Um Mecanismo de Reputação para Redes Veiculares Tolerantes a Atrasos e Desconexões

Wellington Passos de Paula[1], **Sérgio de Oliveira**[2], **José Marcos Nogueira**[1]

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

[2]Universidade Federal de São João Del Rei (UFSJ)
Campus Alto Paraopeba, Ouro Branco, MG – Brasil

{wpassos,jmarcos}@dcc.ufmg.br, sergiool@ufsj.edu.br

Abstract. *Among the proposed applications for Vehicular Ad Hoc Networks (VANETs), we can stick out applications in which network members can exchange information about the traffic conditions and the occurrence of risk events in the roads. In those scenes, the use of wrong information in the decision process executed by the vehicles can cause serious accidents. Therefore, is necessary the development of solutions capable to incentive cooperative behaviors' and punish the malicious ones. This work presents a reputation mechanism for VANETs, called RMDTV. Through this mechanism, network members emit qualifications to other members responsible for sending correct information. These qualifications are added to all generated messages by their carriers in intention of attesting their reliability. Simulations show that RMDTV increases the quality of taken decisions by members of a VANET, even with the presence of a great amount of malicious nodes.*

Resumo. *Dentre as aplicações propostas para as Redes Ad Hoc Veiculares (VANETs), destacam-se aquelas nas quais membros da rede trocam mensagens sobre as condições de tráfego e a ocorrência de eventos de risco nas vias. Nesses cenários, o uso de informações erradas nos processos de decisão executados pelos veículos pode causar graves acidentes. Logo, torna-se necessário o desenvolvimento de soluções capazes de incentivar comportamentos cooperativos e punir os maliciosos. Este trabalho apresenta um mecanismo de reputação para VANETs, denominado RMDTV, no qual membros da rede emitem qualificações a outros membros responsáveis pelo envio de informações corretas. Essas qualificações são adicionadas por seus portadores a todas as mensagens geradas, no intuito de atestar sua confiabilidade. Simulações mostram que o RMDTV aumenta a qualidade das decisões tomadas pelos membros de uma VANET, mesmo com a presença de muitos nós maliciosos.*

1. Introdução

Como um tipo especial de rede *ad hoc* móvel (*Mobile Ad Hoc Network* - MANET), as redes *ad hoc* veiculares (*Vehicular Ad Hoc Networks* - VANETs) têm sido foco de muitos estudos, devido aos seus desafios e às suas inúmeras aplicações, como por exemplo, a troca de mensagens informando condições de tráfego ou outras situações de risco possivelmente existentes na via de deslocamento.

Embora em VANETs sejam empregados dispositivos mais poderosos que aqueles normalmente utilizados nas MANETs, os quais possuem grande capacidade de comunicação e, geralmente, energia ilimitada, membros de VANETs podem ser submetidos a momentos de desconexão total, ocasionados, por exemplo, pela alta mobilidade dos componentes da rede ou mesmo pelas variações do meio físico sem fio. Assim, soluções propostas para essas redes precisam considerar a existência dessas situações.

O conceito de redes tolerantes a atrasos e desconexões (*Delay and Disruption Tolerant Networks* - DTN's) [Fall 2003] surge então como uma solução para possibilitar a comunicação em cenários nos quais a conectividade entre os membros é intermitente ou existem grandes atrasos. Nas DTNs o nó deve armazenar as mensagens recebidas até que seja possível encaminhá-las a outro nó na rede. Tal modelo de comunicação, chamado de armazenagem-e-repasse, é implementado nessas redes a partir da criação de uma nova camada sobre a pilha definida pelo modelo OSI, a camada de agregação (*bundle*).

Além de considerar possíveis momentos de desconexão, outro fator crítico para o sucesso de aplicações em VANETs é o comportamento dos nós da rede. Nesses cenários, nos quais nós trocam informações entre si, existe sempre o risco de algum dos participantes da rede agir de modo egoísta, ou seja, condicionar seu comportamento de acordo com seus interesses pessoais, em detrimento do interesse geral.

Logo, visando minimizar as consequências de comportamentos maliciosos e consequentemente, aumentar a segurança das VANETs, tornam-se necessárias soluções que motivem a cooperação e honestidade dos nós que as compõem. Mecanismos de reputação contribuem com esse objetivo na medida em que permitem aos nós decidir em quem confiar antes mesmo do início da troca de dados. Esses sistemas assumem que o comportamento antigo de um membro da rede indica de forma bem confiável suas ações futuras.

Porém, em VANETs, a alta mobilidade dos elementos de rede, movendo-se a grandes velocidades, diminui muito as oportunidades de conexão experimentadas por esses membros. Assim, tais oportunidades devem ser usadas, majoritariamente, para a troca de dados, o que dificulta a troca de informações de reputação. Logo, a melhor maneira de definir a reputação de um membro seria ele próprio guardar seus dados de reputação.

Neste trabalho é proposto um mecanismo de reputação que faz uso de qualificações emitidas por terceiros. Dessa maneira, toda vez que um nó tem uma experiência de comunicação positiva com outro nó, uma qualificação é emitida e assinada pelo primeiro. Tal qualificação é encaminhada pela rede, mesmo sob condições de desconectividade, até encontrar seu destino. As qualificações recebidas são adicionadas por seus portares às mensagens por eles geradas, no intuito de atestar sua confiabilidade.

O objetivo deste trabalho é a proposição e análise de um mecanismo de reputação que permita aos membros da rede atestar previamente a confiabilidade de novos vizinhos, antes mesmo da realização de uma transação. As principais contribuições do trabalho estão sumarizadas a seguir:

- Concepção de um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões, o qual denominamos Reputation Mechanism for Delay Tolerant Vehicular Networks (RMDTV), que permite aos membros de rede tomar decisões sobre eventos existentes na via, com base nas mensagens recebidas informando as condições dos referidos eventos, de forma mais segura;

- Implementação do mecanismo proposto utilizando o simulador *Opportunistic Network Environment* - (ONE) [Keränen et al. 2009], que permite simular redes nas quais a conectividade é intermitente;

- Avaliação do desempenho do mecanismo proposto quando exposto a diferentes quantidades de intrusos.

Este trabalho está organizado como se segue: na Seção 2 definimos as Aplicações de Mensagem de Perigo Local, um tipo de aplicação de troca de mensagens em VANETs. Nosso mecanismo de reputação é apresentado na Seção 3. Na Seção 4 fazemos uma análise do desempenho do mecanismo proposto quando exposto a diferentes quantidades de intrusos. A Seção 5 apresenta uma revisão da literatura sobre reputação em VANETs. Por fim, concluímos e apresentamos propostas para trabalhos futuros na Seção 6.

2. Aplicação de Mensagem de Perigo Local

Em uma Aplicação de Mensagem de Perigo Local (*Local Danger Warning Application* - LDW) [Kosch 2004], eventos de risco detectados pelos veículos geram mensagens de aviso que são disseminadas pela rede em modo de difusão (*broadcast*). A cada evento detectado é gerada uma nova mensagem informando sua condição. Cada receptor desses dados atua como roteador da mensagem, aumentando assim o alcance deste aviso. Além disso, o aplicativo LDW avalia o conteúdo das mensagens recebidas. Toda vez que esse aplicativo considerar suficiente as evidências de um evento, ele fará uso da interface com o motorista para comunicá-lo da existência do problema, de forma que este motorista possa reagir àquela situação da maneira mais segura possível.

Em aplicações LDW, as mensagens geradas não devem ser encaminhadas continuamente, já que, a partir de certa distância, o evento passa a ser irrelevante para os receptores. Assim, de forma a controlar a detecção de eventos, a distribuição de mensagens e o processo de tomada de decisões, [Dotzer et al. 2005] definem que cada evento existente na rede é circundado por três regiões geográficas (Figura 1).

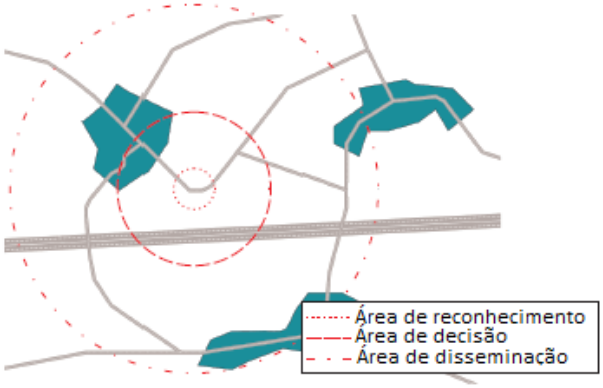

Figura 1. Áreas geográficas de um evento [Ostermaier et al. 2007].

A área mais externa é identificada como *área de disseminação*. Ao entrar nessa região, os veículos começam o processo de coleta e repasse das informações recebidas

sobre o evento. Ao atingir a área intermediária, chamada de *área de decisão*, o veículo determina se alguma ação deve ser tomada acerca das informações recebidas sobre determinado evento. A área central, *área de reconhecimento*, é caracterizada por ser a única região onde um veículo é capaz de detectar, através da leitura de seus sensores locais, a presença de um evento na via, ou seja, somente veículos nessa área podem criar novas mensagens informando a ocorrência de eventos. De maneira análoga, veículos que detectam a extinção de um evento anteriormente anunciado, ao adentrarem em sua área de reconhecimento, geram uma mensagem revogando a sua existência.

Neste trabalho as regiões geográficas assumiram formas circulares. Entretanto tais regiões podem ser adaptadas de acordo com o formato das vias.

3. O Mecanismo de Reputação RMDTV

Para cada mensagem recebida pelo veículo dentro da área de disseminação do evento, com informações sobre seu estado atual, é feita uma avaliação da confiabilidade dos dados, a partir da reputação de sua origem. No Reputation Mechanism for Delay Tolerant Vehicular Networks (RMDTV) cada veículo armazena localmente duas listas contendo, respectivamente, os membros da rede considerados confiáveis e aqueles considerados maliciosos. Assim, o emissor dos dados é classificado em uma das seguintes categorias: *malicioso*, *confiável* ou *desconhecido*.

Se o emissor é considerado malicioso, a mensagem é simplesmente descartada. Se os dados forem originários de uma fonte tida como confiável ou desconhecida, a mensagem é repassada ao mecanismo de decisão, descrito na Subseção 3.1. As mensagens repassadas ao mecanismo de decisão, ou seja, consideradas relevantes pela aplicação, são retransmitidas em modo de difusão (*broadcast*). Essa redistribuição ocorre continuamente enquanto o receptor estiver dentro da área de disseminação do evento e a mensagem não exceder seu tempo de vida (*timeout*). Assim, mensagens geradas por veículos que já deixaram a área de disseminação ainda podem ser utilizadas por outros carros.

Uma vez que os requisitos do processo de decisão sejam atendidos e a decisão tomada, o veículo atualiza os valores de reputação dos nós responsáveis pelas mensagens utilizadas nessa decisão. Todavia, como veremos na Subseção 3.1, em alguns casos o veículo não recebe evidências suficientes da ocorrência ou revogação do evento, de forma que a decisão tomada não é baseada nos dados recebidos. Nessas situações, não é realizada nenhuma alteração nos valores de reputação das origens dos dados recebidos. Para as demais, os passos executados são descritos abaixo.

Independentemente da qualidade da decisão tomada, veículos cujas mensagens informaram o evento corretamente sempre são promovidos a confiáveis. Por outro lado, veículos cujas mensagens informaram o evento incorretamente são punidos (passam a ser considerados maliciosos), somente quando o ataque executado obteve sucesso, ou seja, as informações por eles geradas foram relevantes o suficiente para levar o receptor a uma decisão incorreta. Caso contrário, continuarão a ser considerados desconhecidos quando suas mensagens forem submetidas novamente ao mecanismo de reputação. Com essa estratégia objetivamos atingir um número menor de falsos positivos, já que existe o risco de mensagens geradas por veículos cooperativos, mas recebidas com atraso, informarem uma condição diferente do estado atual do evento. Como nós considerados maliciosos têm suas mensagens descartadas, o desempenho do RMDTV pode ficar dependente do

tempo de redenção definido pela rede.

Apenas os dados de reputação da origem das mensagens são alterados, uma vez que muitas das vezes as mensagens recebidas foram repassadas por veículos que não trafegaram pela área de reconhecimento do evento, mas confiaram no relato de outros nós. De forma a impossibilitar ataques de adulteração de dados, o RMDTV faz uso de um mecanismo de criptografia de chave pública, descrito na Subseção 3.2.

As listas de confiabilidade de cada veículo nunca são publicadas. O compartilhamento de opiniões é feito a partir de um procedimento similar ao *Pretty Good Privacy* - PGP [Zimmermann 1994], no qual um membro da rede, após se comportar de maneira satisfatória em uma transação, recebe e armazena um certificado, assinado digitalmente por seu par, atestando sua confiabilidade. Os certificados recebidos são apresentados aos novos pares em futuras transações, funcionando como as "credenciais" de seu portador. Assim, para cada veículo promovido a confiável, o receptor gera e envia uma qualificação atestando a confiabilidade daquele membro da rede. Dados os problemas de desconexões existentes nas VANETs, uma qualificação pode demorar horas, ou até mesmo dias para chegar ao seu destino. Assim, a aplicação do modelo armazenagem-e-repasse, utilizado pelas redes DTN para o encaminhamento de mensagens, surge como uma solução aos possíveis atrasos existentes durante o roteamento de qualificações.

As qualificações recebidas por um veículo devem ser adicionadas às mensagens de dados por ele geradas. Veremos na Subseção 3.1 que essas qualificações anexadas têm pesos diferenciados no mecanismo de decisão executado pelo receptor das informações. Para evitar uma sobrecarga muito grande na rede, apenas um determinado número de qualificações deve ser adicionado.

A fim de potencializar o compartilhamento de opiniões, veículos que transitaram pela área de reconhecimento de um evento qualificam também outros nós responsáveis por mensagens que corroboram com as impressões por eles experimentadas. Como apenas opiniões positivas são disseminadas, não existe a possibilidade de ataques ao RMDTV nos quais nós maliciosos objetivam denegrir a imagem de veículos cooperativos.

3.1. Processo de Decisão

A tomada de decisão sobre um evento pode acontecer em dois momentos distintos. No primeiro, durante a fase de coleta de dados, o veículo recebe uma mensagem originária de uma fonte considerada confiável. Neste caso, as informações recebidas são consideradas evidência suficiente da existência ou revogação do evento e a decisão é baseada apenas nesses dados. O segundo momento acontece quando o veículo atinge a área de decisão daquele evento sem receber mensagens geradas por fontes confiáveis. Nesta situação, a decisão deve ser tomada imediatamente após a entrada na área de decisão do evento, a partir do uso das mensagens cujas fontes são consideradas desconhecidas pelo veículo.

Neste trabalho, o método de decisão utilizado foi o *Maioria das últimas x mensagens considerando um limite inferior*, definido em [Ostermaier et al. 2007]. Nele, o veículo utiliza apenas as últimas x mensagens recebidas com informações sobre o evento. Entretanto, existe também um limite inferior, de forma que o mecanismo de votação só é utilizado caso o nó receba ao menos um determinado número de mensagens. Quando esse mínimo de opiniões não é atingido, o veículo sempre se decide pela negação do evento. Essa opção é justificada pelas possíveis conseqüências resultantes de decisões

falso negativas e *falso positivas*. Enquanto nas primeiras o veículo normalmente não altera sua velocidade ou rota, nas segundas o motorista pode acabar reduzindo a velocidade do veículo (por exemplo, em situações de proximidade a um acidente), o que aumenta o risco de colisões caso algum dos próximos veículos da via, possuindo quantidade de dados suficiente para executar o processo de decisão, se decida pela inexistência do evento.

A partir das situações descritas, nomeamos as decisões tomadas por um veículo como *decisões indicadas* e *decisões forçadas*. Enquanto as primeiras são resultado da execução do mecanismo de votação, as segundas ocorrem quando o veículo não recebe o número mínimo de mensagens para a execução deste mecanismo.

Algoritmo 1: Algoritmo de tomada de decisão

Entrada: Conjunto M de Mensagens com dados sobre o Evento E
//inicialização de variáveis
for M_0 **to** M_{max} **do**
    if M_i *informou a existência de* E **then**
        $votosExistenciaEvento \longleftarrow votosExistenciaEvento + 1$
        $totalQualifConhecExist \longleftarrow totalQualifConhecExist + ObterQualifConhec(M_i)$
        $totalQualifDesconhecExist \longleftarrow totalQualifDesconhecExist + ObterQualifDesconhec(M_i)$
    end
    else if M_i *informou a revogação de* E **then**
        $votosRevogacaoEvento \longleftarrow votosRevogacaoEvento + 1$
        $totalQualifConhecRevog \longleftarrow totalQualifConhecRevog + ObterQualifConhec(M_i)$
        $totalQualifDesconhecRevog \longleftarrow totalQualifDesconhecRevog + ObterQualifDesconhec(M_i)$
    end
end
if $votosExistenciaEvento + votosRevogacaoEvento \geq THRESHOLD\_MININO\_DECISAO$ **then**
    if $votosExistenciaEvento > votosRevogacaoEvento$ **then**
        $DefineOpiniaoExistenciaEvento(E, true)$
    end
    else if $votosExistenciaEvento < votosRevogacaoEvento$ **then**
        $DefineOpiniaoExistenciaEvento(E, false)$
    end
    else if $votosExistenciaEvento + totalQualifConhecExist > votosRevogacaoEvento + totalQualifConhecRevog$ **then**
        $DefineOpiniaoExistenciaEvento(E, true)$
    end
    else if $votosExistenciaEvento + totalQualifConhecExist < votosRevogacaoEvento + totalQualifConhecRevog$ **then**
        $DefineOpiniaoExistenciaEvento(E, false)$
    end
    else if $votosExistenciaEvento + totalQualifConhecExist + totalQualifDesconhecExist > votosRevogacaoEvento + totalQualifConhecRevog + totalQualifDesconhecRevog$ **then**
        $DefineOpiniaoExistenciaEvento(E, true)$
    end
    else if $votosExistenciaEvento + totalQualifConhecExist + totalQualifDesconhecExist < votosRevogacaoEvento + totalQualifConhecRevog + totalQualifDesconhecRevog$ **then**
        $DefineOpiniaoExistenciaEvento(E, false)$
    end
    else
        $DefineOpiniaoExistenciaEvento(E, false)$
    end
end
else
    //decisão forçada
    $DefineOpiniaoExistenciaEvento(E, false)$
end

O algoritmo 1 mostra a adição do RMDTV ao método *Maioria das últimas* x *mensagens considerando um limite inferior*. Primeiramente, para cada mensagem recebida, o veículo determina o tipo de impressão nela contida (confirmação ou revogação

do evento). Além disso, as qualificações apresentadas pelos emissores dessas mensagens são divididas em 2 tipos: qualificações assinadas por fontes confiáveis e por fontes desconhecidas. As qualificações assinadas por fontes maliciosas são descartadas. A soma absoluta dos parâmetros considerados é calculada. Se o veículo não recebeu a quantidade mínima de informações, definida como *THRESHOLD_MININO_DECISAO*, decide então de maneira forçada pela inexistência do evento. Se essa condição for atendida, é feito um comparativo entre a soma de mensagens informando sobre o evento e a soma daquelas revogando sua existência. Se alguma delas for maioria, a decisão é tomada. Caso contrário, são consideradas as somas das qualificações adicionadas às mensagens por suas fontes. Em um primeiro momento apenas os somatórios das qualificações assinadas por nós confiáveis são utilizados. Se isso não for suficiente, o mecanismo faz uso também daquelas qualificações cujos emissores são desconhecidos do receptor. Na impossibilidade de tomar uma decisão baseada nos dados recebidos, o veículo se decide pela inexistência do evento, pelo mesmo motivo descrito anteriormente para as decisões forçadas. Todavia, essa decisão é considerada pelo RMDTV como uma decisão indicada, haja vista que houve influência das informações recebidas em sua escolha.

3.2. Mensagens

Em uma aplicação LDW, as mensagens enviadas devem conter ao menos informações como identidade da origem, horário de geração e dados específicos sobre o evento observado, como por exemplo, seu local de ocorrência. Assim, cada mensagem é identificada de forma única e o veículo pode calcular a distância entre sua posição atual e o evento relatado. O RMDTV necessita, além da alteração do formato de uma mensagem de dados básica, da especificação de um novo tipo de mensagem, a mensagem de qualificação, utilizada no envio de qualificações aos nós considerados confiáveis por seus pares.

Neste trabalho, consideramos que cada veículo V tem sua identidade definida de forma única no início da rede. Além disso, ele recebe da Autoridade Certificadora (AC) seu par de chaves (pública e privada) correspondente e um certificado, validando sua chave pública. Utilizamos o Algoritmo de Curvas Elípticas (*Elliptic Curve Digital Signature Algorithm* - ECDSA) [Johnson et al. 2001] como solução de criptografia, uma vez que ele é mais leve que o RSA, entretanto sem comprometer a segurança da rede. Essa infraestrutura garante a segurança das mensagens enviadas, como veremos abaixo.

3.2.1. Mensagem de Dados

As mensagens com dados sobre eventos existentes na via são geradas apenas pelos veículos que transitaram pela área de reconhecimento do respectivo evento. Como tais mensagens são retransmitidas pelos receptores circulando pela área de disseminação daquele evento, é preciso garantir a integridade das informações, a fim de evitar ataques de adulteração de dados. Logo, o veículo deve assinar cada mensagem de dados por ele gerada, utilizando sua chave privada, antes de enviá-la pela rede. Além disso, o certificado emitido pela AC, que é simplesmente a assinatura da AC sobre a chave pública do veículo, também é adicionado. Assim, o formato de uma mensagem de dados é dado por:

$$M, Sig_{PrK_V}(M), Cert_{AC}(PuK_V)$$

onde M é a mensagem propriamente dita, $Sig_{PrK_v}(M)$ é a assinatura de V sobre M e $Cert_{AC}(PuK_v)$ é o certificado da chave pública de V.

Para ler o conteúdo de M, cada receptor dessa mensagem deve extrair e verificar a chave pública de V, utilizando a chave pública da AC, para depois verificar a assinatura de V utilizando a chave pública certificada.

Em cada mensagem de dados enviada, V deve acrescentar um determinado número de qualificações por ele recebidas e que ainda não expiraram, no intuito de reforçar a confiabilidade de suas informações. Essas qualificações discutidas abaixo.

3.2.2. Mensagem de Qualificação

As qualificações emitidas pelos veículos devem ser enviadas pela rede em direção ao seu destino, uma vez que cada nó é o responsável pelo armazenamento das qualificações por ele recebidas. Este encaminhamento é realizado apenas através de membros considerados totalmente confiáveis pela aplicação. Assim, a sobrecarga criada é menor e a efetividade de ataques de descarte desse tipo de mensagem é reduzida.

Uma vez que os dados de uma mensagem de qualificação também devem ter a integridade garantida, seu formato é dado por:

$$V_q|T, Sig_{PrK_V}(V_q|T), Cert_{AC}(PuK_V)$$

onde V_q é a identidade do veículo a ser qualificado, T é o horário de geração dessa qualificação, $|$ é o operador de concatenação de dados, V é o veículo qualificador de V_q, $Sig_{PrK_V}(V_q|T)$ é a qualificação emitida, na forma de uma assinatura de V sobre a identidade de V_q, concatenada com o horário de geração, e $Cert_{AC}(PuK_V)$ é o certificado da chave pública de V.

Cada receptor de uma mensagem de dados gerada por V_q deve validar as qualificações por ele apresentadas. Logo, V_q adiciona também $Cert_{AC}(PuK_V)$ a essas mensagens, já que não é possível garantir que todos os veículos da rede possuam a chave pública de V, condição necessária para a validação das qualificações por ele emitidas.

4. Avaliação de Desempenho

O simulador escolhido para a avaliação de desempenho do RMDTV foi o *Opportunistic Networking Environment* - ONE [Keränen et al. 2009]. O ONE simula um modelo de comunicação tolerante a interrupções, no qual os nós seguem o paradigma armazenar-transportar-repassar mensagens (*store-carry-forward*), mantendo-as em um *buffer* até que exista uma oportunidade para o repasse dos dados.

4.1. Caracterização da simulação

As simulações foram executadas em uma seção de aproximadamente 55 km^2 do mapa digital de Belo Horizonte, mostrado na Figura 2, englobando um dos principais corredores da cidade, a Avenida Presidente Antônio Carlos, por onde circulam diariamente milhares de veículos, resultando em vários congestionamentos.

Utilizamos 300 carros, movendo-se de acordo com o *Working Day Movement* - WDM [Ekman et al. 2008], um modelo de mobilidade que simula um dia comum na vida de pessoas que acordam pela manhã, seguem para o trabalho, onde permanecem até o fim da tarde, quando então, seguem para algum ponto de atividade noturna ou retornam diretamente para casa. Adicionamos à rede 6 ônibus (equivalente a 2% do total de carros),

que circulam ininterruptamente por uma rota pré-definida, e uma estação base, disposta ao lado da referida avenida, mais ou menos em seu ponto médio.

O tempo de simulação foi o equivalente a vinte dias. Utilizamos os valores de 200m para alcance de rádio e 1Mbps para largura de banda. Assim como nos trabalhos disponíveis na literatura, não consideramos restrições de armazenamento de dados.

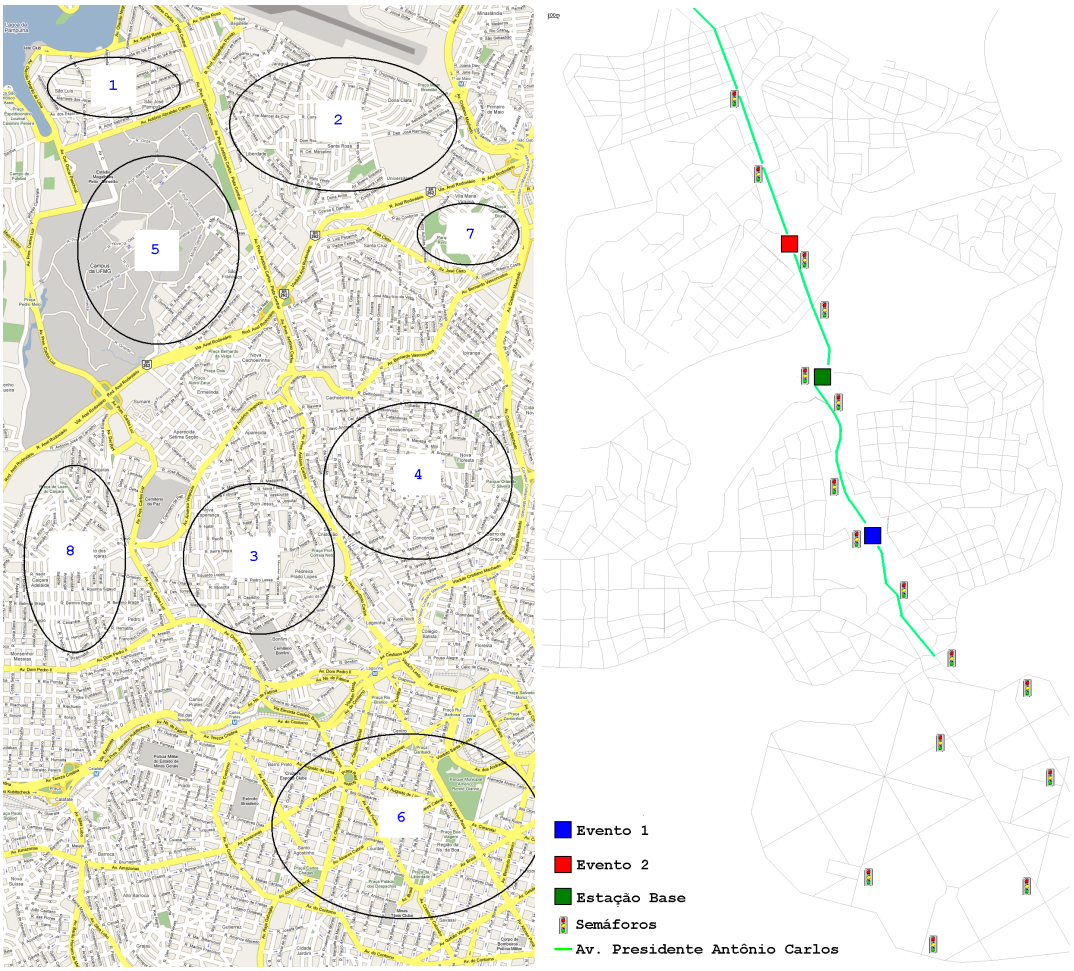

Figura 2. Mapa digital de Belo Horizonte e a representação gráfica no ONE

As regiões onde as pessoas moram, trabalham e realizam atividades noturnas, definidas no WDM, estão marcadas na Figura 2. Criamos dois grupos de nós da rede, entre os quais dividimos os 300 carros simulados na proporção de 60% e 40%, respectivamente, respeitando assim a tendência atual das pessoas viverem em lugares mais afastados do centro das grandes cidades (região 6). Essas definições são sumarizadas na Tabela 1.

Tabela 1. Distribuição dos veículos entre as regiões da Figura 2

	Percentual veículos	Moradia	Trabalho	Atividade Noturna
Grupo 1	60%	1 ou 2	6	8
Grupo 2	40%	3 ou 4	5	7

Para cada nó foi definido um horário padrão, escolhido aleatoriamente entre 7h30min e 9h30min, indicando o início diário do percurso casa-trabalho. Permitimos um

atraso ou adiantamento de até quinze minutos nesse horário, calculado aleatoriamente, em cada dia. Uma vez em seu local de trabalho, os nós lá permanecem durante oito horas. Após esse período, cada nó decide, com probabilidades de 80% e 20% respectivamente, entre seguir direto para casa ou realizar alguma atividade noturna, com duração de uma a três horas. Em casa, os nós dormem até o horário de seguir para o trabalho novamente.

Nos trajetos realizados, os carros e ônibus se movem com velocidades entre 30km/h e 60km/h, valores compatíveis com aqueles permitidos nas avenidas de Belo Horizonte. Além disso, semáforos foram dispostos em alguns cruzamentos (Figura 2). Cada semáforo permanece aberto, e posteriormente fechado, por exatamente 125 segundos simulados, tempo esse igual à média real dos semáforos da cidade. [BHTRANS 2009].

Foram considerados dois eventos dentro da área simulada, identificados na Figura 2. Enquanto o evento 1 simula a existência de um congestionamento no sentido bairro-centro, o evento 2 indica um congestionamento no sentido centro-bairro. As probabilidades de ocorrência são sumarizadas na Tabela 2. Essas probabilidades são baseadas no fato de que pela manhã existem mais veículos se deslocando no sentido bairro-centro, enquanto a tarde essa situação se inverte. Além disso, consideramos também a possibilidade de ocorrência de problemas de tráfego fora dos horários de *rush*.

Tabela 2. Probabilidade de ocorrência dos eventos ao longo do dia

	8h - 9h	**17h - 18h**	**Outros horários**
Evento 1	80%	20%	20%
Evento 2	20%	80%	20%

Como informações sobre as condições do tráfego em prováveis pontos de congestionamento sempre interessam aos membros de uma VANET, qualquer veículo, ao atingir a área de reconhecimento de um dos eventos, gera uma mensagem informando se o trânsito está livre ou congestionado naquele ponto. As mensagens geradas expiram trinta minutos após sua criação. Os raios das áreas de reconhecimento, decisão e disseminação ao redor dos eventos foram, respectivamente, 50m, 300m e 700m.

As qualificações emitidas e o histórico de comportamento dos nós, armazenado nas listas de confiabilidade locais, são válidos durante todo o período simulado. A quantidade de qualificações adicionadas às mensagens de dados foi limitada a no máximo vinte ou seja, média de uma por dia simulado.

De forma a garantir uma baixa sobrecarga gerada pelo tráfego das mensagens de qualificação, estas só podem ser encaminhadas diretamente ao seu destino final ou para os membros considerados a *priori* confiáveis pelos nós da rede (ônibus e a estação base).

Assim como em [Ostermaier et al. 2007], o número máximo de mensagens utilizadas pelo *Maioria das últimas x mensagens considerando um limite inferior* foi 22, enquanto o número mínimo de opiniões para a execução do método foi fixado em 3.

Os intrusos presentes na rede, ao adentrarem na área de reconhecimento de um evento, executam ataques do tipo *alarmes trocados*, ou seja, geram mensagens invertendo a situação atual daquele evento. Assim, em caso de tráfego livre, informam a existência de um congestionamento e vice versa.

Nossa avaliação se concentrou em comparar o desempenho entre duas redes: uma

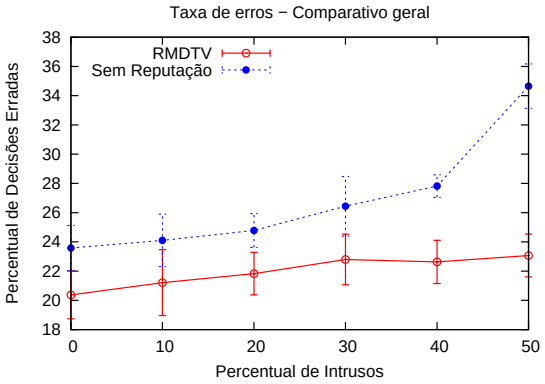

Figura 3. Influência dos intrusos no percentual total de decisões erradas

utilizando o RMDTV como mecanismo de reputação e outra na qual nenhum mecanismo é utilizado. Comparamos o desempenho das duas redes quanto ao percentual de decisões erradas tomadas pelos veículos, onde entende-se por decisão errada o fato de o veículo se decidir por uma situação diferente daquela atualmente existente na via. Todos os resultados apresentados possuem 90% de intervalo de confiança. Cada simulação foi executada com oito sementes diferentes.

4.2. Resultados e Análises

Nas simulações realizadas, partimos de um cenário sem intrusos, finalizando com uma situação onde 50% dos carros existentes são inimigos, aumentando esse percentual a taxas de 10%. Os resultados obtidos são analisados a partir do percentual total de decisões erradas tomadas pelos nós e também a partir das variações diárias dessas decisões.

4.2.1. Percentual Geral de Decisões Erradas

O gráfico da Figura 3 mostra o desempenho geral das redes com e sem a execução do RMDTV. Podemos perceber que existe uma relação quase linear entre o percentual de intrusos e de decisões erradas. A rede executando o RMDTV possui um desempenho melhor que a rede sem reputação em todos os cenários simulados. Considerando-se os pontos médios, essa melhoria varia entre 14% (sem intrusos) e 45% (50% de intrusos).

4.2.2. Variação Diária das Decisões Erradas

Os gráficos da Figura 4 mostram o percentual de erros diários na rede com e sem a execução do RMDTV, com percentuais de 0%, 10%, 30% e 50% de intrusos na rede.

Podemos observar alternâncias diárias, tanto positivas quanto negativas, no percentual de decisões erradas. Tais alternâncias são fruto das variações simuladas no horário padrão em que cada veículo sai de casa diariamente. Assim, da mesma forma que essa variação pode fazer com que um veículo encontre mais nós cooperativos em um dia, pode implicar também, de maneira oposta, no estabelecimento de conexões com uma maioria de nós maliciosos, no dia seguinte.

A rede com reputação apresentou melhores resultados durante todo o tempo simulado, para todos os percentuais de intrusos. Além disso, percebemos uma evolução no distanciamento entre as curvas proporcional ao percentual de intrusos, corroborando o resultado mostrado na Figura 3. Abaixo, discutimos alguns pontos importantes observados.

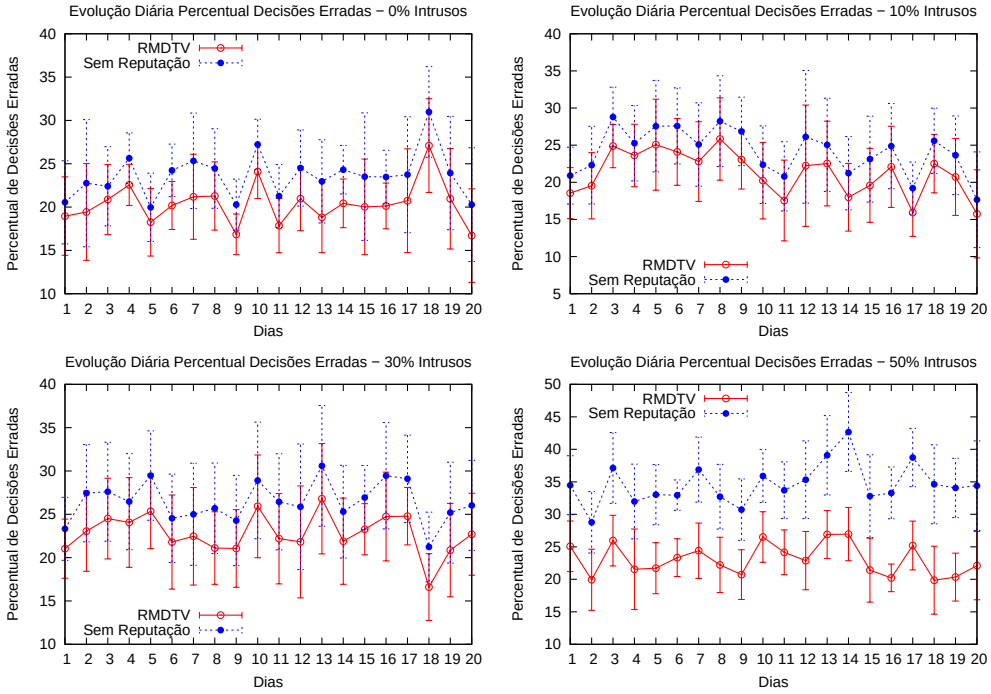

Figura 4. Percentual diário de decisões erradas na rede

A existência de decisões erradas, mesmo na ausência de intrusos, é fruto do dinamismo dos eventos, pois uma vez que haja alguma alteração no estado de um evento, ainda existem muitas mensagens circulando pela rede informando seu estado anterior. Entretanto, o melhor resultado da rede com reputação mesmo nessa situação é fruto de uma tomada de decisão mais ágil quando o RMDTV é executado. Para que um veículo executando o RMDTV tome sua decisão acerca de um evento, basta que ele receba informações geradas por uma fonte confiável. Já em redes sem uso de reputação, o veículo coleta informações sobre o evento até atingir sua área de decisão. Como durante essa coleta podem ocorrer mudanças no estado do evento, a decisão tomada pode ser influenciada por mensagens desatualizadas. Isso acontece até que o sistema se estabilize novamente.

A existência de um percentual menor de erros desde o primeiro dia de simulação, quando ainda não existem relações de confiança entre os veículos, é justificada pela presença dos ônibus, considerados sempre confiáveis, circulando pela área simulada.

5. Trabalhos Relacionados

Mecanismos de reputação em MANETs geralmente consideram a existência de caminhos fim-a-fim a todo o momento entre quaisquer dois membros da rede. Assim, é possível aguardar a confirmação de término de um serviço solicitado antes de atualizar a reputação dos responsáveis por sua execução [Dewan et al. 2004]. Existem ainda propostas que consideram apenas suaves alterações na topologia da rede ao longo do tempo, de forma que o compartilhamento de opiniões entre pequenos grupos seja suficiente definir a reputação dos nós. [Buchegger and Le Boudec 2004]).

Como em VANETs tais considerações não podem ser garantidas, dadas as grandes velocidades de deslocamento dos veículos na rede, devem ser desenvolvidas soluções

próprias para esses cenários, nas quais suas particularidades são respeitadas.

Em [Dotzer et al. 2005] cada veículo adiciona sua opinião sobre a veracidade das mensagens por ele recebidas e encaminhadas em uma aplicação LDW. Todavia, em redes esparsas, a quantidade de opiniões contidas em uma mensagem recebida pode ser extremamente baixa, de forma que mensagens geradas por veículos cooperativos tenham o mesmo peso que aquelas geradas por intrusos.

Na proposta de [Wang and Chigan 2007] a mensagem é enviada salto a salto acompanhada de um *token* validando sua integridade. Assim, a aceitação de seus dados é dependente do conteúdo do *token*. A proposta não se preocupa com a correção da mensagem em si, mas apenas com sua adulteração no roteamento, possibilitando então que mensagens geradas por nós maliciosos sejam disseminadas normalmente pela rede.

[Ostermaier et al. 2007] apresentam um esquema baseado em votos para aumentar a segurança das decisões tomadas pelos veículos em aplicações LDW. Dentre os quatro métodos avaliados, o *Maioria das últimas x mensagens considerando um limite inferior* foi o responsável pelos resultados mais significativos. Como o conceito de reputação não é aplicado, nós maliciosos podem executar seus ataques livremente, na certeza de que suas mensagens serão sempre consideradas no processo de decisão de outros veículos, uma vez que não existem retaliações ao seu mau comportamento.

No trabalho de [Patwardhan et al. 2006] a reputação dos nós da rede é baseada apenas nos históricos de comportamento armazenados localmente. Como esses dados não são compartilhados, existe uma demora considerável no processo de estabelecimento de relações de confiança e detecção de intrusos.

O mecanismo de reputação proposto, chamado RMDTV, faz uso do método *Maioria das últimas x mensagens considerando um limite inferior* para a tomada de decisões em aplicações LDW. Validações posteriores dessas decisões permitem a identificação de nós cooperativos e maliciosos. Com o armazenamento de dados históricos sobre o comportamento dos veículos, é possível o reconhecimento prévio e a exclusão de dados gerados por nós tidos como maliciosos. O compartilhamento de experiências, realizado na forma de qualificações assinadas digitalmente, aumenta a robustez do RMDTV, além de permitir o estabelecimento de relações de confiança antes mesmo do início de transações.

6. Conclusões e Trabalhos Futuros

Neste trabalho, propusemos um mecanismo de reputação para redes veiculares, o RMDTV, que possibilita aos nós da rede atestar a confiabilidade das informações emitidas por outros participantes. Esse mecanismo faz uso de qualificações emitidas por terceiros e roteadas pela rede mesmo sob condições de desconectividade, aliadas às experiências que o próprio nó teve com os emissores dessas qualificações.

Analisamos desempenho do RMDTV em uma VANET executando uma aplicação distribuída de segurança, na qual seus membros trocavam mensagens informando as condições de tráfego em pontos específicos da cidade. Os resultados obtidos mostraram que o RMDTV é capaz aumentar consideravelmente a resiliência de redes veiculares sujeitas a ataques do tipo alarmes trocados, em comparação com cenários onde nenhum mecanismo de reputação é utilizado.

É possível continuar o desenvolvimento do RMDTV alterando a forma de

classificação dos nós em confiáveis ou intrusos. Como mensagens enviadas por nós confiáveis têm um peso muito grande no processo de decisão, enquanto aquelas enviadas por intrusos são simplesmente descartadas, acreditamos que a definição de funções de promoção e rebaixamento progressivos pode aumentar o desempenho do sistema, uma vez que a quantidade de membros promovidos a confiáveis ou rebaixados a intrusos erroneamente tende a diminuir consideravelmente.

Referências

BHTRANS (2009). Empresa de transportes e trânsito de belo horizonte. `http://www.bhtrans.pbh.gov.br`. Acessado em dezembro de 2009.

Buchegger, S. and Le Boudec, J. Y. (2004). A robust reputation system for p2p and mobile ad-hoc networks. In *Proc. of the 2nd Workshop on the Economics of P2P Systems*.

Dewan, P., Dasgupta, P., and Bhattacharya, A. (2004). On using reputations in ad hoc networks to counter malicious nodes. In *ICPADS '04: Proceedings of the Parallel and Distributed Systems, Tenth International Conference*, Washington, USA. IEEE.

Dotzer, F., Fischer, L., and Magiera, P. (2005). Vars: A vehicle ad-hoc network reputation system. In *WOWMOM '05: Proceedings of the Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks*, Washington, USA. IEEE.

Ekman, F., Keränen, A., Karvo, J., and Ott, J. (2008). Working day movement model. In *MobilityModels '08: Proceedings of the 1st ACM SIGMOBILE*, New York, USA.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, New York, USA. ACM.

Johnson, D., Menezes, A., and Vanstone, S. A. (2001). The elliptic curve digital signature algorithm (ecdsa). *Int. J. Inf. Sec.*

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The one simulator for dtn protocol evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, Rome, Italy. ACM.

Kosch, T. (2004). Local danger warning based on vehicle ad-hoc networks: Prototype and simulation. In *WIT '04: Proc. of 1st Inter. Workshop on Intelligent Transportation*.

Ostermaier, B., Dotzer, F., and Strassberger, M. (2007). Enhancing the security of local danger warnings in vanets - a simulative analysis of voting schemes. In *ARES '07: Proceedings of the The Second International Conference on Availability, Reliability and Security*, Washington, USA. IEEE.

Patwardhan, A., Joshi, A., Finin, T., and Yesha, Y. (2006). A data intensive reputation management scheme for vehicular ad hoc networks. In *Proceedings of the Second International Workshop on Vehicle-to-Vehicle Communications*. IEEE.

Wang, Z. and Chigan, C. (2007). Countermeasure uncooperative behaviors with dynamic trust-token in vanets. In *ICC '07: Proceedings of IEEE International Conference on Communications*, Glasgow, Scotland. IEEE.

Zimmermann, P. (1994). Pgp user's guide. Cambridge, MA: MIT Press.