modelo de gerenciamento proposto nesse trabalho possibilita a configuração de diversos componentes de segurança para redes de emergência, considerando interrupções.

O modelo propõe que o gerenciamento de segurança das redes de emergência seja orientado por mensagens, que são enviadas em casos de detecção de intrusos ou para utilização de encriptação, assinatura digital, protocolo para estabelecimento de chaves, protocolos para roteamento dinâmico seguro e seleção de prioridade de pacotes para replicação. Esses são os principais mecanismos de segurança utilizados em redes de emergência e, por isso, foram considerados no gerenciamento de segurança proposto.

A abordagem de redes de emergência considera mensagens enviadas para os centros de controle e desses para os nós da rede, além da presença de vários roteadores pela rede. Apesar de não ser indicada para redes DTN, em situações mais críticas, a criptografia fim-a-fim pode ser utilizada nesse contexto para garantir maior confiabilidade na comunicação com os centros de controle, através de verificação de integridade ou autenticação de origem e destinatário das mensagens.

Como definição para esse modelo de gerenciamento, o usuário DTN apresenta sua chave pública para uma autoridade certificadora DTN para obter uma cópia assinada daquela chave e um conjunto de credenciais assinado para autorizar o usuário a utilizar serviços específicos, o que seria necessário apresentar para um roteador antes de poder utilizar o seu serviço. O roteador verifica a assinatura e armazena chave pública e credenciais em um *cache*, que possui um tempo de expiração.

Os componentes abordados no gerenciamento de segurança proposto foram descritos na seção anterior. A seguir, são listadas as possíveis abordagens de segurança para as redes de emergência segundo o modelo. Cada componente já existente pode ser utilizado de forma independente, isoladamente, ou em conjunto, complementando a ação de outro componente:

- Indicação de prioridade de pacotes;
- Roteamento dinâmico seguro;
- Encriptação fim-a-fim;
- Encriptação salto-a-salto;
- Assinatura salto-a-salto;
- Assinatura fim-a-fim;
- Protocolos para estabelecimento de chaves;
- Sistemas de detecção de intrusos.

4.4. Níveis de segurança

A pesquisa em segurança de redes DTN tem desenvolvido novas técnicas adequadas de segurança para impedir ou minimizar a ação de intrusos. A tolerância à intrusão é um aspecto importante, pois existem situações em que não se pode impedir a ação de nós maliciosos. Neste trabalho, componentes de segurança são configurados baseados em eventos de segurança gerados por sistemas de detecção de intrusos.

Eventos de detecção de intrusos configuram componentes de segurança. Intrusos detectados pelo centro de controle são revogados usando mensagens autenticadas. Intrusos detectados de maneira descentralizada não podem ser revogados pelo centro de controle porque os nós não são confiáveis, mas um evento de detecção de intruso é gerado, de forma a ativar componentes de segurança.

O modelo de gerenciamento de segurança proposto para redes de emergência define a utilização dos componentes de segurança de acordo com níveis de segurança que podem ser configurados para a rede, segundo informações obtidas do gerenciamento como o número de intrusos detectados.

Com a utilização desses níveis, o centro de controle pode configurar facilmente quais funcionalidades de segurança os demais nós devem utilizar, de acordo com a situação ou meio em que a rede se encontra.

Foram definidos níveis de segurança para facilitar decisões autonômicas baseadas em eventos recebidos. Em cada nível de segurança, alguns componentes de segurança são ligados para proteger a rede dos intrusos. O nível de segurança da rede aumenta com a evidência de intrusos e pode também ser decrescido em situações de recursos mínimos. Componentes de segurança, como a detecção de intrusos, podem ser desligados para economizar energia em parte dos nós da rede.

A Tabela 4.1 exibe eventos e ações autonômicas geradas nesses eventos. Em geral, um intruso é suficiente para alterar o nível de segurança, porque indica que o atual nível de segurança permitiu a entrada de intrusos; todavia, em algumas situações, o nível de segurança pode ser alterado após a detecção de mais de um intruso.

Tabela 4.1. Eventos de detecção de intrusos e ações

Evento	Ação
Centro de controle detecta um novo intruso	- Intruso é revogado - Nível de segurança aumenta
Um nó detecta novo intruso	- Nível de segurança aumenta

Tabela 4.2. Níveis de segurança para problemas autonômicos

Nível	Componentes de segurança utilizados
Baixo	- Sem detecção de intrusos nos roteadores - Controle de acesso habilitado - Protocolo de roteamento *epidemic*
Médio	- 10% dos nós executam detecção de intrusos - Controle de acesso habilitado - Criptografia salto-a-salto habilitada - Protocolo de roteamento *PropHet*
Alto	- 20% dos nós executam detecção de intrusos - Criptografia salto-a-salto habilitada - Encaminhamento de pacotes com prioridade - Protocolo de roteamento *spray and wait* - Controle de acesso habilitado
Crítico	- Roteadores executam detecção de intrusos - Criptografia fim-a-fim e salto-a-salto habilitadas - Replicação de pacotes de alta prioridade - Protocolo de roteamento *spray and wait* - Controle de acesso habilitado

A Tabela 4.2 mostra os níveis de segurança. O serviço de detecção de intrusos centralizado está sempre habilitado e não aparece na tabela. Quando o centro de controle detecta um nó intruso, ele é revogado. Em todos os níveis, pode-se utilizar *flags* para indicar replicação de maior

prioridade. As aplicações que utilizam a rede de emergência podem obrigar a definição de prioridade entre: Baixa, Média, Alta ou Urgente. Mensagens definidas como urgentes possuirão um tempo de vida determinado pelo centro de controle e inferior ao das demais, para descarte após término desse tempo.

No primeiro nível, mais baixo, apenas o controle de acesso é habilitado como componente de segurança. Isso deve evitar que a rede consuma recursos ao encaminhar pacotes não autorizados. A detecção de intrusos é utilizada somente no centro de controle. Como não há conhecimento das probabilidades de encontro, os nós utilizam o protocolo de roteamento *epidemic*, dado que as redes de emergência têm expectativa de utilização da ordem de dias e, portanto, não haverá uma sobrecarga significativa de mensagens na rede.

No nível Médio, alguns roteadores habilitam a detecção de intrusos e também é ativada criptografia salto-a-salto, por ser a melhor alternativa conforme discussão sobre a dificuldade de utilização de técnicas fim-a-fim em redes DTN na seção 3.5. Os componentes escolhidos nesse nível implicam em uma sobrecarga de processamento e rede, devendo-se buscar equilíbrio no consumo de recursos ao utilizar o conhecimento já adquirido da rede para os cálculos do protocolo de roteamento *PRopHet*.

No nível Alto, a detecção de intrusos é estendida para 20% dos nós na tentativa de verificar se há outros intrusos na rede. De acordo com a presença de intrusos, a priorização das mensagens pode auxiliar na identificação das mensagens que devem ser replicadas, o que também impede que falsas confirmações de recebimento sejam consideradas. Somente mensagens com definição de prioridade são encaminhadas pela rede para seu destino. Passa a ser utilizado para o roteamento o protocolo *spray and wait* no modo binário, pois a replicação de mensagens no roteamento aumenta consideravelmente a tolerância a ataques. Apesar de aumentar o consumo de recursos da rede, o objetivo é garantir a confiabilidade das mensagens entregues.

O nível Crítico é iniciado se, ainda com o nível Alto ativo, intrusos são detectados. Esse modo somente tem de ser usado se nós intrusos ainda

são detectados quando toda a utilização de criptografia salto-a-salto está ativa. Nesse nível, todos os componentes de segurança apresentados são utilizados e considera-se que nós intrusos podem conhecer algumas chaves da rede, pois ainda conseguem enviar mensagens através da rede. Assim, utiliza-se criptografia redundante, fim-a-fim e salto-a-salto, mesmo considerando as consequências dessa utilização em redes DTN como discutido na seção 3.5. Dessa forma, um intruso terá de conhecer várias chaves para ter acesso às mensagens da rede. Todos os roteadores que armazenam e repassam mensagens passam a utilizar a detecção de intrusos. A presença de grande número de mensagens na rede e possivelmente mensagens não confiáveis indica que deve haver maior seleção de mensagens a serem replicadas. Por isso, passa-se a replicar somente mensagens definidas como alta prioridade para comunicação entre os nós e o centro de controle.

Quando recursos de energia descem a um nível mínimo, os nós podem reduzir o nível de segurança para aumentar o seu tempo de vida. Nesse caso, os componentes de segurança têm um custo de energia maior que a rede pode gastar. Como os nós estão no fim do seu tempo de vida, é melhor tentar trabalhar sem segurança do que gastar a energia restante com segurança.

De acordo com a aplicação da rede de emergência e duração da sua utilização, podem ser estabelecidas métricas para definir momentos em que o nível de segurança pode ser reduzido. Como exemplo, uma rede que atinge o nível de segurança Alto e permanece longo período no mesmo nível, poderia ter uma decisão de redução para o nível Médio, sendo administradas as consequências dessa medida.

A criptografia pode incluir encriptação e assinatura e os objetivos da rede devem determinar qual técnica tem de ser usada. Se os dados da rede são confidenciais, a encriptação tem de ser usada. De outro lado, somente assinatura pode ser utilizada para evitar adulterações e enganos.

4.5. Definição das MIBs

A MIB (*Management Information Base* ou Base de Informação de Gerenciamento) apresenta os objetos que poderão ser gerenciados.

Além das informações agrupadas em Criptografia e Dados, que devem ser alteradas diretamente pelo modelo de gerenciamento proposto, as informações de Administração e Hierarquia também são monitoradas. A MIB Administração define os aspectos diretamente relacionados às mensagens da rede que serão gerenciados.

Considera-se a possibilidade de existência de grupos na rede de emergência, que poderiam representar organizações diferentes como polícia e bombeiros. Esses grupos podem apresentar regras de hierarquia próprias, como a comunicação com outros grupos centralizada em um nó considerado como líder. Tais informações são armazenadas e gerenciadas através da MIB Hierarquia.

O modelo de gerenciamento deste trabalho propõe também a integração de redes de sensores sem fio a redes de emergência. Para tanto, considera a utilização do modelo proposto em Oliveira et al. [2008] bem como suas definições e utiliza o formato das mensagens do protocolo de gerenciamento MannaNMP [Silva, 2005], que descreve os serviços providos e o formato das mensagens, assim como a base de informações de gerenciamento.

Os seguintes objetos, que seguem as especificações do protocolo MannaNMP, devem ser controlados pelo sistema de gerenciamento de segurança proposto.

1. Criptografia

(a) Encriptação fim-a-fim (BOOLEAN) ⇒ Indica se utiliza encriptação fim-a-fim;

(b) Encriptação ponto-a-ponto (BOOLEAN) ⇒ Indica se utiliza encriptação ponto-a-ponto;

(c) Assinatura fim-a-fim (BOOLEAN) ⇒ Indica se utiliza assinatura fim-a-fim;

(d) Assinatura salto-a-salto (BOOLEAN) ⇒ Indica se utiliza assinatura salto-a-salto;

(e) Criptografia baseada na identidade (BOOLEAN) ⇒ Indica se identidade será utilizada como aspecto chave;

(f) Protocolo para estabelecimento de chaves (CHOICE) ⇒ Indica qual método será utilizado para distribuição de chaves.

2. Dados

(a) Nível de segurança (CHOICE) ⇒ Baixo (0), Médio (1), Alto (2), Crítico (3);

(b) Protocolo de roteamento (CHOICE) ⇒ Direct delivery (0), Epidemic (1), PRopHet (2), Spray and Wait (3);

(c) Utiliza priorização? (BOOLEAN) ⇒ Indica se utiliza priorização dos pacotes;

(d) Intruso detectado? (BOOLEAN) ⇒ Indica se nó detectou intruso na rede;

(e) Identificador do intruso (ID) ⇒ Identificador do intruso detectado por este nó;

(f) Identificador de nó revogado (ID) ⇒ Indica o nó intruso a ser revogado;

(g) Lista de nós revogados (LIST) ⇒ Lista dos nós suspeitos que foram revogados;

(h) Lista de chaves revogadas (LIST) ⇒ Lista de chaves que foram revogadas para este nó.

3. Administração

(a) Tempo de Vida de Mensagens (INTEGER) ⇒ Indica o TTL das mensagens que não forem urgentes;

(b) Tempo de Vida de Mensagens Urgentes (INTEGER) ⇒ Indica o TTL das mensagens que foram definidas como urgentes;

(c) Mensagens de Gerenciamento Enviadas (INTEGER) ⇒ Indica o número de mensagens de gerenciamento enviadas por este nó;

(d) Mensagens de Gerenciamentos Recebidas (INTEGER) ⇒ Indica o número de mensagens de gerenciamento recebidas por este nó;

(e) Mensagens de Dados Enviadas (INTEGER) ⇒ Indica o número de mensagens de dados enviadas por este nó;

(f) Mensagens de Dados Recebidas (INTEGER) ⇒ Indica o número de mensagens de dados recebidas por este nó;

4. Hierarquia

(a) Identificador do Grupo (INTEGER) ⇒ Identifica o grupo unicamente;

(b) Tipo de Formação de Grupo (INTEGER) ⇒ Centralizado (0), Distribuído (1);

(c) Integrantes do Grupo (SEQUENCE OF ID) ⇒ Lista de nós integrantes do grupo;

(d) Integrantes do Grupo Ativos (SEQUENCE OF ID) ⇒ Lista de nós integrantes do grupo que estão em operação;

(e) Integrantes do Grupo Reservas (SEQUENCE OF ID) ⇒ Lista de nós integrantes do grupo que estão fora de operação;

(f) Nível da Hierarquia (INTEGER) ⇒ Indica o nível da hierarquia deste nó.

Além dessas informações que podem ser enviadas através da rede e requisitadas pelos centros de controle, as informações relativas a chaves utilizadas devem ser armazenadas nos nós para a criptografia, mas não podem ser enviadas pela rede por questões de segurança.

4.6. Definição das mensagens

O modelo desse trabalho propõe que o gerenciamento de segurança das redes de emergência seja orientado por mensagens, que serão utilizadas para ativar e desativar o uso dos componentes: detecção de intrusos,

utilização de criptografia, protocolos para roteamento dinâmico seguro, seleção de prioridade de pacotes para replicação, entre outros. Uma mensagem de presença de intruso, por exemplo, deve colocar a rede em estado de alerta. Como a identificação precisa do intruso não é possível, a rede tem de reduzir as possibilidades de comunicação do intruso de forma a anular seus efeitos.

A seguir, são listadas as mensagens que devem ser enviadas para o gerenciamento de segurança proposto e suas funções/conseqüências. Nesse caso, as mensagens são do tipo *Set*, utilizadas quando se deseja atribuir ou alterar valores de objetos gerenciados, segundo o protocolo de gerenciamento MannaNMP [Silva, 2005].

Deve haver uma verificação se o objeto é somente leitura, ou seja, seu valor não pode ser alterado. Caso algum dos objetos identificados no campo *VariableBindings* da mensagem seja somente leitura, é gerado um erro. Existe um campo na mensagem (Requer Resposta) que indica se o gerente deseja confirmação (1) ou não (0). Este mecanismo evitará que mensagens sejam enviadas sem necessidade, economizando recursos da rede. Com isso, o gerente poderá selecionar as atribuições que são fundamentais e exigir confirmação. Caso seja exigida confirmação, o gerente aguarda por determinado tempo pela confirmação e reenvia a mensagem caso este tempo expire.

1. Criptografia

- Ativação de encriptação fim-a-fim;
- Ativação de encriptação ponto-a-ponto;
- Ativação de assinatura fim-a-fim;
- Ativação de assinatura salto-a-salto;
- Ativação de criptografia baseada na identidade;
- Protocolo para estabelecimento de chaves: permite a alteração do método inicialmente estabelecido.

2. Dados

- Mudança no nível de segurança da rede: altera a configuração dos componentes de segurança utilizados;
- Mudança no protocolo de roteamento da rede;
- Utilização de priorização das mensagens;
- Detecção de intruso: coloca a rede em estado de alerta, informando o identificador do intruso ao centro de controle;
- Revogação de nó: adiciona o identificador do nó revogado às listas de nós revogados;
- Revogação de chave: adiciona a chave revogada às listas de chaves revogadas dos nós receptores.

3. Administração

- Alteração no tempo de vida das mensagens urgentes;
- Alteração no tempo de vida das mensagens não definidas como urgentes.

Todas as informações objeto das mensagens do tipo *Set* listadas acima e as demais informações da rede de emergência devem ser acompanhadas e requisitadas pelos centros de controle através de mensagens do tipo *Get*.

A mensagem *Get* é utilizada para que o usuário solicite informação sobre objetos gerenciados. Esta informação corresponde ao valor daquele objeto em determinado instante. O gerente aguarda determinado tempo (*timeout*) pela resposta. Caso este tempo expire, a mensagem é enviada novamente. O tempo de espera poderá ser configurado, dependendo das características da rede. O número de retransmissões também poderá ser configurado para evitar que mensagens sejam retransmitidas várias vezes.

4.7. Definição dos eventos

Quando eventos ocorrem na rede de emergência, os nós devem enviar mensagem ao centro de controle para comunicar o ocorrido. Essas mensagens serão utilizadas pelo centro de controle para alterar configurações de gerenciamento da rede imediatamente ou após determinado tempo.

A mensagem de *Trap* é assíncrona, sendo enviada quando ocorre algum evento programado pelo projetista da rede. Caso a rede seja hierárquica, as mensagens são repassadas ao nível superior da hierarquia, até que alcancem o gerente da rede. Quando viável, um nó intermediário poderá tomar decisões sobre o que deve ser feito, tornando a rede mais inteligente e diminuindo o fluxo de mensagens.

A responsabilidade de monitoramento de alguns ou todos os eventos identificados pode ser atribuída somente aos centros de controle ou aos roteadores DTN, para não haver consumo excessivo de recursos. A seguir, são listados os eventos que devem ser comunicados, segundo o modelo proposto e utilizando o formato do protocolo MannaNMP:

- Detecção de intruso: nó identificou um nó suspeito como intruso e, então informa o identificador desse nó ao centro de controle;
- Revogação de chave: pode ser configurado que o nó revogue chaves em situações específicas e então, informe o motivo ao centro de controle;
- Inserção de novo nó: nó identificou um novo nó vizinho com chaves da rede e que não teve sua participação na rede confirmada, então informa o identificador desse nó ao centro de controle;
- Nível mínimo de energia: quando um nó atinge o nível mínimo de energia residual, deve informar ao centro de controle. As chaves dele serão, então, revogadas.

4.8. Conclusão

Nesse capítulo, foi apresentado o modelo de gerenciamento de segurança adaptativo proposto para redes de emergência, com objetivo de evitar o efeito de ataques e economizar recursos ao ativar os componentes de segurança apenas quando for necessário.

O modelo apresentado estabelece a integração entre mecanismos de segurança para redes DTN e possibilita a formação de várias combinações desses componentes de segurança para utilização em redes de emergência, de acordo com as necessidades demonstradas pelo gerenciamento da rede.

Através do auto-gerenciamento da rede, o centro de controle pode configurar níveis de segurança nos nós, adaptando a utilização de componentes de segurança para evitar o efeito dos intrusos. As definições de níveis de segurança, MIBs, mensagens e eventos permitem que os diversos componentes de segurança possam ser facilmente configurados de acordo com a situação momentânea ou meio em que a rede se encontra.

Capítulo 5

Avaliação do modelo

Soluções de segurança para redes de emergência devem ser avaliadas em relação a alguns aspectos críticos, como a latência e a probabilidade de entrega das mensagens. Além disso, a exatidão das alterações dos mecanismos de segurança utilizados deve ser verificada, de maneira que os nós apresentem comportamento adequado e não seja afetado o desempenho da rede.

A utilização do modelo de gerenciamento de segurança adaptativo proposto não deve representar alteração significativa em relação à taxa de entrega de mensagens da rede, visto que são necessárias apenas poucas mensagens de gerenciamento e as alterações do protocolo de roteamento das mensagens objetiva a eficiência da entrega.

É esperado que não se tenha uma abordagem ideal a ser adotada em qualquer tipo de rede e aplicação. Portanto, é interessante identificar para quais tipos de aplicação uma determinada abordagem será mais eficiente.

São utilizados mais recursos do centro de controle, gerente que é o responsável pela inteligência do gerenciamento por possuir capacidade de processamento dos serviços automáticos. Sendo assim, é importante ressaltar que os recursos consumidos pelo gerenciamento não são significativos nos demais nós da rede.

Sendo assim, considera-se como vantajosa a utilização do modelo de gerenciamento de segurança adaptativo proposto para redes de emergência por:

- estabelecer a integração entre os principais mecanismos de segurança utilizados;

- definir níveis de segurança, permitindo que os diversos componentes de segurança possam ser facilmente configurados de acordo com a situação momentânea ou meio em que a rede se encontra;
- ser orientado por mensagens, o que permite que aspectos de segurança possam ser reconfigurados, a partir do recebimento de mensagens pela rede;
- definir MIBs, informações de gerenciamento para armazenar aspectos de utilização dos componentes de segurança;
- garantir e/ou proporcionar maior nível de segurança para redes em situações críticas e de emergência.

5.1. Metodologia

Considerando a avaliação experimental, pode-se citar duas dificuldades principais. Primeiramente, as redes de emergência ainda são relativamente raras, dificultando a análise de comportamento de uma rede de larga escala. Como a tendência é que essas redes sejam compostas por dezenas a centenas de nós, esse tipo de avaliação é importante para validar uma solução. Em segundo lugar, apesar de uma rede real possivelmente apresentar mais detalhes ao modelo de avaliação, ainda é difícil coletar métricas consideradas importantes para redes DTN, em relação à entrega de mensagens, por exemplo. A principal vantagem da experimentação é a avaliação em um ambiente real com as restrições de hardware e as propriedades do meio físico.

A simulação tem como desvantagem o menor nível de detalhes se comparada com o experimento, mas dependendo da modelagem do sistema e da ferramenta adotada, obtêm-se resultados confiáveis. Outra desvantagem é a complexidade das ferramentas existentes, que são difíceis de serem utilizadas e requerem muitos recursos computacionais. Como vantagens, esse mecanismo permite a coleta de métricas de

desempenho importantes e a avaliação da escalabilidade. Portanto, a técnica mais adequada para se avaliar soluções para redes DTN é a simulação.

Para validar o modelo de gerenciamento aqui apresentado, um conjunto de simulações foi realizado para verificar a utilização dos diversos níveis de segurança. O objetivo é mostrar o comportamento da rede de emergência em cada nível, para justificar a manutenção dos níveis inferiores enquanto a presença de intrusos não tiver sido constatada.

Como esse tipo de rede tende a ser composta por uma grande quantidade e diversidade de nós, o desempenho das abordagens em redes de larga escala é um fator considerado importante. Também é importante saber o desempenho das abordagens dependendo das funcionalidades do gerenciamento.

Soluções de segurança em redes DTN devem ser validadas em relação a alguns aspectos importantes como consumo de recursos e sobrecarga de mensagens na rede. Aplicações, protocolos e algoritmos não podem ser escolhidos considerando apenas sua “elegância” e capacidade, assim os impactos da solução proposta serão avaliados bem como o desempenho e funcionalidade alcançados.

Duas métricas críticas que são comumente utilizadas para avaliar redes DTN são a porcentagem de pacotes entregues e a latência da entrega. Como nós podem entrar ou deixar a rede a qualquer momento, alguns pacotes podem nunca ser entregues mesmo quando intrusos não estão presentes.

Deve-se verificar que mensagens somente serão enviadas quando realmente necessário, ou seja, na ocorrência de algum evento. Isso economiza recursos da rede, tanto em processamento quanto em comunicação, e foi observado pelo número de mensagens de gerenciamento criadas na rede. Além disso, propõe-se uma avaliação de desempenho, com o intuito de avaliar a escalabilidade e o impacto das funcionalidades do gerenciamento de segurança.

A partir do modelo de gerenciamento de segurança adaptativo proposto, realizou-se a implementação dos aspectos abordados em cada

nível de segurança, bem como consequências em resposta aos eventos gerados. Para tanto, procurou-se o ambiente mais adequado para simulação das características das redes de emergência.

Utilizou-se o simulador The ONE (Opportunistic Networking Evaluator) [Keranen, 2009], que simula um modelo de comunicação tolerante a interrupções, no qual os nós seguem o paradigma guardar-carregar-repassar mensagens (store-carry-foward), podendo mantê-las em um buffer caso o nó não tenha conexão direta com o destino. Cada teste foi executado repetidamente, sendo alterada a semente geradora do padrão de mobilidade.

The ONE é um simulador desenvolvido em Java, projetado e implementado por Ari Keränen, download disponível na Internet (http://www.netlab.tkk.fi/tutkimus/dtn/theone/). O ambiente de simulação é capaz de:

- gerar movimento do nó usando diferentes modelos;
- visualizar mobilidade e envio de mensagem em tempo real na interface gráfica;
- rotear mensagens entre nós usando diferentes modelos;
- executar os protocolos de roteamento já implementados: Direct Delivery, Spray and Wait, Epidemic e PRopHet.

5.2. Cenário

Como se espera que somente pessoas preparadas atuem na região de um desastre, as simulações consideraram uma rede móvel e heterogênea, com o número total de nós variando entre 30 e 120 nós, além de um centro de controle fixo com maior raio de transmissão. Os demais nós são distribuídos pela rede de forma aleatória e deslocam-se de acordo com probabilidades definidas. Os nós participam de grupos, que representam agentes humanos nas regiões de desastre e veículos como ambulâncias, bombeiros e de transporte. Os pontos de interesse foram definidos como

duas regiões de desastre, uma região com hospitais e outra com abrigos. Os nós se deslocam entre as regiões, como pode ser visualizado na Figura 5.1.

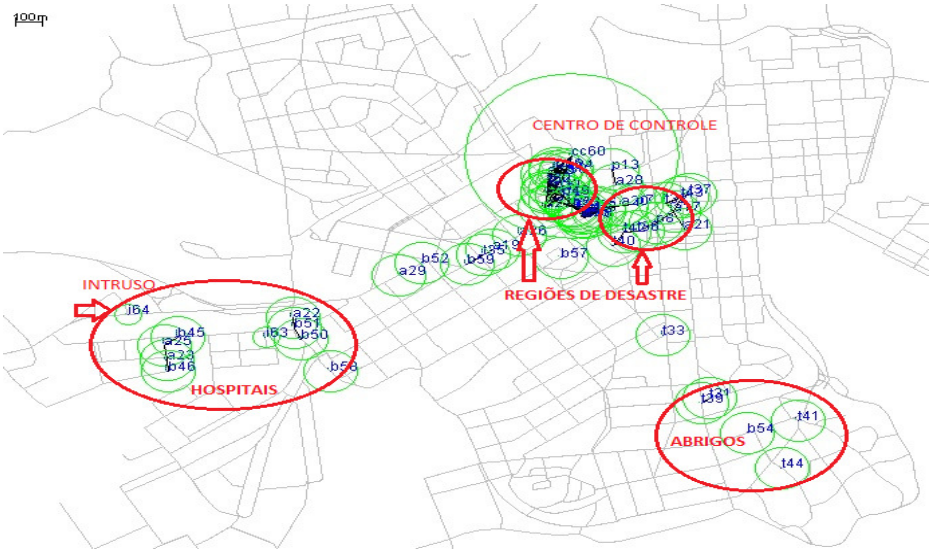

Figura 5.1. Cenário das simulações.

Por considerar o deslocamento em uma região urbana, o cenário utiliza um mapa e as rotas procuram obter o menor caminho possível para o destino dos nós. Foi utilizado o padrão de mobilidade “Shortest Path Map Based Movement” [Ekman, 2008], que é uma derivação do “Random Waypoint”, em que os nós usam o algoritmo de Dijkstra para o menor caminho para definir a rota do local atual até um destino selecionado de maneira randômica, através dos caminhos disponíveis.

Com exceção do centro de controle, os demais nós se movimentam de acordo com a necessidade de recursos, através da região abrangida pela rede, que possui tamanho de 4500 x 3400 metros. Considera-se que veículos transportam vítimas das regiões de desastre para hospitais ou abrigos, enquanto agentes caminham nas regiões para prestar atendimento às vítimas e também enviar informações para toda a equipe de resgate.

Somente existe conexão entre quaisquer dois nós quando ambos estão dentro do respectivo raio de transmissão. Esse raio foi definido como 100m para os nós e 400m para o centro de controle, enquanto a velocidade de transmissão dos dados foi 250kBps e o buffer de mensagens 10MB para cada nó. Mensagens são geradas a cada 30-45 segundos por

algum nó da rede seguindo uma distribuição uniforme e os períodos observados para avaliação foram simulações de 24 horas.

Foram considerados intrusos que podem absorver e descartar pacotes que passam por ele. Para tanto, os intrusos realizam o ataque *greyhole*, permitindo alternar entre encaminhar pacotes ou descartá-los. As rotas podem ser influenciadas pelo intruso, sendo um nó invasor ou um nó legítimo, já violado. Assim, o intruso pode obter informações da rede ou aplicar o ataque de negligência. Como não é esperada uma grande proporção de intrusos, dito anteriormente, o número de nós que realiza ataques foi definido como 3% dos participantes da rede, sendo o menor valor possível igual a 2 intrusos.

5.3. Resultados e Análise

Algumas verificações foram realizadas após implementação, simulação e coleta dos resultados. Inicialmente, era necessário verificar o impacto da utilização do modelo de gerenciamento de segurança adaptativo proposto na probabilidade de entrega de mensagens. Logo após, foi analisado o comportamento da rede em relação aos níveis de segurança propostos nesse modelo.

Os primeiros resultados dos dados coletados corresponderam à probabilidade de entrega das mensagens com utilização do modelo de gerenciamento de segurança adaptativo proposto. A comparação com a taxa obtida sem a sua utilização pode ser observada na Figura 5.2.

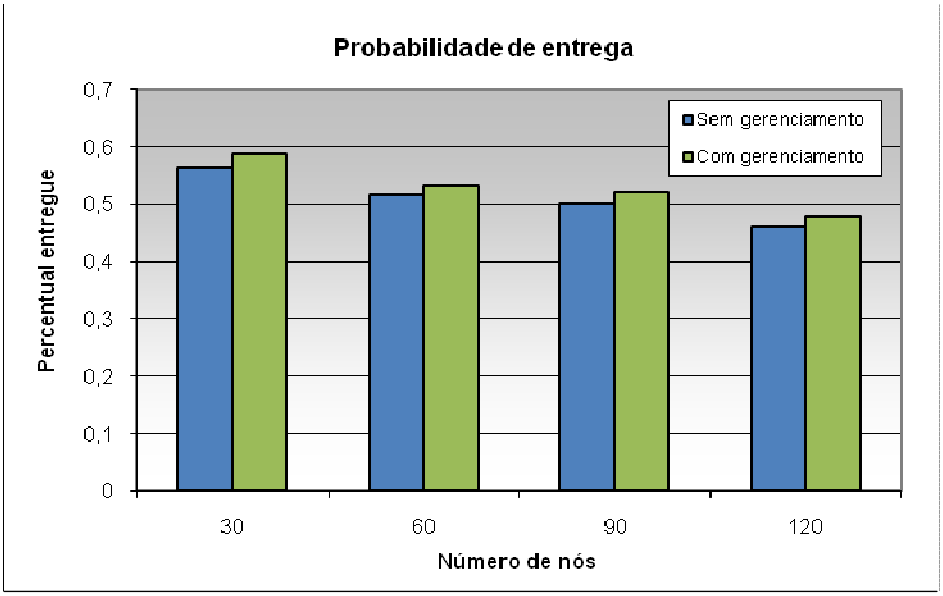

Figura 5.2. Probabilidade de entrega de mensagens da rede.

A análise desses resultados indica que a utilização do gerenciamento apresentou impacto positivo na probabilidade de entrega das mensagens, pois as taxas foram pouco maiores com 30 a 120 nós participantes da rede. A partir dos intervalos de confiança das amostras, com 90% de confiança é possível dizer que a utilização do gerenciamento apresenta melhores taxas. Nas duas situações, observa-se que existe a tendência de diminuição na probabilidade de entrega das mensagens, à medida que aumenta o número de participantes da rede.

A cada simulação, foi verificada ainda a alteração do nível de segurança dos nós, bem como os tempos e situações em que isso ocorre. Os dados coletados são apresentados nos gráficos a seguir com 95% para o intervalo de confiança. Devido a restrições da ferramenta utilizada para os gráficos, não foi possível incluir a representação dos intervalos de confiança. Caso haja interesse, os dados de cada simulação podem ser observados no Apêndice A.

Os tempos decorridos até as transições dos níveis de segurança propostos são mostrados na Figura 5.3. Como todos os nós iniciam a simulação no nível de segurança Baixo, esse é representado somente no tempo inicial. Pode-se observar que houve alteração no nível de segurança apenas a partir do segundo cenário, com 60 nós participando da rede, que

encerraram a simulação no nível Médio. O nível Alto foi alcançado somente com 90 nós participantes, após algum tempo no nível Médio e ainda sem alcançar o nível Crítico no período observado de 24 horas. Somente com utilização de 120 nós na rede de emergência foi alcançado o nível Crítico, sendo assim percorridos todos os níveis de segurança propostos.

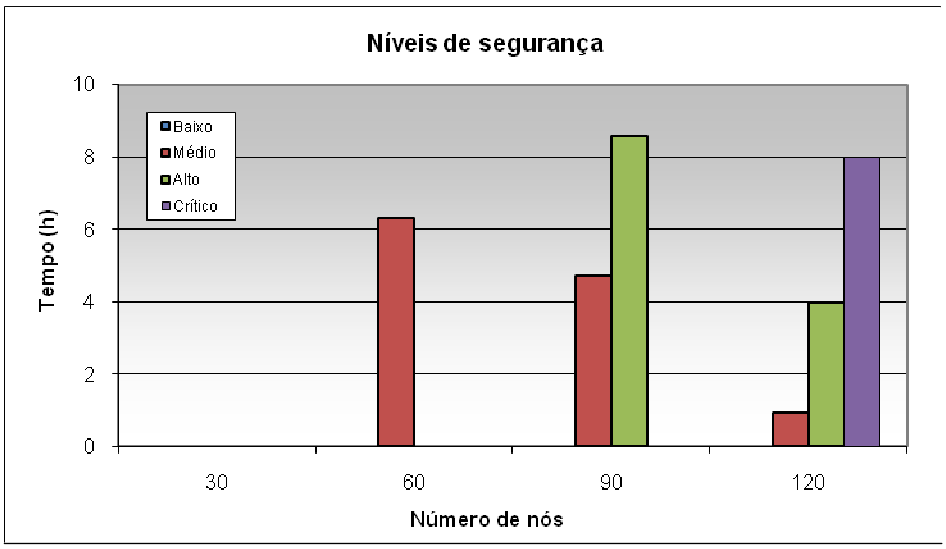

Figura 5.3. Tempo para alcance dos níveis de segurança.

Esses dados indicam que somente em redes com grande número de nós ou em casos específicos, seria necessária a ativação da quantidade máxima de componentes de segurança. Ainda nesses casos, poderia haver economia de recursos durante um tempo com a utilização de menor quantidade de componentes, enquanto não houvesse ameaças à segurança da rede.

Sabendo-se que a rede detectou a necessidade de atingir os níveis de segurança conforme a Figura 5.3, devido ao gerenciamento de segurança adaptativo proposto, é importante verificar se os nós participantes da rede conseguiram se adaptar corretamente através da devida comunicação pelas mensagens de gerenciamento.

A Figura 5.4 apresenta o número de nós que alcançou cada nível de segurança conforme mostrado no gráfico anterior. Todos os nós participantes da rede deveriam utilizar o nível de segurança Baixo, por ser aquele inicialmente definido. Como não houve transição de nível de

segurança com a utilização de 30 nós, todos os participantes encerraram o período analisado sem alcançar outro nível.

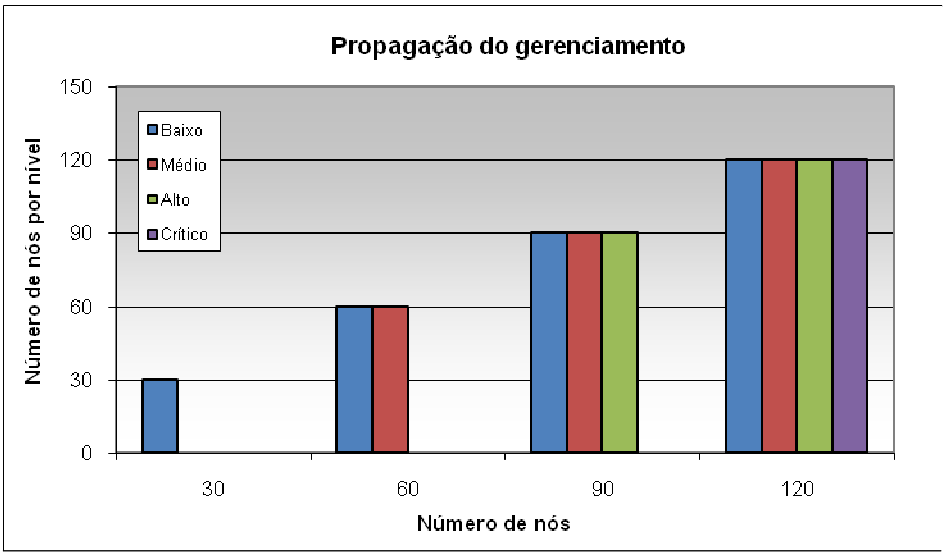

Figura 5.4. Número de nós por nível de segurança ao fim de cada simulação.

Já quando se observa a utilização de 60 nós na rede, todos os nós realizaram a transição solicitada para o nível de segurança Médio. Ou seja, nenhum nó deixou de ser comunicado sobre a mudança e também não houve processamento duplicado de uma mesma transição. Ao serem utilizados 90 nós, observa-se também que todos os nós alcançaram o nível Médio e também o nível Crítico na sequência. Por fim, com 120 nós na rede, percebe-se que todos os nós alcançaram corretamente cada um dos níveis de segurança definidos.

A análise da Figura 5.4 indica que, apesar da conectividade imprevisível, a propagação das mensagens de gerenciamento atinge toda a rede. Quando há alteração do nível de segurança, todos os nós da rede alcançam o nível enviado pelo centro de controle.

Um modelo de gerenciamento de segurança, como apresentado nesse trabalho, permite equilibrar a disponibilidade da rede e a utilização de recursos, ligando e desligando as soluções de segurança quando necessário. Entretanto, o gerenciamento também poderia ter impacto no consumo de recursos da rede. Para avaliar essa possibilidade, verificou-se a quantidade de mensagens geradas na rede.

Foi observado que o número de mensagens de gerenciamento criadas devido à utilização do modelo é muito inferior ao número das demais mensagens da rede, atingindo o percentual máximo de 3% do total de mensagens em situações que o nível Crítico é alcançado. No entanto, foi verificado se a utilização do modelo poderia causar uma sobrecarga de mensagens e consequente aumento no consumo de recursos da rede. A comparação com a taxa obtida sem a sua utilização pode ser observada na Figura 5.5.

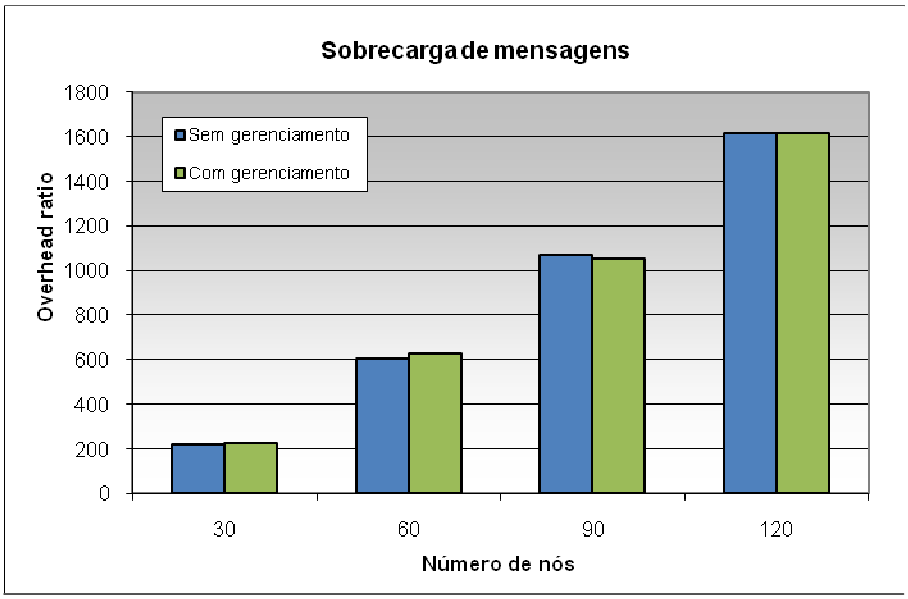

Figura 5.5. Sobrecarga de mensagens gerada na rede.

A análise desses resultados indica que a utilização do gerenciamento não apresentou impacto considerável em relação à sobrecarga de mensagens na rede, pois as taxas variaram dentro dos intervalos de 90% de confiança das amostras. Nas duas situações, observa-se que existe a tendência de aumento de sobrecarga das mensagens, à medida que aumenta o número de participantes da rede. Contudo, pode-se verificar que a utilização do modelo proposto não aumenta a sobrecarga da rede.

Em todas as simulações anteriores, foram considerados 3% dos nós da rede como intrusos. Ainda foram avaliados cenários com variação do número de intrusos: 2, 3, 5 ou 8% dos nós da rede. Os resultados são exibidos na Figura 5.6.

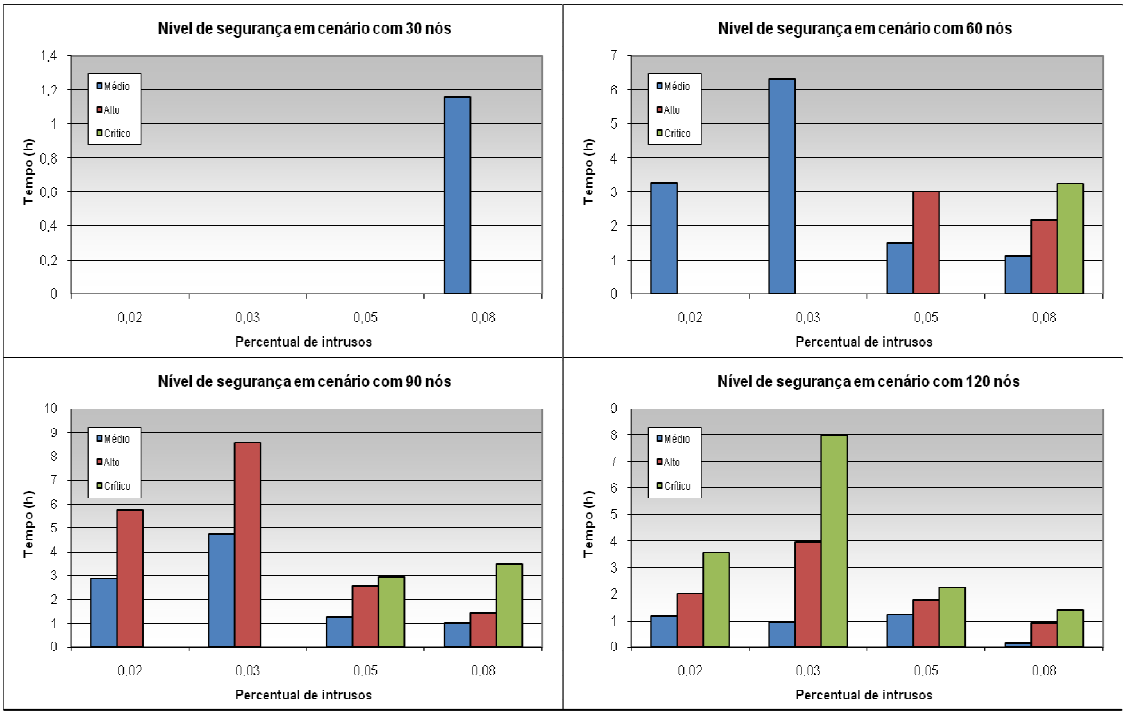

Figura 5.6. Variação do percentual de intrusos na rede.

Os gráficos mostram a relação entre o percentual de intrusos na rede e o nível de segurança atingido durante a simulação. À medida que esse percentual é aumentado, outros níveis de segurança são utilizados e de maneira mais rápida.

Na Figura 5.5, para 30 nós só houve alteração para o nível Médio quando o percentual de intrusos foi de 8% dos nós da rede. Para 60 nós, todos os percentuais apresentaram alteração para o nível Médio, sendo que se alcançou o nível Alto para 5% de intrusos e o nível Crítico para 8% de intrusos. No caso de 90 nós na rede, os níveis Médio e Alto foram alcançados para todos os percentuais, enquanto o nível Crítico foi acionado somente quando houve 5% e 8% de intrusos. Por fim, percebe-se que todos os percentuais atingiram o nível Crítico com 120 nós na rede, reduzindo-se o tempo decorrido das alterações à medida que o percentual de intrusos foi aumentado.

Considerando o modelo de gerenciamento de segurança adaptativo apresentado, é possível avaliar três cenários distintos:

1 - Rede sem segurança: Nesse caso, a disponibilidade da rede pode ser comprometida pela presença de intrusos, reduzindo a produtividade da rede;

2 - Rede com uso constante de algumas soluções de segurança: Nesse caso, a presença de intrusos é evitada ou reduzida, aumentando a disponibilidade da rede, mas o consumo de recursos aumenta para executar essas soluções de segurança;

3 - Rede com gerenciamento de segurança para ativar soluções de segurança somente quando necessário. Se nenhum intruso é detectado, a rede pode utilizar poucos componentes de segurança, minimizando o consumo de energia para prolongar o tempo de vida da rede. Quando a rede detecta um intruso, a solução de gerenciamento aumenta o nível de segurança evitando o efeito do intruso.

A utilização de recursos no terceiro cenário com mecanismos de segurança dependerá da presença de intrusos. No melhor caso, somente sistemas centralizados de detecção de intrusos executam, sem execução nos nós. Quando um primeiro intruso é detectado, o gerenciamento de segurança começa a ativar soluções de segurança através do envio de mensagens. As soluções de segurança serão ligadas gradualmente, evitando o efeito dos intrusos. Em grandes redes, a rede pode ser dividida em setores e as soluções de segurança podem ser ativadas somente onde intrusos são detectados.

Foi possível verificar nas simulações que a utilização do modelo de gerenciamento de segurança resulta em vantagens independente do número de nós da rede, pois nenhum cenário demonstrou necessidade de utilizar todos os componentes de segurança inicialmente. Somente no cenário com maior número de nós atingiu-se o nível de segurança Crítico, sendo que todos os cenários preservaram a confiabilidade da rede.

Capítulo 6

Conclusões

Esse trabalho apresenta um modelo de gerenciamento de segurança adaptativo para redes de emergência, que são formadas em casos de carência de infra-estrutura de rede, para auxiliar as equipes de resgate na comunicação nessas situações. O objetivo do gerenciamento proposto é evitar o efeito de ataques e economizar recursos ao ativar os componentes de segurança apenas quando for necessário.

O modelo para o gerenciamento de segurança apresentado estabelece a integração entre mecanismos de segurança para redes DTN que podem ser utilizados como componentes de segurança em redes de emergência. É possível utilizar várias combinações desses componentes de segurança, de acordo com as necessidades demonstradas pelo gerenciamento da rede.

O modelo propõe o auto-gerenciamento da rede. De maneira autonômica, o centro de controle pode configurar níveis de segurança nos nós, adaptando a utilização de componentes de segurança para evitar o efeito dos intrusos. Quando ocorre um evento de detecção de intrusos, é gerada uma decisão autonômica para alterar o nível de segurança da rede.

Os níveis de segurança definidos permitem que os diversos componentes de segurança possam ser facilmente configurados de acordo com a situação momentânea ou meio em que a rede se encontra. A utilização dos componentes será gerenciada e monitorada através das MIBs definidas.

As análises realizadas demonstraram que houve impacto positivo na probabilidade de entrega das mensagens e não houve variação representativa na sobrecarga de mensagens da rede devido à utilização

desse modelo de gerenciamento de segurança. Os resultados indicam que somente redes com grande número de nós ou ainda casos específicos apresentarão necessidade da ativação da quantidade máxima de componentes de segurança. Mesmo nessas situações, a utilização de menor número de componentes pode representar economia de recursos enquanto não forem detectadas ameaças à segurança da rede.

Apesar da conectividade imprevisível nessas situações, verificou-se que algumas poucas mensagens são necessárias para implementar o gerenciamento de segurança e que as mensagens de gerenciamento enviadas alcançam todos os nós participantes. Assim, é possível economizar recursos sem perda de produtividade da rede enquanto não há evidência de intrusos.

6.1. Contribuições

As contribuições desse trabalho podem ser destacadas no aumento da segurança em redes tolerantes a interrupções (DTN) e especificamente no cenário de redes de emergência, ao propor um modelo para o gerenciamento de segurança que estabelece a integração entre mecanismos que podem ser utilizados como componentes de segurança nessas redes.

O modelo propõe um gerenciamento de segurança orientado por mensagens, enviadas em casos de detecção de intrusos ou para utilização de: encriptação, assinatura digital, protocolo para estabelecimento de chaves, protocolos para roteamento dinâmico seguro e seleção de prioridade de pacotes para replicação. Esses componentes de segurança podem ser configurados através de mensagens e segundo as definições realizadas de níveis de segurança.

Por não haver muitas referências nesse campo de pesquisa, as definições de mensagens, eventos e informações de gerenciamento (MIB) são importantes contribuições. Através dessas definições, foi possível conceber um modelo de gerenciamento de segurança adaptativo que

possibilita a reconfiguração da rede DTN, segundo a abordagem de redes autonômicas, e através do qual poderá ser obtido um nível maior de segurança para essas redes.

A utilização de mecanismos de segurança integrados e de maneira adaptável às necessidades da rede é uma proposta inovadora na abordagem de problemas relacionados à segurança em redes DTN. A concepção e a implementação dessa proposta podem ser referência para outros trabalhos.

O modelo proposto foi avaliado através de simulações, comprovando a inexistência de impacto na entrega de mensagens e mostrando que os mecanismos de segurança podem ser ativados somente se necessário.

6.2. Trabalhos futuros

Para continuidade desse trabalho, espera-se a adaptação do modelo de gerenciamento de segurança à medida que novos mecanismos de segurança forem propostos para redes tolerantes a interrupções. O que se aplica também a novos conceitos e pesquisas que porventura alterem características das redes de emergência.

Propõe-se ainda o estudo de soluções de segurança específicas para os protocolos de roteamento de redes DTN, bem como alterações de componentes de segurança utilizados pelo gerenciamento de acordo com o tipo de ataque detectado.

Referências Bibliográficas

Asplund, M.; Nadjm-Tehrani, S. & Sigholm, J. (2008). *Emerging information infrastructures: Cooperation in disasters.* International Workshop on Critical Information Infrastructures Security.

Burgess, J.; Bissias, G.; Corner, M. D. & Levine, B. N. (2007). *Surviving Attacks on Disruption-Tolerant Networks without Authentication.* ACM International Symposium on Mobile Ad Hoc Networking and Computing.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K. & Weiss, H. (2007). *Delay-tolerant networking architecture.* Technical report, Internet RFC 4838.

Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Travis, E. & Weiss, H. (2001). *Interplanetary Internet (IPN): Architectural Definition.* Technical report, IPN Research Group.

Chaintreau, A.; Hui, P.; Crowcroft, J.; Diot, C.; Gass, R. & Scott, J. (2006). *Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms.* IEEE International Conference on Computer Communications.

Chen, L. J.; Yu, C. H.; Sun, T.; Chen, Y. C. & Chu H. H. (2006). *A hybrid routing approach for opportunistic network.* ACM Special Interest Group on Data Communication.

Chitumalla, P. V.; Harris, D.; Thuraisingham, B. & Khan L. (2008). *Emergency Response Applications: Dynamic Plume Modeling and Real-Time Routing.* IEEE Internet Computing, Vol. 12, No. 1, pp. 38-44.

Currion, P.; Silva, C. & Walle, B. V. (2007). *Open source software for disaster management.* Communications of the ACM, Vol. 50, No. 3, pp. 61-65.

Durst, R. C. (2002). *An infrastructure security model for delay tolerant networks.* Disponível em http://www.dtnrg.org/wiki/Docs.

Ekman, F.; Keränen, A.; Karvo, J. & Ott, J. (2008). *Working Day Movement Model* In Proceedings of ACM SIGMOBILE Workshop on Mobility Models.

Engel, T.; Fischer, D.; Scherer, T. & Dagmara Spiewak, D. (2006). *A Survey on Security Challenges in Next Generation Mobile Networks.* International Conference on Mobile Computing and Ubiquitous Networking.

Fall, K. (2003). A Delay-Tolerant Network Architecture for Challenged Internets. *In Proceedings of ACM Special Interest Group on Data Communication*, pp. 27-34.

Fall, K. (2004). *Messaging in difficult environments.* Technical Report IRB-TR-04-019, Intel Research Berkeley.

Fall, K. (2005). *Disruption tolerant networking for heterogeneous ad-hoc networks.* IEEE Military Communications Conference (MILCOM).

Jones, E. P. C.; Li, L.; Ward, P. A. S. (2005). *Practical routing in delay-tolerant networks.* ACM SIGCOMM Workshop on Delay-tolerant Networking.

Holme, P.; Kim, B. J.; Yoon, C. N. & Han, S. K. (2002). *Attack Vulnerability of Complex Networks.* APS Physics Review E.

Hu, Y. C.; Perrig, A. & Johnson, D. B. (2003). *Rushing Attacks and Defense in Wireless Ad Hoc Network.* IEEE International Conference on Web Information Systems Engineering.

Kate, A.; Zaverucha, G. M. & Hengartner, U. (2007). *Anonymity and Security in Delay Tolerant Networks.* International Conference on Security and Privacy in Communication Networks.

Keranen, A.; Ott, J. & Kärkkäinen, T. (2009). *The ONE Simulator for DTN Protocol Evaluation.* ACM International Conference on Simulation Tools and Techniques.

Lorincz, K.; Malan, D.; Fulford-Jones, TRF.; Nawoj, A.; Clavel, A.; Shnayder, V.; Mainland, G.; Moulton, S. & Welsh, M. (2004). *Sensor Networks for Emergency Response: Challenges and Opportunities.* IEEE Pervasive Computing, Vol. 3, No. 4, pp. 16-23.

Manet (2008). Ietf working group on mobile ad-hoc networks. Disponível em: http://www.ietf.org/html.charters/manet-charter.html.

Mehrotra, S.; Znati, T. & Thompson, C. W. (2008). *Crisis Management.* IEEE Internet Computing, Vol. 12, No. 1, pp. 14-17.

Mota, V. F. S.; Silva, T. H. & Nogueira, J. M. S. (2009). *Introduzindo Tolerância a Interrupção em Redes Ad Hoc Móveis para Cenários de Emergência.* Simpósio Brasileiro de Redes de Computadores.

Oliveira, C. T.; Moreira, M. D. D.; Rubinstein, M. G.; Costa, L. H. M. K. & Duarte, O. C. M. B. (2007). *Redes Tolerantes a Atrasos e Desconexões.* Minicursos do Simpósio Brasileiro de Redes de Computadores, pp. 203-256.

Oliveira, S.; Oliveira, T. R. & Nogueira, J. M. S. (2008). *Um Modelo de Gerenciamento de Segurança em Redes de Sensores Sem Fio.* Simpósio Brasileiro de Redes de Computadores.

Ott, J.; Kutscher, D. & Dwertmann, C. (2006). Integrating DTN and MANET routing. *In Proceedings of SIGCOMM workshop on Challenged networks,* pp. 221-228.

Portmann, M. & Pirzada, A. A. (2008). *Wireless Mesh Networks for Public Safety and Crisis Management Applications.* IEEE Internet Computing, Vol. 12, No. 1, pp. 18-25.

Seth A. & Keshav S. (2005). *Practical Security for Disconnected Nodes.* Workshop on Secure Network Protocols.

Shank, N.; Sokol, B.; Hayes, M. & Vetrano, C. (2008). *Human services data standards: Current progress and future visions in crisis response.* International Conference on Information Systems for Crisis Response.

Silva, F. A.; Ruiz, L. B.; Braga, T. R. M.; Nogueira, J. M. S. & Loureiro, A. A. F. (2005). *MannaNMP: Um protocolo de Gerenciamento para Redes de Sensores Sem Fio.* Simpósio Brasileiro de Redes de Computadores.

Symington S. F.; Farrell S.; Weiss H. & Lovell P. (2009). *Bundle Security Protocol Specification.* draft-irtf-dtnrg-bundle-security-08.txt. Acessado em 12/12/2009.

Walle, B. & Turoff, M. (2008). *Decision support for emergency situations.* Information Systems and E-Business Management, Vol. 6, No. 3, pp. 295-316.

Warthman, F. (2008). *Delay-Tolerant Networks (DTNs) - A Tutorial.* Technical Report, InterPlanetary Internet Special Interest Group.

Apêndice A

A seguir, são apresentados os dados de cada simulação realizada para validar o modelo de gerenciamento de segurança adaptativo para redes de emergência proposto nesse trabalho.

Tabela A.1. Probabilidade de entrega de mensagens da rede

Média

Número de nós	Sem gerenciamento	Com gerenciamento
30	0,5643	0,5879
60	0,5176	0,532
90	0,5001	0,5206
120	0,4602	0,478

Intervalo de Confiança

Número de nós	Sem gerenciamento	Com gerenciamento
30	0,0096	0,0092
60	0,0081	0,0069
90	0,0083	0,0081
120	0,0074	0,0079

Tabela A.2. Tempo para alcance dos níveis de segurança

Número de nós	Nível	Média	Intervalo de Confiança
60	Médio	6,3293	1,0964
90	Médio	4,7019	0,4654
90	Alto	8,5752	1,1884
120	Médio	0,9149	0,1056
120	Alto	3,9642	0,3924
120	Crítico	7,9921	1,3845

Tabela A.3. Número de nós por nível de segurança ao fim de cada simulação

Número de nós	Nível	Média	Intervalo de Confiança
60	Médio	60	0,6929
90	Médio	90	0,6929
90	Alto	90	1,3859
120	Médio	120	1,3859
120	Alto	120	1,3859
120	Crítico	120	2,0788

Tabela A.4. Sobrecarga de mensagens gerada na rede

Média

Número de nós	Sem gerenciamento	Com gerenciamento
30	219,0	227,1
60	604,37	626,1
90	1067,6	1054,8
120	1614,9	1614,6

Intervalo de Confiança

Número de nós	Sem gerenciamento	Com gerenciamento
30	31,8395	18,8669
60	50,2096	91,0261
90	103,4759	87,6303
120	156,5224	187,792

Tabela A.5. Variação do percentual de intrusos na rede

Número de nós	Intrusos (%)	Nível	Média (h)	Intervalo de Confiança
30	8	Médio	1,1546	0,1119
60	2	Médio	3,2646	0,2712
60	3	Médio	6,3293	0,9201
60	5	Médio	1,4819	0,1231
60	5	Alto	2,9920	0,2899
60	8	Médio	1,1058	0,1071
60	8	Alto	2,1510	0,1787
60	8	Crítico	3,2462	0,4719
90	2	Médio	2,8742	0,2387
90	2	Alto	5,7426	0,5565
90	3	Médio	4,7019	0,4557
90	3	Alto	8,5752	0,7124
90	5	Médio	1,2502	0,1817
90	5	Alto	2,5706	0,2135
90	5	Crítico	2,9353	0,2845
90	8	Médio	1,0083	0,0977
90	8	Alto	1,4097	0,1366
90	8	Crítico	3,4918	0,3384
120	2	Médio	1,1455	0,0951
120	2	Alto	1,9990	0,2906
120	2	Crítico	3,5618	0,2959
120	3	Médio	0,9148	0,0886
120	3	Alto	3,9642	0,3842
120	3	Crítico	7,9921	0,7746
120	5	Médio	1,2272	0,1019
120	5	Alto	1,7804	0,2588
120	5	Crítico	2,2471	0,1866
120	8	Médio	0,1175	0,0097
120	8	Alto	0,8937	0,1299
120	8	Crítico	1,3809	0,1147