Certificados Sociais para Segurança em Redes Veiculares Tolerantes a Interrupções

Thiago R. Oliveira[1,2], Sérgio de Oliveira[2], Daniel F. Macedo[1], José Marcos S. Nogueira[1]

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

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

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

Abstract *– Disruption tolerant vehicular networks appear due to the search of information by drivers, which build mobile ad hoc networks that may suffer from long interruptions. This paper proposes a security model that employs self-signed certificates, enabling cars to share keys through direct contacts between two acquaintances, that warrant their identity, so they sign the reciprocal certificate. One certificate signed by a third party can be validated if its public key is available to the other party. Further, the reputation mechanism can still identify certificates of trusted users. The evaluation shows the behavior of a vehicular network that uses social certificates as a cryptographic security mechanism.*

Resumo *– Redes veiculares tolerantes a interrupções surgem pela busca de informações dos motoristas, que podem formar redes ad hoc móveis onde a comunicação pode sofrer longas interrupções. Este artigo propõe um modelo com certificados auto-assinados para possibilitar o compartilhamento de chaves entre duas pessoas que se conhecem e garantem sua identidade, que então assinam o certificado do outro pelo contato direto. Um certificado assinado por um terceiro pode ser validado se sua chave pública estiver disponível à outra parte. Um mecanismo de reputação ainda pode identificar certificados de usuários confiáveis. As avaliações realizadas mostram o comportamento de uma rede veicular com utilização de certificados sociais como mecanismos de segurança criptográficos.*

1. Introdução

Redes veiculares tolerantes a atrasos e interrupções visam disponibilizar novas tecnologias e aplicações, que podem tornar mais seguro o trânsito nas ruas e avenidas por meio de maior comunicação entre os usuários. Em regiões urbanas ou rodovias, geralmente não existe uma infraestrutura de rede ou a mesma não atinge áreas contíguas.

As redes veiculares são heterogêneas, aproveitando a infraestrutura existente nas cidades como as redes metropolitanas e os dispositivos dos próprios usuários, dada a popularização de dispositivos móveis como *notebooks*, *tablets* e *smartphones* com mais recursos disponíveis, que podem ser utilizados por motoristas e autoridades de trânsito. Alguns equipamentos podem estar conectados à Internet móvel, com cobertura em expansão nas áreas urbanas, o que pode fornecer diversas informações sobre o trânsito. Esse artigo aborda a questão de segurança para a meta de comunicação para aplicações

de Sistemas Inteligentes de Transporte do projeto (CIA)[2] da RNP, que envolve várias universidades federais por 2 anos com foco no desenvolvimento de cidades inteligentes.

Uma VANET (*Vehicle Ad Hoc NETworks*) é uma rede móvel *ad hoc* (MANET) [6] com algumas características importantes, como restrições a leis de circulação e vias específicas. Os veículos podem ter velocidades altas, a topologia da rede formada é bastante dinâmica e o conhecimento dos vizinhos alcançáveis pelo veículo muda com frequência. O tempo de contato entre os veículos pode não ser suficiente para estabelecer uma conexão e transferir dados, o que pode fragmentar a rede.

Redes veiculares são formadas por veículos e por equipamentos fixos localizados às margens das ruas e estradas, para permitir a comunicação entre veículos e de veículos com algum ponto de acesso como mostrado na Figura 1. Para tanto, deve-se considerar que as redes formadas por esses elementos possuem várias limitações, pois necessitam de certas condições que nem sempre são satisfeitas. Na comunicação entre veículos, a conectividade fim-a-fim é altamente suscetível à interrupção de comunicação.

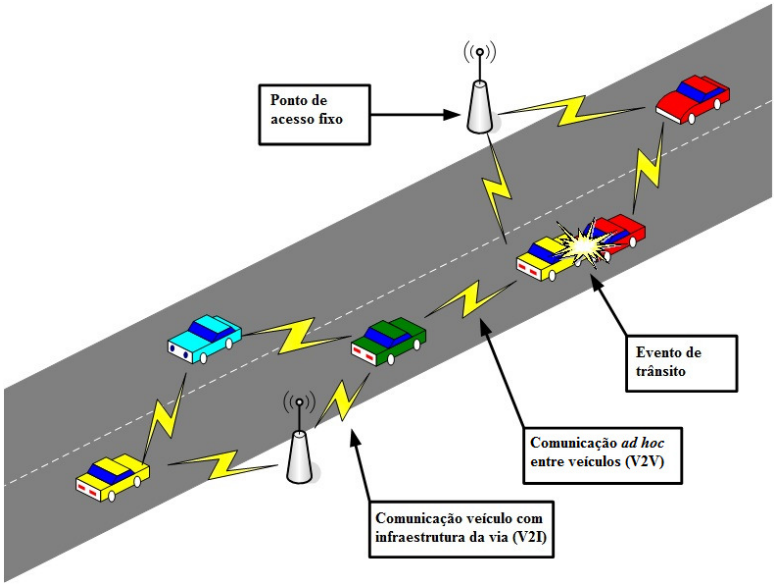

Figura 1 - Comunicação nas redes veiculares

Os dispositivos móveis podem ser utilizados pelos motoristas para obtenção e divulgação de informações, possibilitando alterar as rotas de trânsito utilizadas. Alguma empresa, por exemplo posto de combustível, pode tentar interferir nessas rotas. Nesse contexto, observa-se a necessidade de aumentar a segurança entre esses recursos de forma que troquem mensagens confiáveis, mesmo sem conexão no momento do envio.

A utilização da arquitetura de rede DTN (*Disruption Tolerant Networks*) [1] é necessária para se trabalhar em redes com conectividade intermitente ou com atrasos longos. Uma DTN utiliza um esquema de comunicação assíncrona e não há necessidade de um caminho fim-a-fim. 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.

A segurança torna-se mais desafiadora em redes DTN devido às suas características específicas, como mobilidade imprevisível e latência variável. É necessário eliminar mensagens expiradas e evitar vazamento de informações, devido à conectividade esporádica e grande possibilidade de atraso em transmissão de mensagens. Esses

aspectos devem ser considerados para utilizar redes veiculares tolerantes a interrupções com objetivo de incentivar a participação de todos os veículos em uma rede social.

É necessária uma alternativa que torne viável a autenticação das mensagens, pois o gerenciamento de chaves com tolerância a desconexões ainda é uma questão em aberto. O estabelecimento de chaves entre elementos da rede permite a autenticação no enlace. Na criptografia de chave pública, por exemplo, cada usuário tem um par de chaves privada e pública. Um esquema de distribuição de chaves seguro e eficiente possibilita a autenticação dos nós da rede. Entretanto, nenhum esquema de gerenciamento de chaves ainda é reconhecido como adequado para redes tolerantes a interrupções [6].

Um certificado é um arquivo, assinado digitalmente por uma autoridade certificadora confiável, confirmando a identidade do usuário e contendo uma cópia confirmada da chave pública do usuário. A certificação digital pode garantir alguns requisitos de segurança essenciais na rede. Um certificado auto-assinado ou assinado por um terceiro, não reconhecido como autoridade certificadora oficial [7], pode ser validado se sua chave pública estiver disponível à outra parte.

Este trabalho investiga o compartilhamento de chaves entre elementos da rede por meio do uso de certificados em redes veiculares tolerantes a interrupções, sendo tratadas como redes sociais. Propomos o uso de certificados sociais para troca de material criptográfico em relacionamentos cotidianos, como encontro com amigos ou ajuda a outro veículo, para estabelecer um grau de confiança entre os elementos da rede. Associado a esse material, pode-se utilizar um mecanismo de reputação de forma que os usuários beneficiados possam também emitir uma assinatura para o certificado de quem o ajudou. O princípio de reputação é uma recompensa para usuários que se comportam bem na divulgação de informações do trânsito e repassam informações verdadeiras.

O conteúdo deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados, enquanto a Seção 3 discorre sobre o modelo de rede. A Seção 4 define os mecanismos de segurança considerados para redes veiculares tolerantes a interrupções. O modelo de certificação proposto é descrito na Seção 5 e sua avaliação é apresentada na Seção 6. Na Seção 7, as conclusões e trabalhos futuros são apresentados.

2. Trabalhos Relacionados

Veículos que recebem informações de outros veículos ou entidades da rede precisam saber a confiabilidade de quem gerou aquela informação. O nível de privacidade pode ser ajustado pelo usuário, sendo ainda aberta a área de anonimicidade e privacidade adaptativa, onde usuários poderiam selecionar a privacidade que desejam ter [3]. Tais questões são abordadas neste trabalho tratando usuários numa rede social.

As redes veiculares possuem desafios específicos em relação à segurança [4]. Pouca atenção tem sido dedicada à segurança em redes veiculares, que é um desafio crucial e um elemento chave nesse aspecto é a confiança [5], devido ao grande número de nós independentes envolvidos e a presença de fatores humanos na rede que podem aumentar a tendência de mau comportamento. O conhecimento prévio existente entre os usuários da rede é utilizado para definir a confiabilidade deste trabalho.

A maioria das propostas para redes veiculares trata de problemas específicos, como a autenticação e a privacidade dos nós da rede. Um mecanismo de reputação para redes veiculares considerando tolerância a atrasos e desconexões é proposto em [7], mas assume que todos os veículos são certificados. Algumas propostas existentes descrevem

arquiteturas de segurança mais genéricas [9]. Este trabalho se diferencia por atender os vários requisitos de segurança das redes veiculares e pela tolerância a interrupções.

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. Um modelo para gerenciamento de segurança considerando aspectos das redes DTN foi proposto em [8]. Tais propostas não foram reconhecidas como soluções definitivas ou dependem da existência de alternativas para gerenciamento de chaves, como apresentado neste artigo.

Iniciativas existentes para redes veiculares são direcionadas para um ou outro cenário, muitas vezes restringindo o acesso ou sem considerar tolerância a interrupções. Tanto quanto podemos saber, não existe na literatura proposta para segurança em redes veiculares que viabilize a participação de todos os veículos com mecanismos de segurança implícitos, considerando as restrições de recursos dessas redes.

3. Modelo de rede e comunicação

Redes veiculares são heterogêneas em hardware, visto que devem estimular a participação de todos os motoristas através da utilização de seus *notebooks*, *palmtops*, *tablets* ou *smartphones*, com várias tecnologias de rede para comunicação entre esses 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. Nós podem participar ou deixar a rede dinamicamente.

Os nós da rede podem representar veículos, nós sensores para o monitoramento, pontos de acesso fixos nas vias para prover conexão externa aos veículos e servidores com pessoas qualificadas para controle do tráfego. Sensores e etiquetas RFID podem ser utilizados para monitoramento do trânsito e envio dessas informações. Os equipamentos podem estar limitados à comunicação *ad hoc* ou perderem conectividade com a rede metropolitana em alguns trechos das vias.

A característica de acesso eventual às redes metropolitanas pode ser usada para atualizar listas de usuários e chaves, mas não para garantir esses requisitos de segurança em tempo real. A comunicação *ad hoc* entre os veículos é motivada, pois não se pode considerar que há conexão constante com equipamentos de uma rede metropolitana sem fio (WMAN), disponibilizadas pelo poder público ou via redes celulares 3G/4G.

Dispositivos dos próprios usuários devem ser utilizados na rede veicular de forma que todos os motoristas possam participar sem a necessidade de adquirir novos equipamentos. A utilização do *smartphone* já adquirido causa maior incentivo que dispositivos novos embarcados no carro. Sempre que houver a tecnologia disponível, será utilizado o IEEE 802.11p que padroniza a comunicação em redes veiculares [4].

A comunicação entre os usuários pode ocorrer de forma direta, através de *Bluetooth* ou modo *ad hoc;* informações podem ser transmitidas para os pontos de acesso fixos e compartilhadas; além da sincronização de listas de usuários quando os equipamentos dos usuários estiverem diretamente ligados à Internet, na sua residência por exemplo.

Redes veiculares possibilitam uma variedade muito grande de configurações. A ampla diversidade de nós participantes, que vão desde nós sensores a robustos servidores de controle de tráfego, a mobilidade e as aplicações impedem que a caracterização do problema de provimento de segurança seja feita de forma única.

Objetiva-se neste trabalho propor soluções de segurança para redes veiculares sem hierarquia de nós e com formas de distinção entre as mensagens que devem ser consideradas para as decisões. Se uma informação afeta a rota utilizada pelo veículo no deslocamento, deve-se excluir a possibilidade do informante ser alguém diretamente interessado em rotas específicas, como um posto de combustível na via sugerida.

4. Mecanismos de Segurança para Redes Veiculares

Os dados enviados pelos motoristas devem ser tratados, de forma a garantir o anonimato e a privacidade dos usuários. Além disso, devem ser analisados para a detecção de informações maliciosas. Por exemplo, o dono de um posto anuncia que certa avenida está com um fluxo muito melhor que a realidade, pois quer aumentar a quantidade de carros que passam na região para aumentar o seu lucro, ou um usuário mal intencionado que quer provocar um engarrafamento em uma região da cidade.

Os requisitos de segurança em redes veiculares podem variar de acordo com as situações e cenários em que elas são utilizadas, um fator essencial considerado neste trabalho é a conectividade intermitente. A mobilidade presente nesse cenário se apresenta como um desafio fundamental para as redes veiculares, sendo necessário suportar recursos altamente variáveis dentro de curtos períodos de tempo, ou ainda atrasos de propagação extremamente longos.

Este trabalho propõe o roteamento com seleção de prioridade de pacotes para replicação, utilização de reputação e um mecanismo alternativo para substituição do gerenciamento de chaves; além de considerar a existência de mecanismos de detecção de intrusos, técnicas de criptografia e revogação de nós.

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

4.1. Roteamento prioritário

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. Portanto, é importante tratar o roteamento para garantir a segurança da rede.

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].

Decidiu-se utilizar nesse trabalho o protocolo *Spray and Wait* no modo binário, pois a melhor defesa em redes DTN contra ataques de perda maliciosa de pacotes é o uso de caminhos múltiplos. 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.

Propõe-se o uso de *flags* para definir replicação de maior prioridade como 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.

Tais *flags* auxiliam contra intrusos, que podem inundar continuamente a rede com envio de pacotes para qualquer nó e nunca repassarem qualquer pacote recebido de outros nós.

Permitir aos motoristas que expressem aspectos da importância das mensagens da rede pode ser um benefício considerável, tanto para os usuários quanto para a infraestrutura da rede que os suporta [1]. 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.

Esse trabalho considera que as aplicações que utilizam as redes veiculares devem obrigar a definição de prioridade das mensagens como: Baixa, Média, Alta ou Urgente. Mensagens definidas como urgentes possuem um tempo de vida determinado pela rede e inferior ao das demais, para descarte após término desse tempo.

4.2. Reputação

Quando um membro autenticado da rede atenta contra o funcionamento das aplicações, torna-se necessário o uso de mecanismos de segurança adicionais. Sistemas de reputação são utilizados para garantir o comportamento cooperativo em redes distribuídas como MANETs, VANETs ou redes *Peer-to-Peer* (P2P). [7]

Em VANETs, a reputação de um veículo pode ser considerada como um histórico sobre as informações repassadas aos outros veículos. Essa reputação é então utilizada como critério importante na tomada de decisões, tais como encaminhar ou descartar pacotes enviados por esse veículo, considerá-lo ou desconsiderá-lo como opção no roteamento de dados, considerar ou desconsiderar informações por ele repassadas, etc.

O princípio de reputação é uma recompensa para os usuários que se comportam bem na divulgação de informações do trânsito e repassam informações verdadeiras. Nesse trabalho, os veículos que divulgam informações úteis para outros veículos podem receber uma assinatura de bonificação em seu certificado por meio do mecanismo de reputação. Assim, é possível que outros usuários reconheçam-no como confiável segundo o mecanismo de reputação por meio de certificados proposto na seção 5.4.

4.3. Detecção de intrusos

Na presença de um intruso, 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 a rede. Assim, faz parte dos objetivos deste trabalho permitir que as redes veiculares mantenham bom funcionamento e sejam confiáveis, mesmo sob a ação de um ataque.

Mesmo para ataques para os quais já existam mecanismos de prevenção, a necessidade da detecção de intrusos ou abordagens complementares se justifica porque mesmo os métodos mais eficazes de prevenção podem falhar. O mecanismo de reputação proposto neste trabalho poderá atuar em conjunto aos mecanismos preventivos. A vantagem de técnicas descentralizadas é a disponibilidade instantânea da informação, visto que os nós podem detectar intrusos no momento da comunicação.

4.4. 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, o mecanismo de reputação pode encaminhar implicitamente 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.

4.5. Técnicas criptográficas

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.

Para redes tolerantes a interrupções, 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. A alternativa é usá-los a cada passo do roteamento. Nesse caso, é necessário um compartilhamento de chaves entre os vários nós que precisam se comunicar diretamente para a execução do roteamento, conforme a proposta desse trabalho descrita na seção 5.2.

4.5.1. Encriptação

A criptografia pode ser utilizada em redes veiculares para garantir maior confiabilidade na comunicação, através de verificação de integridade ou autenticação de origem e destinatário das mensagens. A encriptação pode ser um processo salto-a-salto, feito cada vez que uma mensagem atinge um nó de repasse.

Um dos objetivos desse trabalho ocorre do fato que 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.

4.5.2. Assinatura digital

Assinatura é um processo criptográfico que adiciona um código autenticado com uma chave a uma mensagem e o recebedor tem que conhecer a chave para verificar a assinatura. Em redes DTN, as chaves devem ser 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 [14].

4.5.3. 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.

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]. Este trabalho propõe um mecanismo alternativo para compartilhamento de chaves, por meio da utilização de certificados assinados pelo próprio usuário e quem confia nele.

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 [13]. 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.

4.5.4. Criptografia baseada na identidade

Como uma área recente de pesquisa, os mecanismos que utilizam criptografia baseada na identidade [11] fornecem muitos dos benefícios da criptografia de chave pública e reduzem a sobrecarga envolvida 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 menor para segurança da rede.

Pode-se utilizar criptografia de chave pública como o ponto de partida para o estabelecimento 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.

5. Modelo de Certificação Social

O modelo de certificação social, apresentado a seguir, objetiva prover comunicação segura para troca de informações entre os veículos e com as entidades responsáveis por organizar o trânsito. Os principais requisitos de segurança se interrelacionam, visto que dizem respeito à identidade de quem envia as informações, que não deve ser conhecida (anonimicidade), mas é preciso ser verificada e deve ter sua reputação computada. Ao receber informação de algum outro veículo, é importante saber se essa informação tem uma origem reconhecida, e caracterizar sua reputação como positiva ou negativa.

Em toda troca de mensagens na rede veicular, deve ser manifestado o interesse dos outros motoristas nas informações por meio de *flags* para indicar replicação de maior prioridade. Essa adequação, proposta na seção 4.1 deste trabalho, visa complementar o protocolo de roteamento *Spray and Wait* no modo binário, pois a replicação de mensagens no roteamento aumenta consideravelmente a tolerância a ataques.

5.1. Certificação Digital

A certificação digital pode garantir alguns requisitos de segurança essenciais na rede. Neste trabalho, no entanto, considera-se que a sua presença estará restrita a parte dos usuários, devido aos seus custos de implantação e manutenção. Pelo certificado, os usuários podem ter a garantia de acessar os sistemas corretos, de forma autêntica e privada.

O modelo deste trabalho visa aumentar a abrangência do acesso, especialmente em regiões sem cobertura da rede metropolitana, como em rodovias, não restringindo o acesso a nós autenticados por uma autoridade certificadora. Se a comunicação à rede metropolitana pudesse ser garantida em todo o tempo de operação da rede, os problemas de segurança seriam minimizados pelo uso dos certificados digitais dos servidores, e se restringiriam à manutenção das senhas e proteção dos sistemas contra invasões.

5.2. Certificados Assinados por Amigos

É necessário considerar alternativas para que os veículos consigam estabelecer os requisitos de segurança necessários, pois as redes veiculares não podem contar com acesso aos servidores de autenticação e os elementos da rede não possuirão certificados válidos, devido aos custos dos mesmos. A troca de material criptográfico deve ser feita de forma segura, por entrega direta sem uso da rede, ou de forma a garantir os requisitos básicos de segurança. Como os veículos não são certificados e não dispõem de nenhum material criptográfico inicial, não é possível garantir seus requisitos de segurança.

O problema deste trabalho pode ser abordado como uma rede complexa, adotando o modelo *"Small World"* para modelar redes veiculares como redes sociais. O modelo é apresentado como intermediário entre um grafo regular e um grafo aleatório [10].

A troca de material criptográfico de forma direta será usada para iniciar o estabelecimento dos requisitos de segurança. O funcionamento se baseia nos contatos diretos entre dois veículos, por exemplo, estacionados lado a lado ou em uma garagem. Os usuários num mesmo ambiente podem parear seus equipamentos por *Bluetooth*. Para garantir que não existe um intruso nessa comunicação, é possível estabelecer uma senha temporária que pode ser digitada por ambos os motoristas nesse contato inicial.

Esse contato direto entre amigos, definidos como duas pessoas que se conhecem e garantem sua identidade, possibilita que um assine o certificado do outro. Assinar o certificado do outro e compartilhar com ele sua chave pública possibilita uma rede de relacionamento na qual todos os veículos que possuam amigos em comum consigam validar os certificados usando as chaves do amigo. Como conhecem a chave pública do amigo, a utilizam para verificar a assinatura emitida pelo amigo para outro certificado.

Um certificado assinado por um terceiro, que não seja reconhecido como autoridade certificadora oficial, pode ser considerado válido se sua chave pública estiver disponível à outra parte. Assim, os veículos poderão validar todos os certificados assinados pelas chaves que eles conhecem. Como podem conhecer milhares de chaves, aumenta a probabilidade de encontrar uma chave em comum com os outros veículos.

5.3. Certificados Assinados por Amigos de Amigos

O princípio da assinatura por amigo de amigos é estender ao máximo as assinaturas sobre um certificado, incluindo assinaturas de amigos e certificados de reputação, para que os elementos de rede confiáveis possam ser diferenciados. As assinaturas de amigos podem ser estendidas também para os "amigos dos amigos", como em uma rede social. Isso ampliaria a possibilidade de compartilhamento de material criptográfico de dois veículos quaisquer que se encontrassem eventualmente no trânsito.

O funcionamento, baseado no PGP (*Pretty Good Privacy*)[1], ocorre seguinte forma:

1. O veículo gera um certificado auto-assinado;

[1] http://www.rnp.br/cais/keyserver/

2. O certificado pode ser assinado pelos amigos em contatos diretos, como em emparelhamento direto *Bluetooth*. Ao se aproximar do equipamento de um amigo, a geração das assinaturas dos certificados seria iniciada, por meio do compartilhamento de uma senha gerada no momento e trocada entre os amigos;

3. O certificado, assinado pelos amigos, pode ser compartilhado quando os dispositivos estiverem diretamente conectados à Internet, na sua residência por exemplo. Os amigos dos amigos reconheceriam o certificado, assinado por um amigo, e também o assinariam, compartilhando a convicção do amigo de que é um certificado confiável.

4. O veículo armazena as assinaturas de todos os amigos e amigos dos amigos, com as chaves públicas de todos. As assinaturas são usadas para validar a sua chave pública e as chaves dos amigos armazenadas para validar as chaves públicas dos demais.

5. Ao encontrar um veículo, a comunicação se inicia pela pesquisa de um amigo, ou amigo de amigo, conhecido. A identificação de um amigo em comum permite que os dois confirmem suas identidades pelas assinaturas e chaves públicas disponíveis.

6. Caso não esteja disponível a assinatura de alguém de sua rede social, é possível buscar uma assinatura conhecida originada por reputação. Essa assinatura poderá ser reconhecida se o emissor estiver na rede social de quem verifica o certificado. A reputação pode aumentar as chances de reconhecer o veículo informante, indicando que alguém da sua rede social foi beneficiado por esse veículo e reconheceu sua ajuda.

5.4. Reputação Certificada

Um mecanismo de reputação também é usado para validar o processo e confirmar que os usuários estão agindo em benefício da rede. A reputação terá efeito semelhante às assinaturas dos certificados, diferenciando apenas pelo indicativo do certificado de bonificação, emitidos pelos beneficiados por informações repassadas. Um certificado pode acumular várias assinaturas indicando sua reputação e será considerado se as recomendações positivas forem maior número que indicações negativas.

Por exemplo, um veículo que identifica um acidente e manifesta essa informação para rede, poderá receber uma bonificação de reputação positiva, se sua informação for útil a um terceiro. A bonificação será assinada com o certificado do veículo beneficiado com a informação. Todos os usuários que tiverem acesso à chave pública desse veículo serão capazes de confirmar a bonificação e reconhecer o veículo informante na rede.

A bonificação é mais uma possibilidade de reconhecimento do veículo pelos demais. Nesse caso, ele terá uma bonificação assinada que indica que alguém deu crédito à sua indicação e isso lhe foi útil. Se o veículo que deseja verificar as credenciais do outro é amigo, ou "amigo de amigo" do veículo que atribuiu a bonificação em questão, ele será capaz de identificar a validade da bonificação por meio do certificado.

5.5. Assinaturas Válidas

Este trabalho propõe três tipos de assinaturas emitidas para os certificados dos usuários que podem os credenciar para garantir a segurança em uma comunicação: assinaturas dos amigos, assinaturas dos amigos dos amigos e assinaturas de reputação. As assinaturas dos amigos são obtidas por contato direto e, por isso, implicam em uma relação próxima de conhecimento. Assinaturas de amigos dos amigos são obtidas por meio de interações em redes públicas como a Internet, sempre assinadas com os certificados dos respectivos amigos em comum.

De forma complementar, pode ser considerado o certificado de reputação que foi emitido por um desconhecido, caso tenha alguma intersecção em sua rede social e tenha sido beneficiado pela ação do veículo certificado com bonificação positiva.

Todo o processo deve ocorrer de forma rápida. Considerando uma centena de amigos, os "amigos dos amigos" poderiam contar com até 10.000 pessoas, porém como sempre existem amigos em comum, esse número tende a cair [10]. Usando mecanismos de chave pública curtas como logaritmo discreto ou curva elíptica, seria possível armazenar todas as chaves em alguns megabytes. Resumos das chaves de 20 bits poderiam ser usados para localizar chaves em comum. Esse processo deve ser rápido e encontrar as chaves em comum, então os certificados são validados com essas chaves.

6. Avaliação

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

Para validar o modelo de certificação aqui apresentado, um conjunto de simulações foi realizado para verificar o comportamento da rede, em função do número de elementos da rede e do número médio de elementos diretamente alcançáveis. O objetivo é mostrar o comportamento da rede veicular com utilização dos certificados auto-assinados, à medida que os motoristas passam a participar e serem autenticados pelos outros usuários, considerando os aspectos da tolerância a interrupções.

Como se espera uma grande variedade de usuários participando das redes veiculares, as simulações consideraram uma rede móvel e heterogênea, com o número total de nós variando entre 150 e 600 nós. Os nós são distribuídos pela rede de forma aleatória e deslocam-se de acordo com probabilidades definidas entre as regiões de um cenário urbano. Os pontos de interesse foram definidos como regiões centro, universidade e bairros. Os nós se deslocam entre as regiões pelas vias de uma cidade, como pode ser visualizado na Figura 2.

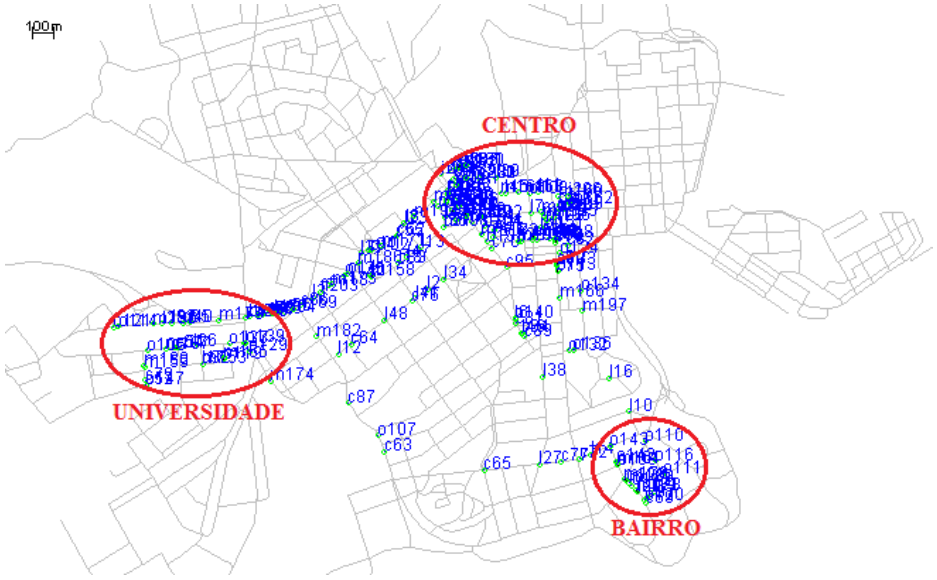

Figura 2 - Cenário das simulações

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*" [15], 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.

Os nós se movimentam através da região abrangida pela rede, que possui tamanho de 4500 x 3400 metros, no entanto há pontos sem conectividade nessa área. Somente existe conexão *ad hoc* entre quaisquer dois nós quando ambos estão dentro do respectivo raio de transmissão. Considerando o padrão IEEE 802.11p [4] para redes veiculares, esse raio foi definido como 100m para cada nó, enquanto a velocidade de transmissão dos dados foi 250kbps e o buffer de mensagens 10MB para cada nó.

Para considerar as características DTN da rede veicular, utilizou-se o simulador The ONE (*Opportunistic Networking Evaluator*) [16], que mantém as mensagens em um *buffer* caso o nó não tenha conexão direta com o destino. Mensagens são geradas por algum nó da rede em intervalos curtos, a cada 30-45 segundos, e os períodos observados para avaliação foram simulações de 24 horas. Cada teste foi executado repetidamente, no mínimo oito vezes, sendo alterada a semente geradora do padrão de mobilidade.

Inicialmente, foi verificado o impacto da utilização do modelo de certificação social proposto na rede por meio do número médio de nós considerados confiáveis, ou seja, amigos ou amigos dos amigos. Logo após, foi analisado o comportamento da rede veicular à medida que os motoristas passam a participar e as mensagens serem autenticadas pelos outros usuários, considerando os aspectos da tolerância a interrupções. Os resultados são apresentados nos gráficos a seguir.

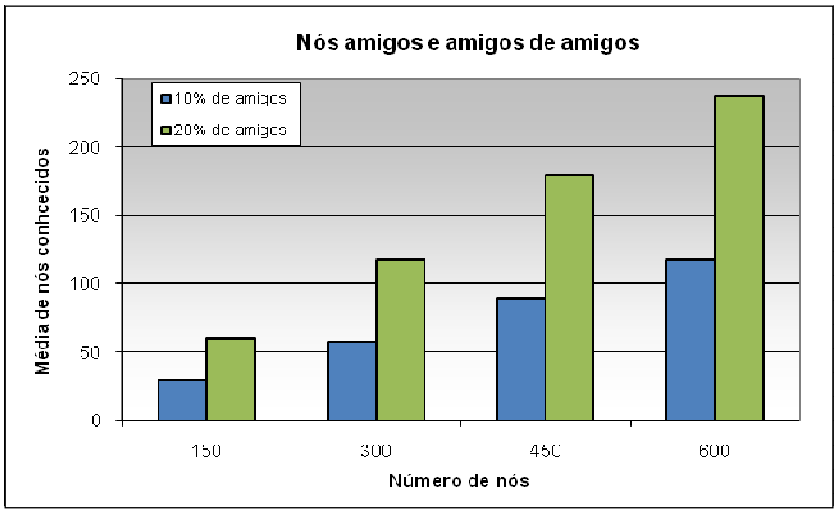

Figura 3 - Número médio de nós conhecidos

Na Figura 3, o percentual de amigos que cada nó da rede veicular possui foi estimado em 10 e 20% dos nós da rede. Pode-se observar que o percentual estipulado como número de amigos na simulação interfere diretamente na média de nós conhecidos, que considera também os amigos dos nós amigos. À medida que o número de nós da rede aumenta, há um incremento significativo na média de nós conhecidos pelos nós da rede, pois o maior número de amigos agrega outros usuários confiáveis.

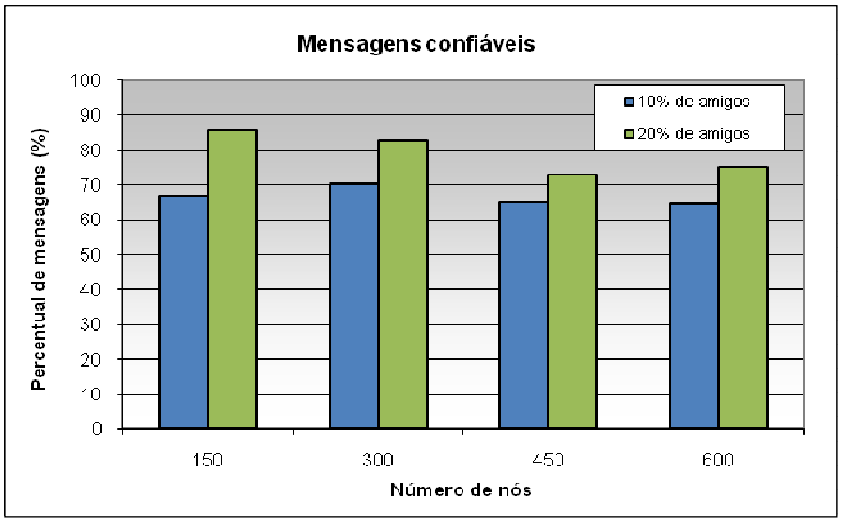

Figura 4 - Percentual de mensagens confiáveis das recebidas

A Figura 4 mostra o impacto da utilização dos certificados sociais como critério na seleção de mensagens confiáveis pelos usuários da rede veicular, considerando a conectividade imprevisível (DTN) e o número de mensagens recebidas pelos nós da rede. Com intervalo de confiança de 90%, o percentual de mensagens confiáveis em todos cenários analisados foi superior a 60%, atingindo mais de 85% em relação às mensagens entregues no cenário com 150 nós e 20% de amigos.

Apesar das características DTN da rede veicular, as mensagens recebidas pelos nós participantes foram analisadas para decidir sobre sua confiabilidade. A alteração do percentual de amigos de cada nó de 10 para 20% dos nós da rede representou até aproximadamente 20% de acréscimo no número de mensagens consideradas confiáveis, por serem enviadas por amigos do usuário ou amigos desses amigos.

Foi possível verificar nas simulações que a utilização do modelo de certificação social resulta em vantagens independente do número de nós da rede, pois representa maior segurança para os nós em relação à confiabilidade da rede. O número de mensagens entregues diminui, pois se restringe aos nós confiáveis. Como inicialmente não existiam chaves para autenticação das mensagens, o mecanismo proposto representa uma alternativa ao gerenciamento de chaves baseando-se numa rede social.

7. Conclusão e Trabalhos Futuros

Esse artigo apresenta um modelo de certificação social com foco na segurança de redes veiculares tolerantes a interrupções. Objetiva-se comunicação segura para troca de informações entre os veículos e com as entidades responsáveis por organizar o trânsito.

A proposta parte do relacionamento e conhecimento prévio dos usuários para estabelecer um grau de confiança em uma rede social. A utilização de certificados auto-assinados pelos motoristas possibilita o compartilhamento de chaves através de contato direto, entre duas pessoas que se conhecem e garantem sua identidade, que então assinam o certificado do outro mutuamente. Os certificados podem ser considerados válidos por outros usuários que tenham a chave pública da assinatura disponível.

Além disso, o mecanismo de reputação possibilita também que usuários beneficiados possam emitir uma assinatura com bonificação positiva para identificar o outro certificado como um elemento de rede confiável.

Como trabalhos futuros, propõe-se a avaliação do mecanismo de reputação proposto, bem como alterações do modelo de certificação proposto de acordo com a configuração inicial e possível integração com outras redes sociais como o Facebook.

Agradecimento: Este trabalho contou com recursos da RNP (http://www.rnp.br).

8. 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] Karagiannis, G., Altintas, O. et al. (2011). "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions" – IEEE Communications Surveys & Tutorials.

[4] Alves, R. S., Campbell, I. V. et al. (2009). "Redes Veiculares: Princípios, Aplicações e Desafios." Minicursos do Simpósio Brasileiro de Redes de Computadores, pp. 199-254.

[5] Raya, M. and Hubaux, J. P. (2005). "The Security of Vehicular Ad Hoc Networks." In Proceedings of ACM Workshop on Security of ad hoc and sensor networks.

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

[7] Paula, W. P.; Oliveira, S. and Nogueira, J. M. S. (2010). "Um Mecanismo de Reputação para Redes Veiculares Tolerantes a Atrasos e Desconexões." Simpósio Brasileiro de Redes de Computadores.

[8] Oliveira, T. R., Oliveira, S. and Nogueira, J. M. S. (2010), "Modelo de Gerenciamento de Segurança Adaptativo para Redes de Emergência" – In Simpósio Brasileiro de Redes de Computadores.

[9] Papadimitratos, P., Buttyan, L. et al. (2008). Secure vehicular communication systems: design and architecture. IEEE Wireless Communications Magazine, Vol. 46, No. 11, pp. 100–109.

[10] Gakenheimer, R. (1999). "Urban mobility in the developing world." Transportation Research Part A: Policy and Practice, vol. 33, no. 7-8, pp. 671-689.

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

[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.

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

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

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

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