Um Sistema de Reputação Descentralizado para Avaliar a Confiança dos Nós em Redes Veiculares

Claudio P. Fernandes[1], Israel de Simas[2], Michelle Wangham[1]

[1] Programa de Mestrado em Computação Aplicada –Universidade do Vale do Itajaí (UNIVALI)

[2] *Programa de Pós-Graduação em Engenharia de Automação e Sistemas (UFSC)*

euclaudio@redes.ufsm.br, israel.de.simas@gmail.com, wangham@univali.br

Abstract. *In vehicular networks, cooperation between nodes is needed for proper performance of traffic applications. The objective of this work is to analyze the reliability of the vehicles in an application of Local Danger Warning (LDW) for vehicular networks in order to identify the presence of malicious nodes and discard their alerts through the development of a decentralized reputation system. The effectiveness of reputation system and the impacts of the use of the proposed system by a LDW application for roads were evaluated through experiments with network and traffic simulators.*

Resumo. *Nas redes veiculares, a cooperação entre os nós se faz necessária para um desempenho adequado das aplicações de segurança no trânsito. O objetivo deste trabalho é analisar a confiança dos veículos em uma aplicação de Alerta de Perigo Local (LDW) para redes veiculares de forma a identificar a presença de nós maliciosos e descartar seus alertas por meio de um sistema de reputação descentralizado. A eficácia do sistema de reputação e os impactos decorrentes do uso do sistema por uma aplicação LDW para rodovias foram avaliados através de experimentos realizados com simuladores de rede e de tráfego.*

1. Introdução

A extensão das MANETs (*Mobile Ad hoc Networks*) em ambientes veiculares deu origem a uma nova categoria – as VANETs (*Vehicular Ad Hoc Networks*) - que tem como objetivo melhorar as condições de circulação dos tráfegos urbanos e rodoviários de forma segura e eficiente e garantir a comunicação entre os diversos usuários móveis inseridos na rede. Este cenário consiste de veículos atuando como roteadores móveis, com o objetivo de enviar, receber, armazenar e encaminhar os pacotes pela rede [Ostermaier et al 2007].

Segundo Lee et al. (2008), um dos principais estímulos para as redes veiculares é o desejo de aumentar ainda mais a segurança em ruas e rodovias melhorando, também a eficiência do tráfego, utilizando-se da comunicação entre os veículos. Dentre as aplicações, destacam-se as de alerta de perigo local (LDW – *Local Danger Warnings*) devido ao significativo benefício coletivo trazido pela disseminação de mensagens que informam situações de risco nas vias, como por exemplo, a presença de óleo na pista.

Em uma Aplicação de Alerta de Perigo Local (LDW), a cada evento detectado é gerado um alerta informando sua condição. Cada receptor desses dados atua como roteador da mensagem, aumentando assim o alcance deste aviso. Além disso, em uma aplicação LDW, os nós avaliam o conteúdo dos alertas recebidos. Toda vez que a aplicação considerar suficiente as evidências de um evento, esta 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 [Kosch 2004].

Nesta aplicação, o uso de informações erradas nos processos de decisão executados pelos veículos pode colocar em risco a segurança de vidas humanas. A segurança em VANETs é um fator bastante relevante, pois estas estão suscetíveis a ataques por nós maliciosos [Raya et al. 2006]. Nas aplicações LDW, 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, torna-se necessário o desenvolvimento de soluções capazes de incentivar comportamentos cooperativos e punir os comportamentos maliciosos. Sistemas de reputação contribuem com esse objetivo na medida em que permitem aos nós decidirem em quem confiar [Ostermaier et al. 2007]. Esses sistemas assumem que o comportamento antigo de um nó da rede, indica de forma bem confiável suas ações futuras [Paula et al 2010].

Este artigo tem por objetivo descrever um sistema de reputação descentralizado para avaliar a confiança dos nós em uma aplicação LDW, de forma a identificar a presença de nós maliciosos e descartar seus alertas. Para a avaliar a eficácia do sistema proposto e os possíveis impactos do sistema em uma aplicação LDW para rodovias, foram realizados experimentos com simuladores de rede e tráfego bidirecionalmente acoplados.

2. Trabalhos Relacionados

Embora existam vários trabalhos sobre sistemas de reputação para comércio eletrônico ou redes P2P, alguns possuem as bases de dados centralizadas ou não funcionam bem em redes altamente dinâmicas como nas VANETs. Apesar de serem um tipo especial de MANETs, as VANETs são extremamente dinâmicas, possuem alta mobilidade, a topologia da rede muda rapidamente, as desconexões são frequentes e o número de nodos pode ser muito elevado. Nas MANETs, os nós permanecem estáveis durante um período relativamente longo e se deslocam lentamente, não havendo grande mobilidade dos nós. Como resultado, muitos sistemas de reputação existentes em MANETs não são adequados para as redes veiculares [Wang e Chigan 2007]. Após a execução de um protocolo de busca (revisão sistemática), foram identificados seis trabalhos que descrevem sistemas de reputação com o objetivo de evitar ou minimizar ataques de nós maliciosos em VANETs, sendo alguns destes específicos para a classe de aplicação LDW.

Ostermaier et al. (2007) propuseram um sistema de reputação baseado em votação para VANETs que visa avaliar a credibilidade das mensagens (eventos) para aumentar a segurança das decisões tomadas pelos veículos sobre eventos reportados em aplicações LDW. O trabalho avaliou o resultado de quatro métodos de decisão da credibilidade do perigo relatado baseados no sistema de votação. O sistema proposto não trata da reputação dos nós, mas sim das mensagens (eventos). O custo computacional de procesammento e a sobrecarga na rede decorrentes do uso deste mecanismo não foram avaliados pelos autores.

Em Wang e Chigan (2007), o mecanismo de confiança *Dynamic Trust-Token* (DTT) tem o objetivo de detectar a modificação de mensagens na rede por nós maliciosos e isolar estes nós de forma a prevenir que estes interfiram nas próximas mensagens. Quando um nó viola esta integridade, este é considerado malicioso. O mecanismo baseia-se apenas no comportamento dos veículos em tempo de execução, definindo desta maneira reputações instantânea e não avalia nós maliciosos que propagam mensagens falsas na rede.

No mecanismo de reputação denominado RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*) [Paula et al 2010], cada membro da rede qualifica uma informação (correta ou não) de um outro membro e emite uma mensagem de qualificação

(confiabilidade). O emissor da mensagem armazena as mensagens de qualificação e as usa nos próximos envios como se estas fossem suas credenciais que comprovam suas mensagens corretas já propagadas na rede. Ou seja, o sistema faz uso de qualificações emitidas por terceiros para atestar a confiança nos nós. Neste mecanismo, não existe um rebaixamento progressivo dos nós na rede, desta forma basta que o veículo apresente um comportamento malicioso uma única vez, para que este passe a ser considerável 100% malicioso. Da mesma maneira, basta que envie uma mensagem de qualificação correta para ser considerado 100% confiável.

Lo e Tsai (2010) apresentam um sistema de reputação para determinar se uma mensagem recebida pelo nó é significativamente confiável para ser mostrada ao motorista. Um nó calcula a reputação de um evento somando o número de vezes que este foi gerado pelos demais nós da rede. Se este valor for maior que um limite de reputação estabelecido (*threshold*), então o sistema conclui que o evento foi gerado corretamente. Caso contrário, o sistema avalia que o evento não mais existe ou que este é um evento falso. Quando o número de ocorrências de um evento exceder o limiar de confiança, significa que mais veículos detectaram o evento e, portanto, a probabilidade deste ser verdadeiro é maior. Desta forma, caso um evento exceda estes dois parâmetros, este é considerado confiável e é enviado aos demais nós. Neste trabalho, existe a necessidade de configuração dos *thresholds* para cada evento de forma a fornecer informações precisas e confiáveis para os condutores.

Em Daeinabi e Ghaffarpour (2011), os autores propõem um sistema chamado DMV (*Detection of Malicious Vehicles*) que visa monitorar nós maliciosos que rejeitam ou duplicam pacotes recebidos de forma a isolá-los dos nós considerados honestos. Cada veículo é monitorado por vizinhos confiáveis chamados de nós verificadores. Caso um nó verificador, identifique um comportamento anormal de um veículo, este reporta para uma Autoridade Certificadora (AC) para que esta atualize o valor de desconfiança do veículo. Um nó é considerado malicioso quando o seu valor de desconfiança é superior a um *threshold* mínimo. Quando isto ocorre, este veículo é retirado da lista branca e é acrescentado na lista negra. A AC transmite periodicamente estas listas para os líderes de agrupamento da rede. Neste trabalho, como a base de consulta da reputação de um nó é centralizada nos líderes de agrupamento, existe, dentro de um agrupamento, um único ponto de falha e um gargalo de desempenho (se um grande número de veículos requisitarem informações de reputação). Além disso, este trabalho não trata do problema do envio de mensagens falsas na rede.

Li et al. (2012) propõem um sistema de reputação para redes veiculares que permite avaliar a confiabilidade da mensagem recebida de acordo com a reputação do veículo que gerou esta mensagem. O sistema proposto faz uso de um servidor de reputação centralizado. Quando um veículo recebe uma mensagem, caso este ainda não tenha tido uma experiência anterior com o emissor, este consulta o servidor de reputação para obter a reputação global calculada através da média ponderada das experiências anteriores dos demais nós da rede. Além dos problemas de falha e desempenho de uma abordagem na qual o servidor é centralizado, os autores não tratam a situação quando um nó é desconhecido também para o servidor de reputação.

A Tabela 1 apresenta uma comparação dos sistemas de reputação encontrados na literatura, considerando as seguintes características: (1) se as informações consultadas para o cálculo da reputação estão armazenadas em uma base centralizada, descentralizada ou local; (2) se o sistema é utilizado em uma aplicação LDW; (3) como este pode ser classificado - otimista (nós desconhecidos são confiáveis) ou pessimista (nós desconhecidos

são não confiáveis) e global (os nós se utilizam de informações dos outros nós da rede para calcular a reputação) ou local (somente as observações locais dos nós são consideradas); e (4) qual reputação é calculada pelo sistema (dos nós ou das mensagens) e as técnicas utilizadas para obter a reputação.

Tabela1: Comparação dos Trabalhos Relacionados

Trabalhos	Base de Info. Consultada	App LDW	Abordagem	Sistema de Reputação
Ostermaier et al (2007)	Descentraliz.	Sim	Otimista	Mensagens. Sistema de Votação
Wang e Chigan (2007)	Local	Não	Otimista Local	Mensagens. Reputação Instantânea
RMDTV (Paula et al. 2010)	Descentraliz.	Sim	Otimista Global	Nós. Qualificações das mensagens feitas por terceiros
ERS (Lo e Tsai 2010)	Descentraliz.	Sim	Pessimista[1] Global	Mensagens. Detecção do mesmo evento pelos demais nós da rede
Daeinabi e Ghaffarpour (2011)	Centralizada	Não	Otimista Local	Nós. Avaliação do comportamento dos nós por terceiros (contador).
Li et al. (2012)	Centralizada	Não	Indefinida Global	Nós. Média ponderada para reputação global.
Sistema Proposto	Descentraliz.	Sim	Otimista Global	Nós. Métodos Estatísticos. Sistema de Votação. Lista de Reputação

3. Sistema de Reputação Descentralizado Proposto

Segundo Li et al. (2012), detectar nós maliciosos tornou-se um dos problemas mais difíceis no que diz respeito a segurança em VANETs. Minimizar os ataques e as consequências de comportamentos maliciosos é muito importante em soluções que necessitam da cooperação e da honestidade dos nós, tais como as aplicações LDW. Tais aplicações podem ser muito úteis para prover segurança do trânsito nas rodovias, porém, a confiança nos nós, que propagam e difundem os alertas, deve ser avaliada. O objetivo da solução descrita neste trabalho é identificar a presença de nós maliciosos em uma aplicação LDW, chamada de RAMS+, de forma a descartar seus alertas.

A rede veicular é composta por veículos e unidades de acostamento (*RSUs - Road Side Unit*). As *RSUs* são equipamentos que servem como nós intermediários para a troca de informações com os veículos. Diante do recebimento de uma mensagem de alerta, cada veículo, de acordo com a distância que este estiver do local da ocorrência (região geográfica da aplicação LDW), deve utilizar o sistema de reputação para avaliar o nível de confiança no veículo que gerou o alerta. O sistema proposto, ao calcular a reputação dos nós, considera que somente poucos relacionamentos prévios existem, o que exige o cálculo da confiança de nós desconhecidos. No sistema, as unidades de bordo dos veículos e as RSUs não estão ligadas a um ponto central responsável por avaliar a confiança dos nós e por conter a base de reputação dos nós participantes, o que caracteriza o sistema como descentralizado. Com as informações sobre o comportamento dos veículos, armazenadas de forma distribuída, a disponibilidade deste conteúdo, altamente dinâmico, é garantida.

O sistema de reputação proposto faz uso de uma estratégia investigativa, ou seja, a reputação do nó é avaliada consultando outros nós participantes da rede, e faz uso também de uma estratégia otimista na qual os nós têm reputação boa até que se prove o contrário.

[1] O quão pessimista é dependerá do valor do limite de reputação definido na configuração do sistema.

No sistema, consideram-se como premissas: (1) cada veículo tem sua identidade definida de forma única na rede; (2) os veículos possuem componentes que possibilitem a comunicação e a execução dos aplicativos tais como, sensores, unidades de armazenamento, unidade de comunicação sem fio, sistema de posicionamento (GPS) e uma interface com o usuário para mostrar ao condutor os alertas e a localização dos eventos relatados; (3) os eventos podem ser sempre detectados pelos sensores dos veículos; e que (4) o GPS tem precisão suficiente para detectar em qual local da rodovia encontra-se o veículo.

Cada veículo possui uma base de conhecimento individual (BCI), que contém informações sobre as interações passadas que este teve com outros veículos. A BCI armazena as experiências passadas mais recentes e o veículo a utiliza para o cálculo da reputação direta. Para encontrar a reputação global do veículo, o sistema proposto calcula ainda a reputação agregada (indireta), definida a partir de informações de terceiros, muito importante para o cálculo da reputação de veículos desconhecidos. No sistema proposto, outra informação que auxilia a tomada de decisão de um veículo que recebeu uma mensagem de alerta é uma lista de reputação propagada pelas *RSUs*. Esta lista é muito importante, quando o veículo está muito próximo do local do evento, já que este pode não ter tempo suficiente para calcular a reputação global, e por manter uma base de reputação mais abrangente e atualizada (ver Seção 3.4).

3.1 Aplicação LDW (RAMS+)

No RAMS+ (*Road Alert Message Service - plus*), os sensores dos veículos são responsáveis pela detecção automática dos perigos nas rodovias (experiência do veículo). O sistema recebe a sinalização dos eventos pelos sensores, gera as mensagens de alerta e as envia em *broadcast*. O RAMS+ baseia-se nas três regiões geográficas semelhante ao que acontece nas aplicações LDW. Estas regiões são (ver Figura 1):

- **Área de Reconhecimento:** é a área mais próxima do evento (interna), na qual o perigo pode ser detectado pelos sensores dos veículos. Apenas os veículos dentro desta área são realmente capazes de detectar a presença de um perigo e criar a mensagem de alerta.
- **Área de Decisão**: é a área intermediária, na qual o veículo determina se alguma ação deve ser tomada a respeito dos alertas recebidos tendo como base a reputação do veículo que originou a mensagem.
- **Área de Disseminação:** é a área mais longe do evento (externa), na qual os veículos realizam o processo de coleta e repasse das informações recebidas sobre o evento tendo como base a reputação do veículo emissor. Nesta área, a mensagem ainda não é apresentada ao motorista.

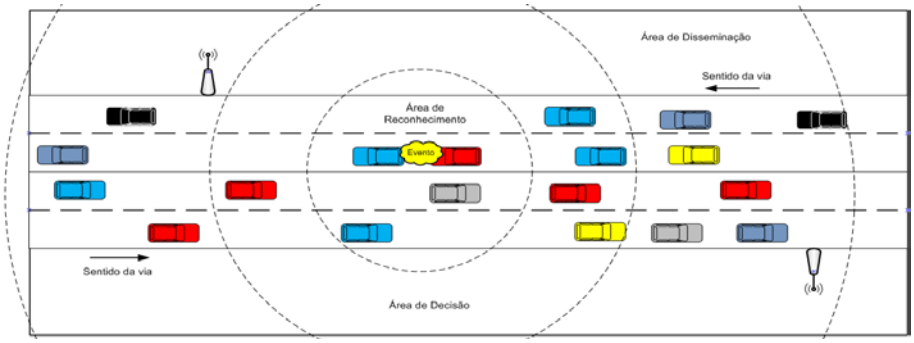


Figura 1: Definições das áreas LDW

O RAMS+ instalado nos veículos troca as seguintes mensagens:

- **Mensagem de Alerta (*MenAlert*):** toda vez que um veículo entra na área de reconhecimento e os sensores detectam um evento, o RAMS+ cria e distribui pela rede uma mensagem *MenAlert* informando o perigo (e.g. a presença de óleo na pista), quando o evento foi detectado, a localização e a identificação do emissor do alerta. Na região geográfica de disseminação, uma mensagem de alerta emitida por um veículo avaliado como confiável é reenviada pela rede até que esta atinja um tempo limite, cuja finalidade é indicar que esta mensagem foi criada recentemente.
- **Mensagem de Revogação de Alerta (*MenRevog*):** esta mensagem tem como objetivo informar aos veículos que receberam uma mensagem de alerta (*MenAlert*) que este evento/perigo já foi revogado, ou seja, o evento realmente ocorreu, porém já não existe mais. Somente veículos que fazem a manutenção da rodovia podem revogar um alerta.

3.2 Integração do Sistema de Reputação à aplicação RAMS+

As atividades executadas pelo RAMS+ com o sistema de reputação integrado, após o recebimento de uma mensagem de alerta (*MenAlert*), estão identificadas na Figura 2. Após verificar que a mensagem *MenAlert* é uma mensagem nova e que esta foi criada a um tempo menor que o limiar de mensagem recente, o RAMS+, por meio do sistema de reputação, deve obter a reputação do emissor consultando a Lista de Reputação (LR) recebida e avaliar se esta está acima de um limiar de reputação que considera este veículo confiável (e.g. 0,5). Caso este veículo seja considerado não confiável, a mensagem é descartada. Caso o veículo não esteja na lista de reputação ou caso este tenha sido considerado como confiável, a aplicação irá calcular a distância que o veiculo está do evento relatado. Caso este veículo esteja muito próximo do local do evento (e.g. 100 metros), o alerta é mostrado para o condutor do veículo, pois pode não haver tempo hábil para a realização da consulta aos outros veículos (cálculo da reputação global). Caso contrário, a aplicação irá calcular a reputação global do emissor do alerta conforme a Equação (3) descrita na Seção 3.3. Se o resultado da reputação for maior que o limiar de reputação, o emissor é avaliado como confiável. Caso este esteja na área de decisão, o alerta é mostrado para o condutor e repassado para os demais veículos. Quando o emissor for avaliado como confiável e a distância do veículo estiver fora da área de decisão, um novo processo é criado com a finalidade de monitorar a entrada do veículo na área de decisão, para que o alerta seja posteriormente mostrado ao condutor quando este entrar nesta área.

3.2.1 Base de Conhecimento Individual

Conforme descrito anteriormente, cada veículo registra e mantém um histórico em sua base de conhecimento individual (BCI) dos resultados das interações que teve diretamente com outros veículos, contabilizando o número de vezes que estes eventos foram confirmados ou não confirmados.

O sistema de reputação utiliza a BCI de um veículo A para calcular a reputação direta dos demais veículos com os quais A interagiu no passado. Cabe salientar, que o número máximo de interações armazenadas no histórico do BCI serão as últimas 10 interações com cada nó. Este limite tem como objetivo manter o BCI somente com avaliações mais recentes, permitindo que um veículo que mude de comportamento, por exemplo, passando a agir de forma maliciosa, possa ser detectado mais rapidamente.

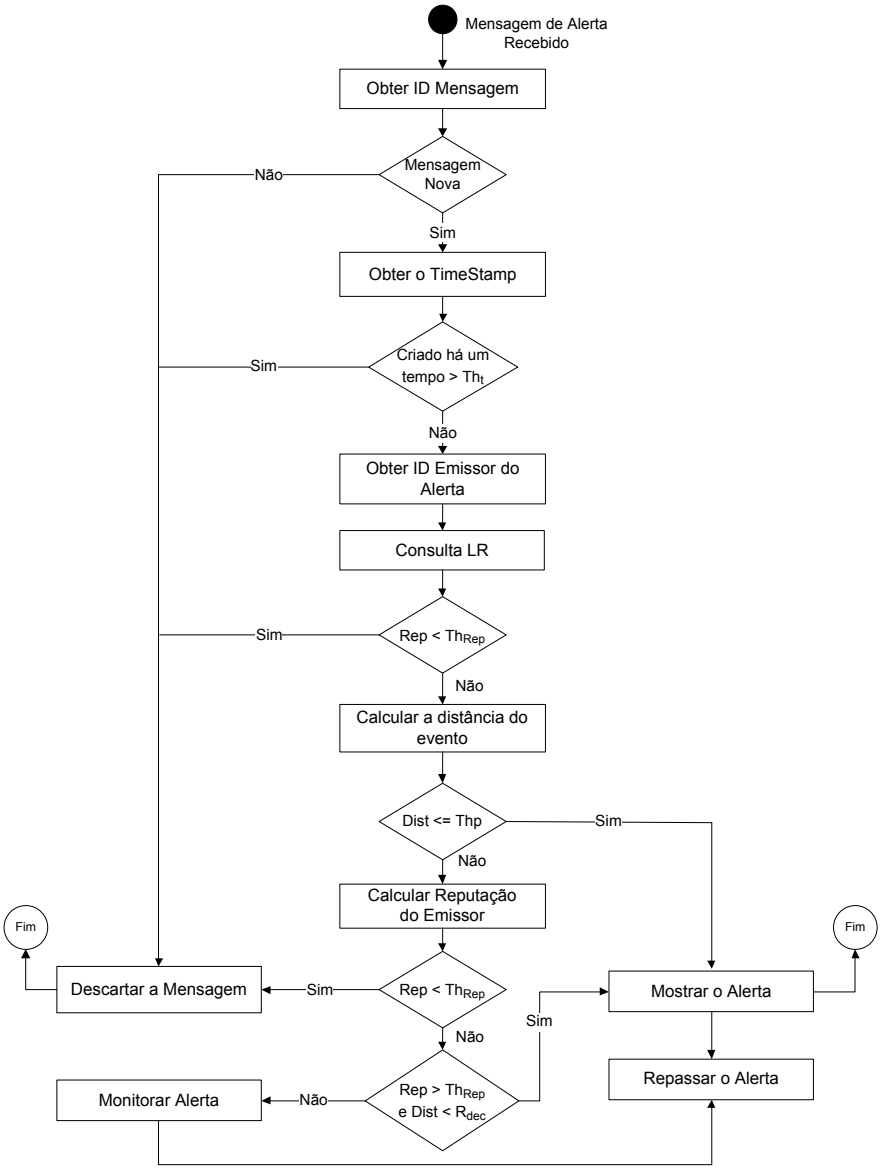


Figura 2 Diagrama de Atividades - Tomada de decisão

3.2.2 Validação de Alerta e Atualização da BCI

Um veículo, ao passar pelo local do evento relatado em uma mensagem *MenAlert*, deve, através de seus sensores, verificar a real existência do evento para então enviar uma mensagem que valida a ocorrência do evento (*MenValid*) aos demais veículos, confirmando ou não este evento. Esta mensagem é criada pelo veículo que recebeu um alerta e que está executando o processo Monitorar Alerta ou quando o RAMS+ é informado pelo sensor do veículo a detecção de um evento. O acréscimo desta nova mensagem no RAMS+ visa atestar a credibilidade das mensagens de alertas recebidas entre os veículos e, consequentemente, servirá para identificar eventos falsos relatados por nós maliciosos.

As Mensagens de Validação de Alerta (*MenValid*) são consolidadas e armazenadas localmente nos veículos em uma Base de Validação de Alerta (BVA), que tem como função principal armazenar informações que serão utilizadas pelo veículo para avaliar se os eventos

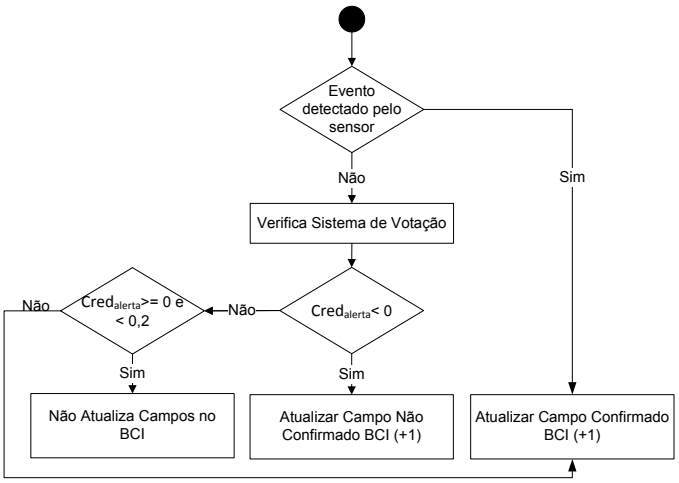
relatados foram comprovados pelos demais veículos. A BVA é composta pelos campos: IDV (placa do veículo que gerou o alerta); IDMsg (identificador da mensagem *MenAlert*); *Acks* (total de veículos que ao passar pelo local do evento, confirmaram o evento na mensagem *MenAlert*); *Naks* (total de veículos que ao passar pelo local do evento, não detectaram o evento), conforme ilustrado no exemplo da Figura 3A.

A BVA é utilizada também para a atualização da BCI, após o recebimento de mensagens de validação de alertas (*MenValid*). O diagrama de atividades ilustrado na Figura 3B apresenta os passos que devem ser executados para que um veículo atualize sua base de conhecimento individual (BCI). Um veículo, ao passar pelo local do evento relatado em uma mensagem de alerta (*MenAlert*) e atestar, através de seus sensores, a presença do evento, este deve atualizar sua BCI incrementando o valor de +1 no campo de interações confirmadas do veículo que originou a mensagem. Caso o evento não seja detectado pelo sensor do veículo (não confirmado), o RAMS+, antes de atualizar a BCI do veículo e punir o emissor do alerta, (incrementando o valor +1 no campo não confirmado), avalia as opiniões dos outros veículos sobre o alerta recebido (com base nas mensagens *MenValid* recebidas), utilizando para isto um sistema de votação que avalia a credibilidade do alerta.

Para avaliar a credibilidade, o sistema de votação coleta os dados da mensagem avaliada da BVA e executa os seguintes passos: (1) calcula se o número de confirmações do alerta (*ACKs*) é maior que o de não confirmação (*NACKs*), por meio da Equação 1. (2) Caso esta diferença não seja considerável ($Cred_{alerta}$ entre 0 e 2), o sistema não irá atualizar a BCI, pois não há evidências para punir ou promover o veículo que originou o alerta. Caso comprovado que houve mais mensagens que confirmam a ocorrência do alerta ($Cred_{alerta}$ maior que 0,2), o sistema irá incrementar o campo *BCIConfirmados* do veículo que originou o alerta. Caso seja identificado mais *NACKs* que *ACKS* ($Cred_{alerta}$ menor que *0*), o sistema irá punir o veículo que originou o alerta incrementando o campo *BCINaoConfirmados*.

$$Cred_{alerta} = \left|\frac{ACKs - NACKs}{ACKs + NACKs}\right| \quad (1)$$

IDV	IDMsg	Acks	Nacks
MCX 1040	02354	8	2
ICX 1348	02567	21	13
ICC 0935	02450	8	19
MCK 1011	02333	16	1
IWK 0971	02121	9	10



(A) **(B)**

Figura 3: (A) Exemplo de uma BVA; (B) Fluxo para Atualização da BCI.

Este sistema de votação visa aumentar a segurança das decisões tomadas a respeito da punição de um veículo, visto que existe a possibilidade do evento relatado na mensagem já não mais existir quando o veículo passar pelo local da ocorrência e este não recebeu a mensagem de revogação do alerta (*MenRevog*).

3.3 Cálculo da Reputação Global

No sistema de reputação proposto, cada veículo faz uso da BCI para calcular a reputação direta que representa a visão individual que um veículo *i* possui a respeito da confiança em outro veículo *j*, baseada apenas nas interações passadas entre estes. Semelhante ao descrito em [Mello et al. 2009], no sistema proposto, optou-se pela utilização de uma análise bayesiana para determinar a probabilidade de um veículo *j* honrar futuras interações (cálculo da reputação direta).

No sistema de reputação proposto, os parâmetros α e β funcionam como registros (confirmados e não confirmados) do total de interações entre os veículos *i* e *j*, registros estes obtidos da BCI e utilizados para o cálculo da reputação direta (RD). De forma semelhante ao que foi proposto em [Mello et al. 2009], o sistema de reputação calcula o valor esperado (VE) da distribuição beta para verificar a probabilidade de um determinado veículo honrar sua interação com outro veículo, conforme Equação (2).

$$RD_{(i,j)} = \left\{ \frac{\alpha}{\alpha + \beta} \right\} \tag{2}$$

Sendo *RD(i,j)*, o valor da reputação direta do veículo j (valor esperado do veículo *j* em honrar futuras interações) em relação ao veículo i. Tem-se que α representa o total de interações confirmadas + 1 e β representa o total de não confirmadas + 1 das interações entre *i* e *j*. Deve-se indicar que, ao iniciar o sistema de reputação a base de reputação é nula, por isso a distribuição beta é uniforme. O valor da reputação direta é definido como um número real no intervalo entre [0,1], sendo que 1 representa o grau mais alto de reputação. Para avaliar o nível de confiança em um veículo, o limiar de reputação é uma variável parametrizável do sistema.

Entretanto, em aplicações LDW para rodovias, observa-se que nem sempre é possível existir experiências diretas entre os veículos, neste caso, o RAMS+ irá calcular a Reputação Agregada. A reputação agregada calculada por um veículo *i* será uma média ponderada das reputações diretas informadas pelos veículos vizinhos, em relação ao valor de reputação (credibilidade) que o veículo *i* possui sobre estes veículos, conforme a Equação (3) e como proposto em [Mello et al., 2009].

$$RA\ (i,j) = \begin{cases} \dfrac{\sum(\mathrm{Cred}(a) * \mathrm{RD}(a,j))}{\Omega} & se\ \Omega\ \neq 0 \\ 0{,}5 & se\ \Omega = 0 \end{cases} \qquad Cred(a) = \begin{cases} RD\ (i,a) & se\ a\ \in BCI \\ 0{,}5 & se\ a\ \notin BCI \end{cases} \tag{3}$$

Sendo que *RA (i,j)* representa o valor de reputação agregada de i em relação a j dentro do intervalo de [0,1], *Cred(a)* representa a credibilidade que i possui sobre a. *RD (a,j)* representa a reputação direta de *j* calculada pelo nó *a*; e Ω representa a quantidade de nós testemunhas consultados. A relevância da *RA (i,j)* está fortemente relacionada a *Cred(a)*, pois a Equação (3) mostra que as opiniões recebidas por *i* serão ponderadas de

acordo com a credibilidade que *i* possui sobre os veículos que estão em sua BCI (nós conhecidos).

De posse dos valores da *RD* e *RA*, é possível calcular o valor da reputação global (*Rep*) de j do ponto de vista de i, pela Equação (4).

$$Rep(i,j) = \theta * RD(i,j) + (1-\theta) * RA(i,j) \quad (4)$$

Na Equação (4), θ é uma constante no intervalo entre [0,1] que indica a importância da reputação direta sobre a reputação indireta. Com o valor calculado através da Equação (3), caso a reputação esteja abaixo do limiar de reputação (e.g. 0,5), a mensagem recebida não será apresentada ao condutor e não será repassada aos demais veículos da rede (será descartada), pois esta foi gerada por uma fonte não confiável.

3.4 Lista de Reputação

Um veículo que se desloca pela rodovia, ao passar por uma *RSU*, deve transferir suas experiências passadas armazenadas em sua BCI através de uma mensagem *MenBCI*. Para definição de uma lista de reputação (LR) dos veículos que trafegam pela rodovia, as *RSUs* usam as BCIs dos veículos que passam por estas para calcular a reputação de cada um destes veículos. O sistema de reputação instalado nas RSUs possibilita calcular a reputação de provavelmente todos os nós que estão propagando mensagens de alertas na rodovia, tendo como base as experiências dos demais nós da rede, tornando possível uma rápida identificação de nós maliciosos.

Esta lista de reputação tem como conteúdo o ID do veículo, a data e hora em que cada reputação foi calculada, bem como o valor de reputação agregada do veículo entre o intervalo de [0-1]. O valor da reputação agregada (Rep(a)) calculado pela *RSU* para o veículo *a* é obtido conforme indicado na Equação 5.

$$\mathrm{Rep}_{(a)} = \left\{ \frac{\sum \mathrm{Conf\ BCI}_{(a)} + 1}{(\sum \mathrm{Conf\ BCI}_{(a)} + 1) + (\sum \mathrm{NConf\ BCI}_{(a)} + 1)} \right\} \quad (5)$$

Sendo que ∑ *Conf BCI(a)* representa o somatório de todos os campos confirmados armazenados nas BCIs dos veículos que passaram pela RSU e tiveram uma interação direta com *a*. ∑ *NConf BCI(a)* representa o somatório de todos os campos não confirmados armazenados nas BCIs dos veículos que passaram pela unidade de acostamento e tiveram uma interação direta com *a*. Por fim, o valor de 1 (um) é utilizado para que a base de informação não seja nula.

4. Avaliação do Sistema Proposto

Com o objetivo de avaliar o sistema de reputação proposto, foram realizadas simulações para verificar a eficácia do sistema e o impacto do uso deste sistema na eficiência da aplicação LDW (RAMS+). Nos experimentos, foram utilizados o simulador de redes OMNeT++ (*Objective Modular Network Tested in C++*) e o módulo INET *framework* para implementação do RAMS+ e do sistema de reputação. Com o objetivo de tornar as simulações mais realistas, foi utilizada a ferramenta geradora de cenários de mobilidade SUMO (*Simulation of Urban Mobility*) acoplada bidirecionalmente com o OMNeT++.

Os parâmetros do simulador de redes (OMNeT++/INET) foram definidos de acordo com o padrão IEEE 802.11g e com o *datasheet* do equipamento *Access Point Cisco Aironet 1260*. Tendo como base o trabalho de Ostermaier et al. (2007) e, após algumas análises empíricas, definiu-se como sendo de 500 metros o raio de alcance dos rádios dos veículos.

Nos experimentos, para a criação da via de circulação rodoviária utilizada no RAMS+, foi considerado um trecho real da rodovia BR-101. O trecho é composto por dois sentidos e duas faixas para cada sentido, tendo quatro faixas de rodagem no total, com uma velocidade máxima estipulada em 110 km/h para automóveis. Foram definidos cinco cenários de densidade de veículos (250, 500, 750, 1000 e 1250 veículos/900s)[2]. Estes fluxos simulam os tráfegos esparso, médio e denso. Cabe ressaltar que em todos os cenários, o tamanho da autoestrada é mantido em 5 km. Para a configuração dos veículos que circulam no trecho, foram definidas três classes: automóveis, caminhões e ônibus.

Em relação aos parâmetros do RAMS+, existem duas *RSUs* responsáveis pela propagação da lista de reputação. Uma está posicionada no quilômetro um e a outra no quilômetro três. Já as distâncias das áreas das regiões geográficas de reconhecimento, decisão e disseminação, são 50m, 300m e 3000m, respectivamente. Foi considerado para fins de simulação um evento dentro da área de reconhecimento (1.500m). Este evento indica a existência de óleo na pista.

Os parâmetros definidos para o sistema de reputação foram: limiar de proximidade (50m); limiar de reputação (0,5); peso da reputação (θ) = 0,6; e o tempo de espera para a consulta da reputação agregada feita aos nós vizinhos (500ms). Para obtenção dos resultados, foram realizadas cinco simulações para cada cenário de densidade e uma média aritmética simples dos resultados de cada cenário foi calculada. Todos os resultados obtidos nos experimentos possuem 95% de intervalo de confiança.

Para avaliar a eficácia do sistema de reputação, utilizou-se como métrica o percentual de falsos negativos, ou seja, taxa do número de nós que identificaram como sendo não malicioso um nó malicioso em relação ao número total de nós na rede veicular. Cabe salientar que a métrica de falsos positivos não foi considerada (veículo honesto considerado malicioso), pois este valor tende a ser zero mesmo diante de nós desconhecidos (abordagem otimista). A única maneira de ocorrerem falsos positivos é diante da formação de conluios. Ataques de conluio de nós maliciosos não foram simulados.

A fim de caracterizar a ação de um nó malicioso na rede, um alerta falso foi gerado por este veículo para verificar se o sistema de reputação é capaz de identificá-lo. Neste experimento, foram considerados quatro cenários. No primeiro cenário, o veículo malicioso, propaga um alerta falso, porém, no momento da propagação, este nó possui um bom valor de reputação perante os demais veículos da rede e também pelas *RSUs*. O valor de reputação deste veículo na Lista de Reputação é de 0,7. As BCIs dos demais veículos estão configuradas para que o valor da reputação seja de 0,7. No segundo cenário, o veículo malicioso é considerado não confiável e possui um valor de reputação de 0,4 tanto nas BCIs quanto na lista de reputação. No terceiro, o veículo malicioso é considerado confiável na Lista de Reputação, porém em 50% dos veículos, as BCIs estão configuradas para que a reputação seja 0,4 (não confiável). Por fim, no quarto cenário, o nó malicioso é desconhecido para os demais veículos da rede. Não há informações sobre este nem na LR e nem na BCI. Os resultados obtidos para o pior caso (densidade de veículos esparsa - 250

[2] Densidades para um tempo de 15 minutos (900s) de simulação. De acordo com a Polícia Rodoviária Federal, a densidade média em 15 minutos é de 625 veículos.

veículos) e para o melhor caso (densidade densa – 1250 veículos) encontram-se resumidos na Tabela 2. Tem-se que quanto menor a densidade, maior é a taxa de falsos negativos.

Conforme pode ser observado na Tabela 2, as taxas de falsos negativos do cenário 1 são as mais elevadas. Isto explica-se pelo fato do veículo malicioso possuir uma boa reputação na rede no momento da propagação do alerta e, consequentemente, necessitar de um tempo maior para o decaimento de sua reputação até que os demais veículos o considerem malicioso. No cenário 2, a taxa de falsos negativos foi 0. A razão decorre do fato de o veículo já ser considerado malicioso pelos demais nós. Desta maneira, após identificar o emissor, a mensagem de alerta falso foi imediatamente descartada e não foi repassada aos demais veículos. Observa-se no cenário 3 que as taxas de falsos negativos são menores que no 1, uma vez que alguns carros já possuem experiências negativas com o veículo malicioso e, devido à reputação agregada e a LR, este valor tende a baixar de 0,5 mais rapidamente ao longo da simulação. E, por fim, no cenário 4, pelo fato de não existir nenhuma informação a respeito do veículo malicioso, o valor da reputação foi de 0,5 (abordagem otimista), desta maneira o decaimento do valor de reputação do veículo malicioso, quando comparado ao cenário 1, é mais rápido.

Tabela 2: Resultados Obtidos – Percentual de Falsos Negativos

Cenários (variação da confiança no nó malicioso)	Falsos Negativos	
	Pior caso	Melhor caso
1. Nó malicioso considerado confiável	21,20%	10,24%
2. Nó malicioso considerado não confiável	0%	0%
3. Nó malicioso considerado parcialmente confiável	14,4%	6,48%
4. Nó malicioso, sem informações na LR e nas BCIs	17,20%	8,08%

Para avaliar os impactos decorrentes do uso do Sistema de Reputação na eficiência da aplicação RAMS+, foram consideradas as seguintes métricas: o total de veículos que receberam a mensagem de alerta, o número de colisões de pacotes na rede e o tempo para recebimento das mensagens, considerando duas situações: sem o sistema de reputação e com o sistema de reputação. Nestas simulações, considerou-se apenas o envio de alertas verdadeiros. Os resultados obtidos estão sintetizados nas Figuras 4 e 5.

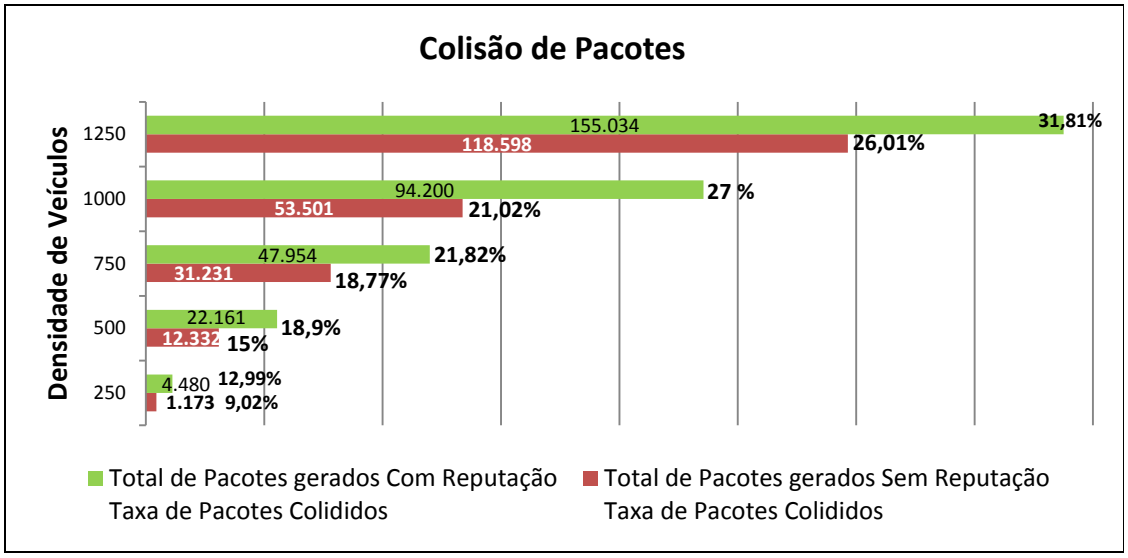


Figura 4: Total e Taxa de Pacotes Colididos

Conforme era esperado, o número de colisões de pacotes quando o sistema de reputação é utilizado é maior do que quando o sistema está desligado (ver Figura 4), já que

o número de mensagens com o sistema de reputação aumenta 30%. Porém, observa-se que o percentual de colisão em relação ao número total de colisões só é considerado alto (acima de 25%) quando a densidade de veículos é alta e acima da média da rodovia (625 veículos). Conforme ilustrado na Figura 5, há um impacto (pequeno) no número de carros que não receberam a mensagem de alerta quando o sistema é utilizado. Esta diminuição deve ser em razão das colisões de pacotes na rede e no atraso para reenvio dos alertas.

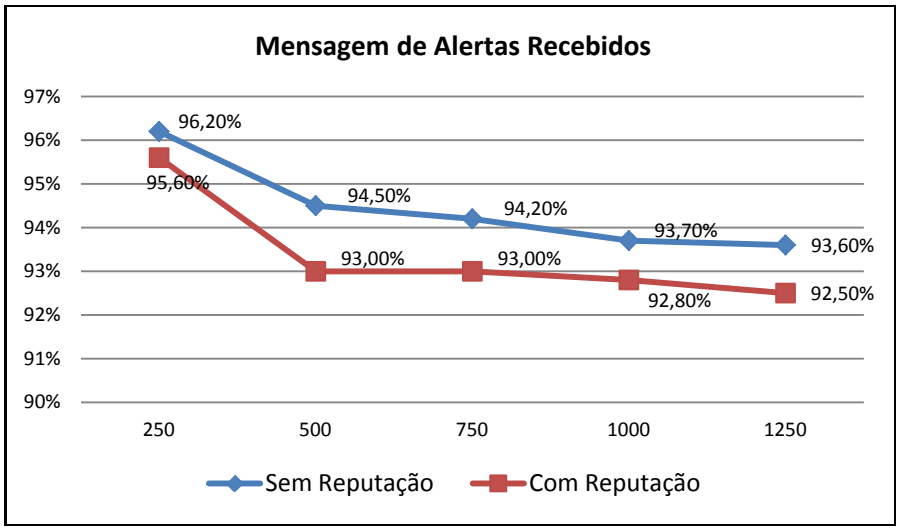


Figura 5: Taxa de Veículos que receberam o *MenAlert*

Em relação ao tempo após a criação do alerta até o recebimento deste pelos veículos participantes da rede, obteve-se no cenário para 2000 veículos/hora (ou 500 veículos em 15min de simulação), que 69% de veículos tiveram um tempo médio inferior a 10 ms, que 16% dos veículos tiveram um tempo médio inferior a 31ms e que 6% tiveram um tempo médio de 0,5s[3]. A degradação média do tempo quando comparado com o sistema que está desligado é de 18%. Observa-se que estes atrasos não prejudicam a tomada de decisão uma vez que o veículo que teve o maior atraso identificado estava a 1890 metros do evento, o que lhe permitiria diminuir a velocidade e até mesmo frear sem dificuldades.

5. Conclusão

Segurança pode ser considerado um fator crítico em qualquer tipo de rede, entretanto, em redes veiculares, devido as suas características e limitações, trata-se de uma questão ainda mais delicada. Ataques em redes VANETs, por exemplo, a transmissão de dados fraudulentos sobre congestionamento das estradas, pode ser bastante prejudicial.

O sistema de reputação proposto inova em relação aos trabalhos relacionados por ser descentralizado, otimista, global, direcionado as aplicações LDW e que visa identificar a reputação dos nós e não a credibilidade das mensagens (com o objetivo de descartar alertas falsos propagados por nós maliciosos), utilizando para isto diferentes técnicas. A primeira a ser usada é uma Lista de Reputação dos nós que trafegam na rodovia, calculada e propagada pelas *RSUs*. Estas listas são muito importantes para acelerar a divulgação de nós maliciosos na rede, em especial, diante de densidades esparsas. Além disso, quando os nós estão muito

[3] 9% dos veículos restantes não receberam o alerta.

próximos do local do evento, apenas esta técnica é utilizada para avaliar a confiança do nó emissor. Caso contrário, a reputação global do nó emissor pode ser calculada combinando a reputação direta (experiência do próprio nó) com a reputação agregada (experiência dos vizinhos). Um sistema de votação é utilizado para dar mais segurança ao processo de punição de nós maliciosos (baixar a reputação). Vale destacar que até mesmo a confiança de nós desconhecidos pode ser avaliada na solução proposta.

As simulações realizadas puderam comprovar a eficácia do sistema proposto. Em alguns cenários, o percentual de falsos negativos não é desprezível. Porém, a opção por uma abordagem otimista (sem falsos positivos) traz esta penalidade. Acredita-se também ser possível reduzir estes índices fazendo outras escolhas nos parâmetros configuráveis do sistema e até mesmo do rádio usado nas simulações, tornando o sistema ainda mais adaptativo. Apesar dos impactos na eficiência e eficácia do RAMS+ provocados pelo uso do sistema reputação, os prejuízos que podem vir a ser causados por nós maliciosos são imensamente maiores do que os impactos apresentados nas simulações, umas vez que, nos resultados das simulações, estes não impedem a reação dos motoristas em tempo hábil.

Referências

Daeinabi A. e Ghaffarpour R. A. (2011), "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks", In: Journal Multimedia Tools and Applications, Volume 66, p. 325–338.

Kosch, T. (2004), "Local danger warning based on vehicle ad hoc networks: Prototype and simulation", In: Proceedings of 1st International Workshop on Intelligent Transportation (WIT 2004).

Lee J. et al. (2008), "Vehicle local peer group based multicasting protocol for vehicle-tovehicle communications", In: The Fourth International Workshop on Vehicle-to-Vehicle Communications.

Li, Qin et al. (2012), "A Reputation-based Announcement Scheme for VANETs", In: Vehicular Technology, IEEE Transactions on, Volume 61, p. 4095-4108.

Lo, N. e Tsai, C. (2010), "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks", In: EURasiP Journal on Wireless Communications and Networking.

Mello, E. R. ; Fraga, J. S. ; Wangham, M. S. (2009) Uso de um modelo de confiança para a composição de Serviços Web. In: Simpósio Brasileiro de Redes de Computadores - SBRC.

Ostermaier B. et al. (2007), "Enhancing the security of local danger warnings in VANETs - a simulative analysis of voting schemes", In: Proceedings of ARES'07.

Paula, W.P. et al. (2010), "Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões", In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Gramado. SBRC, p. 545-550.

Raya, Maxim et al. (2005), "The security of vehicular ad hoc networks", In: Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN).

Wang, Z. e 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.

