Modelo de Gerenciamento de Segurança Adaptativo para Redes de Emergência

Thiago Rodrigues de Oliveira[1], Sérgio de Oliveira[2], José Marcos Nogueira[1]

thiagool@dcc.ufmg.br, sergiool@ufsj.edu.br, jmarcos@dcc.ufmg.br

[1] Departamento de Ciência da Computação, Universidade Federal de Minas Gerais
Av. Antônio Carlos, 6627, Belo Horizonte, MG - Brasil

[2] Universidade Federal de São João Del Rei
Campus Alto Paraopeba, Ouro Branco, MG - Brasil

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. This paper proposes a security management framework to dynamically configure and reconfigure emergency networks, with goal to adapt the use of security components according to management information received by decision-maker responsible entities. The security management model includes the definition of security levels, management information base, protocol messages and events. The evaluations realized show an emergency network behavior with activation of security mechanisms if necessary.*

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. Esse artigo propõe um modelo de gerenciamento de segurança para configurar dinâmica e autonomicamente redes de emergência, com objetivo de adaptar a utilização de componentes 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 gerenciáveis, mensagens do protocolo e eventos. As avaliações realizadas mostram o comportamento de uma rede de emergência com a ativação de mecanismos de segurança quando necessário.*

1. Introdução

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.

Um fator que favorece a montagem de redes de emergência é a popularização de dispositivos móveis como notebooks, PDAs 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) 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*) [1]. Através de um esquema de comunicação assíncrona, uma rede DTN pode ter melhor alcançabilidade, especialmente em redes com nós esparsos com as seguintes propriedades: comunicação baseada em mensagens assíncronas agregadas (*bundles*); não há necessidade de um caminho fim-a-fim, pois as mensagens podem ficar armazenadas nos nós até que seja estabelecida uma conexão; atrasos podem ser longos e variados; por fim, sua tolerância a altas taxas de erros.

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.

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

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.

Além disso, características específicas desse tipo de redes, como mobilidade imprevisível e latência variável, 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.

O interesse em segurança varia dependendo do ambiente e aplicação, embora autenticação e privacidade sejam geralmente críticos [3]. 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.

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.

O conteúdo é apresentado em seções, sendo que essa primeira apresenta o problema abordado. A Seção 2 apresenta os trabalhos relacionados e a Seção 3, o modelo de rede adotado para esse trabalho. A Seção 4 define os componentes de segurança utilizados no modelo de gerenciamento proposto. Aspectos para prover auto-gerenciamento são descritos na Seção 5. O modelo proposto é detalhado na Seção 6 e sua avaliação é apresentada na Seção 7. Na Seção 8, as conclusões e trabalhos futuros são apresentados.

2. Trabalhos Relacionados

Uma arquitetura para redes de emergência e alguns requisitos de segurança foram propostos em [3]. 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.

O modelo de segurança para a arquitetura DTN difere das redes tradicionais, pois o conjunto de princípios inclui os próprios roteadores [2]. 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.

Tipicamente, soluções de redes móveis ad hoc têm sido modificadas e existem pesquisas de segurança distribuída, como o uso de autoridades certificadas distribuídas [4]. Soluções originais da comunidade de pesquisa de redes tolerantes a atrasos e desconexões incluem o uso da encriptação baseada na identidade [5], 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 [6] foram apresentadas algumas idéias preliminares sobre a distribuição e gerenciamento de chaves para DTN, mas percebe-se que ainda são questões abertas.

Em [7], 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.

Este trabalho propõe também a integração de redes de sensores sem fio (RSSF) a redes de emergência. Para tanto, considera a utilização do modelo de gerenciamento de segurança proposto para RSSF em [8], bem como suas definições para os sensores.

Tanto quanto podemos saber, não existe na literatura uma abordagem de provimento de segurança que seja dinâmica e considere os objetivos ou restrições de recursos das redes de emergência.

3. 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 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.

Do ponto de vista de segurança, o centro de controle é confiável, ou seja, não está sujeito a ataques, e não apresenta restrições de recursos como os outros nós participantes da rede. O centro de controle é origem ou destino de todas as mensagens da rede. Somente são considerados participantes autorizados na rede, para evitar os efeitos negativos da inclusão de possíveis intrusos.

Objetiva-se neste trabalho propor soluções de segurança para redes de emergência com características de serem: *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.

4. Componentes de Segurança para Redes de Emergência

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 comparativamente grandes antes de se iniciar a comunicação.

Para redes tolerantes a interrupções com recursos de conexão preciosos, uma técnica fim-a-fim para segurança não é muito atrativa. Existe a possibilidade de utilizar recursos escassos para mensagens indesejáveis quando se transporta tráfego por todo o caminho até seu destino sem realizar autenticação e checagem de controle de acesso.

Esse trabalho considera o roteamento dinâmico seguro, a seleção de prioridade de pacotes para replicação, a existência de mecanismos de detecção de intrusos, a utilização de técnicas de gerenciamento de chaves, a possibilidade de criptografia salto-a-salto e fim-a-fim, bem como um esquema de revogação de nós.

As soluções de segurança de maior interesse para este trabalho foram organizadas e classificadas em componentes de acordo com seus objetivos.

4.1. Roteamento dinâmico seguro

Redes de emergência são baseadas na auto-configuração, auto-manutenção e auto-otimização. A maior parte dos protocolos de roteamento propostos para redes DTN não considera o aspecto da segurança como um dos objetivos principais. Assim, torna-se importante considerar o roteamento para garantir a segurança da rede.

O ataque mais simples consiste em fazer com que um nó descarte todos os pacotes que 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.

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. Sem autenticação,

intrusos poderiam propagar informações incorretas sobre as tabelas de roteamento de qualquer nó.

Os protocolos de roteamento mais divulgados foram considerados: *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 [12].

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 e ainda ser indicador para caracterizar urgência e consequente tempo de vida (TTL) das mensagens, pois há mensagens que perdem o sentido se não forem entregues em certo espaço de tempo.

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 possuem um tempo de vida determinado pelo centro de controle e inferior ao das demais, para descarte após término desse tempo.

4.2. Detecção de intrusos

A detecção de intrusos em redes de emergência deve lançar mão de mais técnicas diferentes das redes convencionais, devido à diferença nos modelos, ataques e recursos. Dois tipos de técnicas podem ser utilizados para detecção de intrusos: centralizada ou descentralizada. Na técnica centralizada, o centro de controle é responsável por detectar intrusos, visto que possui um grande conjunto de informações à sua disposição, o que facilita o processo de detecção. Na técnica descentralizada, alguns ou todos os nós executam operações simples para detectar intrusos [4]; a grande vantagem é a disponibilidade instantânea da informação, visto que os nós podem detectar os ataques exatamente no momento em que eles ocorrem.

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

4.3. 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.

4.4. Técnicas Criptográficas

Os processos de criptografia têm como objetivo comum impedir que uma determinada entidade denominada intruso obtenha informações sigilosas. Os objetivos da rede devem determinar qual técnica de criptografia tem de ser usada, tais como

formas de encriptação e assinatura. 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.

4.4.1. Encriptação

Encriptação é uma técnica para adicionar privacidade a mensagens da rede. Isso pode ser um processo fim-a-fim, feito uma vez por mensagem, ou um processo salto-a-salto, feito cada vez que uma mensagem atinge um nó de repasse.

A abordagem desse trabalho considera mensagens que tem os centros de controle como origem ou destino, 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, através de verificação de integridade ou autenticação de origem e destinatário das mensagens.

Protocolos DTN devem prover um meio de encriptar elementos de forma que mensagens em trânsito não possam ser lidas na prática. O protocolo de agregação não provê nenhuma confidencialidade para a origem ou destino [2]. 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.

Em redes DTN, o tempo de expiração das credenciais provê um mecanismo para lidar com sistemas de compromisso. 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 do conjunto de credenciais.

4.4.2. Assinatura

Assinatura é um processo criptográfico que adiciona um código autenticado como uma chave a uma mensagem e o recebedor tem que conhecer a chave para verificar a assinatura. As chaves podem ser compartilhadas fim-a-fim e permitir verificação somente pelo centro de controle ou compartilhadas pelos nós vizinhos para permitir a verificação salto-a-salto. Técnicas de assinatura tornam possível a autenticação e integridade na comunicação. O uso dessas técnicas de segurança pode evitar a inserção de pacotes falsos e a adulteração de mensagens.

Uma das diferenças das redes DTN é que uma mensagem autenticada usando uma assinatura digital, a princípio, pode ser verificada por qualquer elemento da rede no caminho. Se a mensagem contém informação suficiente, então qualquer nó pode pelo menos verificar a exatidão criptográfica da assinatura [4].

4.4.3. Gerenciamento de chaves

Um esquema de distribuição de chaves seguro e eficiente permite a autenticação dos nós da rede. O controle de acesso à rede pode impedir e eliminar diversos tipos de ataques, a menos que o inimigo comprometa nós legítimos da rede. A captura e a adulteração de um nó podem permitir ao inimigo utilizar as chaves armazenadas nesse nó. É necessário prever quais chaves podem ser descobertas a partir dessa adulteração.

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 [7]. 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.

As características das redes DTN exigem novas abordagens para que seja possível atender os requisitos de segurança necessários a algumas aplicações. Por isso, nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado [6].

4.4.4. Criptografia baseada na identidade

Como uma área recente de pesquisa, os mecanismos que utilizam criptografia baseada na identidade [5] fornecem muitos dos benefícios da criptografia de chave pública e reduzem o overhead envolvido na obtenção e verificação de chaves públicas. Embora esse mecanismo sofra alguns inconvenientes por requerer que os destinatários se comuniquem com um servidor, parece 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.

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 autoridade DTN e 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 e os demais roteadores podem confiar na autenticação dos roteadores anteriores para verificar a autenticidade. Além de os roteadores descartarem 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.

5. Decisões Autonômicas

Redes de emergência têm de ser auto-adaptáveis, configurando seus componentes para o uso racional dos recursos. Neste trabalho, componentes de segurança são configurados baseados em eventos gerados por sistemas de detecção de intrusos.

Eventos de detecção de intrusos configuram autonomicamente componentes de segurança. Intrusos detectados pelo centro de controle são revogados usando mensagens autenticadas. Quando ocorre detecção de maneira descentralizada, um evento de detecção de intruso é gerado e componentes de segurança são ativados, mas o nó suspeito não pode ser revogado, pois somente o centro de controle é confiável.

Tabela 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

A Tabela 1 exibe eventos e ações autonômicas geradas pelos eventos. Em geral, a detecção de 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.

No trabalho relatado neste artigo, 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.

A Tabela 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.

Tabela 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

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. Como não há conhecimento das probabilidades de encontro, os nós utilizam o protocolo de roteamento *epidemic*.

No nível Médio, alguns roteadores habilitam a detecção de intrusos e também é ativada criptografia salto-a-salto. Os componentes escolhidos nesse nível implicam em uma sobrecarga de processamento e rede, devendo-se 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. Como a replicação de mensagens no roteamento é crucial para conseguir a tolerância a ataques, passa-se a utilizar o protocolo spray and wait no modo binário. 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.

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 conhecem algumas chaves da rede. Assim, utiliza-se criptografia redundante, fim-a-fim e salto-a-salto. Dessa forma, um intruso terá de conhecer várias chaves para ter acesso às mensagens da rede. Todos os roteadores que armazenam e repassam as 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. 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.

6. Modelo de Gerenciamento

O modelo de gerenciamento, apresentado a seguir, é composto de uma base de informações de gerenciamento, mensagens trocadas e eventos. O modelo considera que os componentes de segurança descritos acima podem ser parte de situações de gerenciamento. Nesse sentido, a configuração dos componentes de segurança é dinâmica, o que significa que eles podem ser incluídos, excluídos, ativados, e desativados em tempo de operação. Eventos fornecem informações para a rede no sentido de tornar possível a configuração e a re-configuração dos componentes de segurança de uma maneira autonômica.

6.1. Base de Informações de Gerenciamento (MIB)

Para configurar componentes de segurança, um número de objetos de gerenciamento foi definido para a MIB. Os objetos são organizados de acordo com o tipo de componente de segurança que os utilizam: criptografia, dados e administração.

6.1.1. Criptografia

Objetos booleanos indicam se o sistema usa uma função específica de segurança; seus nomes são auto-explicativos: Encriptação fim-a-fim, Encriptação salto-a-salto, Assinatura fim-a-fim, Assinatura salto-a-salto, e Criptografia baseada na identidade.

6.1.2. Dados

Vários tipos de controle de dados são enviados através da rede pelos nós ou pelo centro de controle. Uma parte deles foi definida pela MIB:

Nível de segurança (Choice) ⇒ Baixo (0), Médio (1), Alto (2), Crítico (3);
Protocolo de roteamento (Choice) ⇒ Direct delivery (0), Epidemic (1), PRopHet (2), Spray and Wait (3);
Utiliza priorização? (Boolean) ⇒ Indica se utiliza priorização dos pacotes;
Intruso detectado? (Boolean) ⇒ Indica se um intruso foi detectado na rede;
Identificador do intruso (ID) ⇒ Identificador do intruso detectado;
Identificador de nó revogado (ID) ⇒ Identifica o nó intruso para ser revogado;
Lista de nós revogados (List) ⇒ Lista de nós suspeitos e revogados;
Lista de chaves revogadas (List) ⇒ Lista de chaves revogadas por um nó.

6.1.3. Administração

Tempo de Vida de Mensagens (Integer) ⇒ Indica o TTL das mensagens que não forem urgentes;
Tempo de Vida de Mensagens Urgentes (Integer) ⇒ Indica o TTL das mensagens que foram *definidas como urgentes;*
Mensagens de gerenciamento enviadas (Integer) ⇒ número de mensagens de gerenciamento enviadas pelo nó;
Mensagens de gerenciamento recebidas (Integer) ⇒ número de mensagens de gerenciamento recebidas pelo nó;
Mensagens de dados enviadas (Integer) ⇒ número de mensagens de dados enviadas pelo nó;
Mensagens de dados recebidas (Integer) ⇒ número de mensagens de dados recebidas pelo 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.

6.2. Definição das Mensagens

O modelo propõe um gerenciamento de segurança orientado por mensagens, onde mensagens de controle são usadas para ativar ou desativar componentes: detecção de intrusos, utilização de criptografia, protocolos para roteamento dinâmico seguro, seleção de prioridade de pacotes para replicação, entre outros. Uma mensagem indicando a presença de um intruso colocaria 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.

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 [8] bem como suas definições e utiliza o formato das mensagens do protocolo de gerenciamento MannaNMP [9], que descreve os serviços providos e o formato das mensagens, assim como a base de informações de gerenciamento.

Um número de mensagens de gerenciamento foi definido e é listado a seguir. Em termos do modelo gerente/agente, elas são do tipo *set* e são usadas para estabelecer ou alterar os valores dos objetos, como definido no protocolo MannaMNP.

6.2.1. Mensagens para criptografia

As mensagens são para: ativação de encriptação fim-a-fim; ativação de encriptação salto-a-salto; ativação de assinatura fim-a-fim; ativação de assinatura salto-a-salto; ativação de criptografia baseada na identidade.

6.2.2. Mensagens de dados

As mensagens definidas são: *mudança no nível de segurança* (mudança de configuração dos componentes de segurança); *mudança no protocolo de roteamento*; *utilização de priorização das mensagens*; *detecção de intruso* (coloca a rede em estado de alerta e envia o identificador do intruso para o centro de controle); *revogação de nós* (inclui o identificador do nó revogado na lista); *revogação de chave* (inclui a chave revogada na lista de chaves revogadas de nós recebedores).

6.2.3. Mensagens para administração

As mensagens são para alteração do tempo de vida das mensagens, diferenciando entre as que foram ou não definidas urgentes.

6.3. Eventos

Na ocorrência de eventos, os nós enviam mensagens para informar o centro de controle. Essas mensagens são usadas pelo centro de controle para alterar a configuração da rede, o que pode ser feito imediatamente ou algum tempo depois. No caso de redes hierárquicas, as mensagens seriam encaminhadas para os maiores níveis de hierarquia até alcançar o gerente. Nós intermediários podem tomar decisões em resposta aos eventos informados, o que torna a rede mais inteligente e pode diminuir o fluxo de mensagens. Para reduzir o uso de recursos, a responsabilidade de monitoramento de alguns ou todos os eventos é atribuída ao centro de controle ou somente a alguns nós. A comunicação baseia-se no protocolo MannaNMP e utiliza mensagens de *trap*.

Os eventos definidos são os seguintes: *Detecção de intruso* (nó identificou um nó suspeito); *Revogação de chave* (um nó intruso foi revogado); *Inserção de novo nó* (um novo nó vizinho foi identificado com chaves da rede e não teve sua participação na rede confirmada); *Nível mínimo de energia* (um nível mínimo de energia de um nó foi alcançado, as chaves desse nó têm de ser revogadas).

7. Avaliação

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 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 1.

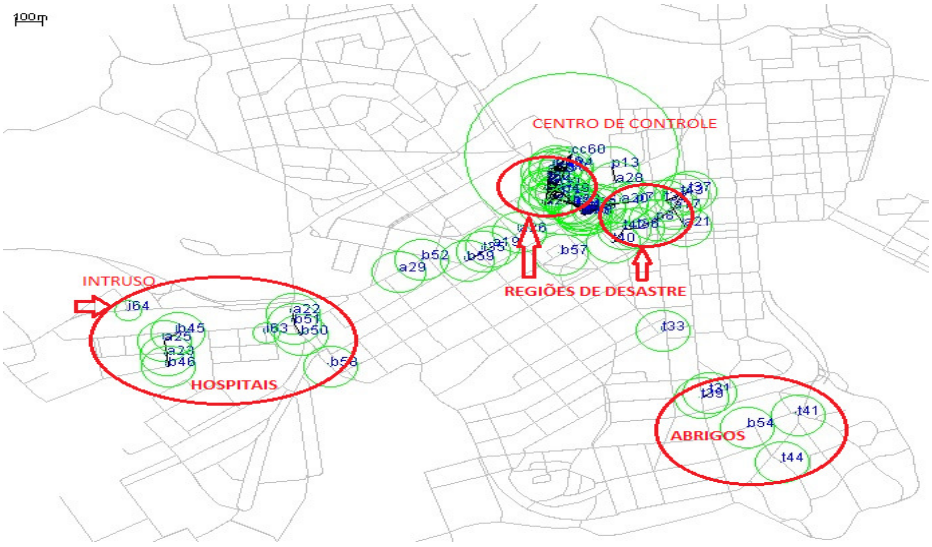

Figura 1 - Cenário das simulações

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*" [10], que é uma derivação do "*Random Waypoint*", onde 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.

Para considerar as características da rede DTN, utilizou-se o simulador The ONE (*Opportunistic Networking Evaluator*) [11], 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, no mínimo oito vezes, sendo alterada a semente geradora do padrão de mobilidade.

O número de nós intrusos foi definido como 3% dos participantes da rede, sendo o menor valor possível de 2 intrusos. Somente existe conexão entre 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. Foi simulado um período de 24 horas.

A cada simulação, foi verificada a alteração do nível de segurança dos nós, bem como os tempos em que isso ocorre, apresentados nos gráficos a seguir.

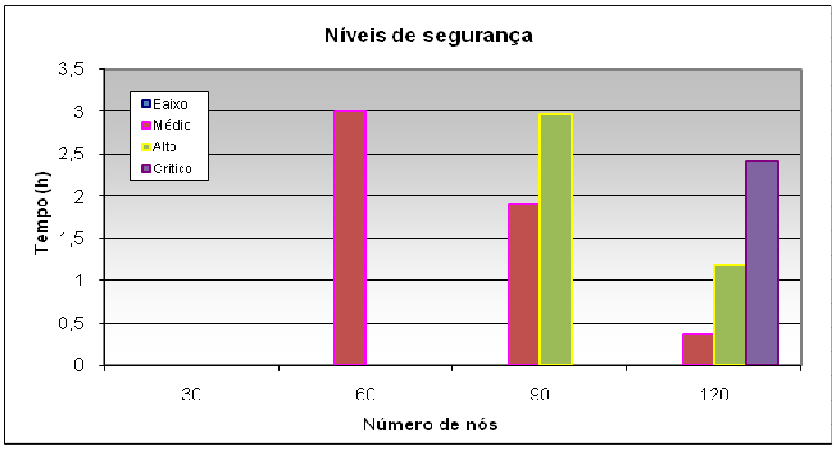

Figura 2 - Tempo para alcance dos níveis de segurança

Como todos os nós iniciam a simulação no nível de segurança Baixo, esse não aparece na Figura 2. Pode-se observar que houve alteração no nível de segurança apenas no segundo cenário, com 60 nós participando da rede. O nível Alto foi alcançado somente com 90 nós participantes e o nível Crítico com 120 nós.

A Figura 3 mostra que, apesar da conectividade imprevisível (DTN), 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.

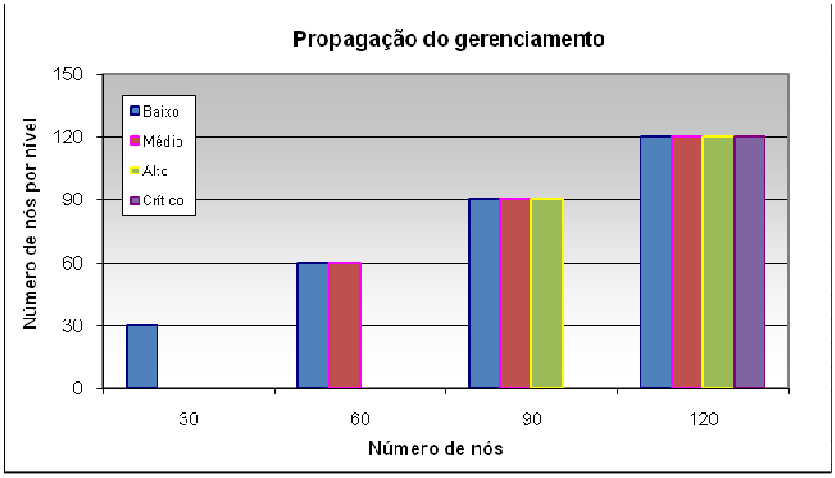

Figura 3 - Número de nós por nível de segurança ao fim de cada simulação

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 na quantidade de mensagens. Verificou-se que o número de mensagens de gerenciamento criadas é muito inferior em relação às demais mensagens da rede, atingindo o máximo de 3% no caso em que o nível Crítico é atingido.

Considerando o modelo 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.

Apesar das características DTN da rede de emergência, verificou-se que as mensagens de gerenciamento enviadas alcançam todos os nós participantes.

8. Conclusão e Trabalhos Futuros

Esse artigo apresenta um modelo de gerenciamento de segurança adaptativo para redes de emergência. O objetivo é evitar o efeito de ataques e economizar recursos ao ativar os componentes de segurança somente quando for necessário.

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. Um evento de detecção de intrusos gera decisão autonômica que altera o nível de 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 essas alcançam todos os nós participantes. É possível economizar recursos sem perca de produtividade da rede enquanto não há evidência de intrusos.

Como trabalhos futuros, propõe-se o estudo de soluções de segurança específicas para os protocolos de roteamento de redes DTN, bem como alterações de componentes do gerenciamento de acordo com o tipo de ataque detectado.

9. Referências

[1] Fall, K. (2004), "Messaging in difficult environments" – Intel Research Berkeley.

[2] Fall, K. (2003), "A Delay-Tolerant Network Architecture for Challenged Internets" – Intel Research Berkeley.

[3] Portmann, M. and Pirzada, A. A. (2008), "Wireless Mesh Networks for Public Safety and Crisis Management Applications" – IEEE Internet Computing.

[4] Burgess, J., Bissias, G., Corner, M. D., Levine, B. N. (2007), "Surviving Attacks on Disruption-Tolerant Networks without Authentication" – ACM Mobihoc.

[5] Seth, A. and Keshav, S. (2005), "Practical Security for Disconnected Nodes" – NPSEC.

[6] Symington, S. F., Farrell, S., Weiss, H. and Lovell, P. (2009), "Bundle Security Protocol Specification" – draft-irtf-dtnrg-bundle-security-08.txt.

[7] Durst, R. C. (2002), "An infrastructure security model for delay tolerant networks" – In http://www.dtnrg.org.

[8] Oliveira, S., Oliveira, T. R. and Nogueira, J. M. S. (2008), "Um Modelo de Gerenciamento de Segurança em Redes de Sensores Sem Fio" – In Simpósio Brasileiro de Redes de Computadores.

[9] Silva, F. A., Ruiz, L. B. et al. (2005), "MannaNMP: Um protocolo de Gerenciamento para Redes de Sensores Sem Fio" – In Simpósio Brasileiro de Redes de Computadores.

[10] Ekman, F., Keränen, A., Karvo, J. and Ott, J. (2008), "Working Day Movement Model" – In Proceeding of ACM SIGMOBILE workshop on Mobility models.

[11] Keranen, A. and Ott, J. (2007), "Increasing reality for DTN protocol simulations." Networking Laboratory, Helsinki University of Technology, Tech. Rep.

[12] Mota, V. F. S., Silva, T. H. and Nogueira, J. M. S. (2009), "Introduzindo Tolerância a Interrupção em Redes Ad Hoc Móveis para Cenários de Emergência" – In Simpósio Brasileiro de Redes de Computadores.