Um algoritmo de reputação centralizado para redes veiculares contra ataques de inconsistência e bad-mouthing

Diego V. Natividade[1], **Luiz H. A. Correia**[1], **Aldri Santos**[2]

[1]Departamento de Ciência da Computação – Universidade Federal de Lavras (UFLA)
Caixa Postal 3037 – 37.200-900 – Lavras – MG – Brasil

[2]Departamento de Informática – Universidade Federal do Paraná (UFPR)
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brasil

natividade@bol.com.br, lcorreia@ufla.br, aldri@inf.ufpr.br

Abstract. *Attacks of inconsistency and bad-mouthing are disastrous for reputation services that support decisions on vehicular networks. The critical information exchange, such as traffic or traffic safety, should be reliable to avoid accidents and enable correct decision making. Reputation algorithms must react against attacks in the network and ensure credibility and accuracy in calculating the reputation of each vehicle. This paper proposes the reputation algorithm* `LETICIA` *(Lightweight and EfficienT Information exChange In Ad-hoc network) to mitigate attacks of the malicious vehicles in the network. Simulation results show that the* `LETICIA` *effectively reduced the reputation of the malicious vehicle against inconsistency attacks while maintaining the reputation of the vehicle honest against collusion attacks by bad-mouthing, when compared to the algorithms* `ARS`*,* `BYOR` *and* `BYOR-LF`*.*

Resumo. *Os ataques de inconsistência e bad-mouthing são desastrosos aos serviços reputação que apoiam decisões nas redes veiculares. A troca de informações críticas, como segurança de trânsito ou de tráfego, precisam ser confiáveis a fim de evitar acidentes, e possibilitar tomadas de decisão corretas. Os algoritmos de reputação devem reagir de modo eficaz contra ataques na rede, garantindo a credibilidade de cada veículo. Neste trabalho é proposto o algoritmo de reputação* `LETICIA` *(Lightweight and EfficienT Information exChange In Ad-hoc network) para mitigar ataques de veículos maliciosos na rede. Resultados de simulação mostram que o* `LETICIA` *reduziu efetivamente a reputação do veículo malicioso contra ataques de inconsistência, ao mesmo tempo que manteve a reputação do veículo honesto contra ataques de conluio por bad-mouthing, quando comparado aos algoritmos* `ARS`*,* `BYOR` *e* `BYOR-LF`*.*

1. INTRODUÇÃO

Os ataques para falsificação de dados durante a troca de mensagens entre os nós de uma rede ou de uma aplicação podem gerar consequências desastrosas [Pedroso et al. 2019, Su et al. 2020]. Em algumas aplicações a informação trocada entre os nós é crítica, como por exemplo, informações das condições de tráfego ou de segurança de trânsito nas redes veiculares. O envio de informações falsas nesse tipo de rede pode causar acidentes, desviar o motorista de sua rota, criar falsas situações de engarrafamento e também qualificar um veículo da rede de forma desleal ou imprecisa. É essencial que os nós de uma rede

tenham confiança nas informações trocadas com seus vizinhos. Os sistemas de reputação visam estabelecer a confiança e dar credibilidade às informações trocadas entre os nós da rede. Segundo [Engoulou et al. 2019], reputação refere-se às observações do comportamento passado de uma entidade, que podem indicar um comportamento futuro da mesma. Entidades que têm um histórico de bom comportamento, tendem a permanecer com bom comportamento. O mesmo pode ser dito para indivíduos com mal comportamento. Esse mesmo conceito por ser aplicado às redes veiculares, por exemplo, para que um veículo decida se deve ou não confiar nas informações enviadas por um veículo desconhecido, pode-se utilizar a reputação dele como parâmetro de comportamento.

Os sistemas de reputação são normalmente centralizados, isto é, quando há uma entidade central que computa e controla a reputação dos participantes, e distribuídos, quando os próprios participantes armazenam e distribuem suas opiniões sobre os outros, sem que haja uma entidade controladora [Jøsang et al. 2007]. Contudo, para [Su et al. 2020], esses sistemas podem ainda ser (a) centrado na entidade, quando as reputações refletem o comportamento das entidades que enviam as mensagens na rede; ou (b) centrado na mensagem, quando as mensagens encaminhadas é que levam a reputação independente da entidade que as criou. A reputação de uma certa entidade é dada por opiniões ou *feedbacks* emitidas por outras entidades com as quais teve contato anterior. Estes *feedbacks* são posteriormente agregados e um valor de reputação é calculado para cada entidade. Esse valor pode ser expresso em binário, em intervalos (0 a 1 ou -1 a 1), por um número inteiro positivo, ou mesmo de forma textual como ruim/regular/bom/ótimo [Ruohomaa et al. 2007].

As aplicações de segurança de trânsito nas redes veiculares trocam mensagens críticas entre os dispositivos da rede. Essa troca de mensagens críticas deve ser confiável, segura e resiliente a ataques, e os veículos que participam da comunicação devem ser confiáveis. Muitos tipos de ataques contra reputação e integridade são executados por veículos maliciosos nas redes veiculares, sendo os mais conhecidos Bogus, Sybil, Newcomer, Betrayal, Inconsistência, Bad-mouthing e Conluio [Hasrouny et al. 2017, RoselinMary et al. 2013, Trček 2017, Zhang 2011, Banković et al. 2011]. Um sistema de reputação robusto para redes veiculares deve ser capaz, tanto de julgar os veículos envolvidos na comunicação, quanto reagir a possíveis ataques, reduzindo a reputação de veículos maliciosos para mitigar seus efeitos. Aplicações críticas em VANET devem punir drasticamente veículos maliciosos e incrementar de forma ponderada a sua reputação. Os atuais sistemas encontrados na literatura reduzem suavemente a reputação do veículo malicioso e ainda permitem a sua rápida recuperação. Muitos desses trabalhos falham por não apresentarem simulações ou experimentos, não avaliarem a rede sob ataques maliciosos, ou avaliarem esses sistemas com um número reduzido de veículos.

Este trabalho apresenta `LETICIA` (*Lightweight and EfficienT Information exChange In Ad-hoc network*), um novo algoritmo de reputação para redes veiculares desenvolvido para mitigar ataques de inconsistência e conluio por *bad-mouthing*. `LETICIA` foi desenvolvido para um sistema de reputação centralizado, baseado na entidade. Este algoritmo mesmo voltado para as redes veiculares, pode ser empregado em vários tipos de aplicações, como reputação de vendas em sites de comércio eletrônico, comunidades de aconselhamento, redes P2P, redes ad hoc e redes de sensores sem fio. Para avaliar e comparar os algoritmos de reputação utilizados nas redes veiculares, foi desenvolvido

o *framework* RVV (Reputação de Veículos em VANET). Este *framework* possibilita a criação de uma rede veicular, na qual apenas um veículo envia uma mensagem por vez, e os demais veículos enviam seus *feedbacks* de avaliação da mensagem recebida para um servidor central, que agrega e calcula a reputação do veículo emissor. O servidor é capaz de reputar os veículos da rede pela troca de mensagens e envio de *feedbacks*. O RVV possibilita a implementação de forma modular de vários algoritmos de reputação e permite avaliar ataques de inconsistência e conluio por *bad-mouthing* e suas variações.

Este artigo está organizado como descrito a seguir. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve as características e funcionalidades do *framework RVV*. A Seção 4 descreve o algoritmo LETICIA, resiliente a ataques de inconsistência e de conluio por *bad-mouthing*. Na Seção 5 o algoritmo LETICIA é avaliado e comparado com outros algoritmos da literatura. Finalmente, a Seção 6 apresenta as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

A literatura tem revelado diferentes abordagens ao gerenciamento da reputação em redes veiculares. Muitas propostas apresentam sistemas de reputação para avaliar a confiabilidade das mensagens ou dos veículos, afim de de mitigar os efeitos da disseminação de mensagens falsas ou de ataques na rede. As abordagens são diversas, como o desenvolvimento de *frameworks* que fazem a assinatura digital de mensagens, coletam opiniões dos veículos sobre outros, calculam e disseminam informações sobre a reputação dos veículos na rede e outras, que avaliam os sistemas de reputação contra ataques maliciosos na rede.

Um dos trabalhos pioneiros sobre sistemas de reputação em VANETs foi proposto em [Dotzer et al. 2005]. Os autores desenvolveram o VARS (*Vehicle Ad-hoc network Reputation System*), que usa opiniões diretas e indiretas sobre as mensagens enviadas. As opiniões sobre a confiabilidade de uma mensagem são anexadas pelos veículos durante o seu encaminhamento, sendo que a reputação do remetente interfere nessas opiniões.O veículo avalia as opiniões e decide se aceita ou não a mensagem. O VARS foi avaliado somente para ataques básicos, como modificação ou exclusão de mensagens por nós não autorizados na rede. Os autores comentam que o sistema pode ser suscetível a ataques mais sofisticados como o ataque de conluio. Os autores [Li et al. 2013] propuseram o RGTE (*Reputation-Based Global Trust Establishment)*, onde os nós de uma rede veicular informam ao centro de gerenciamento de reputação sobre a confiança que possuem nos outros veículos. A solução compartilha informações de reputação baseado na correlação de atributos dos veículos. As reputações são armazenadas em um tabela que mantém por um período de vida a reputação que um veículo possui sobre outro veículo. Em veículos com bom comportamento a reputação é aumentada lentamente, enquanto que diminui rapidamente para veículos com mal comportamento. Os veículos não recebem as recomendações de confiança diretamente dos demais, mas através da central de reputação. Apesar dos autores afirmarem que o RGTE é eficiente contra ataques de reputação, nenhum experimento foi realizado para comprovação.

O ARS (*Anonymous Reputation System for Vehicular Ad hoc Networks*) é um sistema de reputação no qual os veículos que geram e encaminham as mensagens são avaliados por um servidor de reputação centralizado [Jaimes et al. 2016]. Nas mensagens são anexados os pseudônimos do veículo que as criou e dos veículos que encaminharam

a mensagem. Resultados mostram que o ARS reduz a disseminação de mensagens falsas na rede. Entretanto, o sistema não foi avaliado contra nenhum tipo de ataque na rede. Em [Mühlbauer and Kleinschmidt 2018], os autores propuseram o BYOR (*Bring Your Own Reputation*), um sistema de reputação para redes veiculares. No BYOR os veículos recebem sua reputação assinada digitalmente quando estão dentro da área de cobertura da infraestrutura (RSU - *Road Side Unit*). O sistema opera de maneira parcialmente descentralizada, onde o contato com a RSU não precisa ser permanente para operar, mas apenas esporádico. A RSU também aborda a questão da privacidade do veículo por meio de certificados digitais de curto prazo, nos quais todas as mensagens enviadas são assinadas digitalmente. Para o cálculo da reputação, os autores usaram um algoritmo de soma simples dos *feedbacks* recebidos e um algoritmo de inferência Baysiana. O último ainda conta com uma variação utilizando um fator de longevidade `f`. Este fator define que somente os `f` últimos *feedbacks* serão armazenados para o cálculo da reputação. Entretanto, os autores avaliaram seus algoritmos em simulações com um número limitado de veículos e, embora tenham afirmado que o modelo seja robusto contra ataques de *bad-mouthing*, não avaliaram este tipo de ataque.

Um esquema de gerenciamento de reputação para identificação de veículos maliciosos em VANET foi apresentado em [Su et al. 2020]. A proposta do IDES (*Instant Data Evaluation Scheme)* é coletar a reputação global de veículos e possibilitar o reconhecimento instantâneo de mensagens não confiáveis. Os autores pressupõem que a comunicação fim-a-fim entre veículos seja provida por uma rede 5G de alto desempenho. O sistema de reputação é centralizado e a decisão sobre a confiança nos dados recebidos de um veículo é tomada de acordo com a reputação do veículo que gerou os dados. A reputação do veículo emissor é atualizada de acordo com a validação dos dados do veículo receptor. Um emulador auto-desenvolvido avaliou o comportamento do IDES na presença de ataques maliciosos nos modos de disseminação de mensagens falsas (*Bogus e Secret*) e conluio. O IDES foi comparado somente ao *framework* HTMF (*Hybrid Trust Management Framework*) criado para redes sociais veiculares [Hussain et al. 2016].

3. *Framework* para avaliação de reputação em VANET

O *framework* `RVV` (Reputação de Veículos em VANETs) foi desenvolvido para avaliar e calcular a reputação de veículos por meio de opiniões ou troca de mensagens na rede. Ele foi escrito e implementado em linguagem C++ e Python, sendo auto-desenvolvido como em [Su et al. 2020], para avaliar algoritmos de reputação contra ataques maliciosos nas redes veiculares. O *framework* simula uma rede com vários veículos, na qual apenas um veículo envia mensagens por vez e os demais opinam sobre a mensagem recebida. No RVV o sistema de reputação é centralizado, as opiniões são chamadas de *feedbacks* da mensagem recebida e são enviadas ao servidor `CACR` (Centro de Agregação e Computação de Reputação). Um veículo que recebe uma mensagem de outro, envia um *feedback* positivo ou negativo, de acordo com a veracidade da mensagem, ou com seu comportamento na rede. O `CACR` é responsável por agregar, processar e distribuir as reputações dos veículos de acordo com os *feedbacks* recebidos de outros veículos.

A implementação atual do *framework* `RVV` é capaz de lidar com dois tipos de ataques: ataques de inconsistência, ilustrado na Figura 1, e os ataques de conluio por *bad-mouthing*, ilustrado na Figura 2. Esses ataques foram divididos em subgrupos, utilizando uma taxonomia definida pelos autores, a fim de categorizá-los, como descrito a seguir.

Ataque de inconsistência: um atacante se comporta de forma instável, enviando mensagens verdadeiras e falsas alternadamente, comprometendo assim o funcionamento da rede [Zhang 2011]. Na Figura 1, o veículo vermelho (`A`) realiza o ataque de inconsistência ao enviar mensagens na rede ora verdadeiras ora falsas. Já os veículos verdes que opinam (`1..n`), sempre emitem um *feedback* fidedigno, isto é, *feedback* positivo para mensagens verdadeiras e *feedback* negativo para mensagens falsas. Os subgrupos para o ataque de inconsistência são:

(i) **ataque de inconsistência bipolar**: o veículo envia uma mensagem positiva e uma negativa, alternadamente;

(ii) **ataque de inconsistência restrito**: o veículo envia mensagens verdadeiras e falsas a uma taxa fixa, por exemplo, envia dez mensagens verdadeiras e dez falsas, repetindo este comportamento até o final da simulação;

(iii) **ataque de inconsistência distribuído**: durante toda a simulação, o veículo malicioso tem uma probabilidade de enviar mensagens falsas, por exemplo, de todas as mensagens enviadas na simulação 30% são falsas.

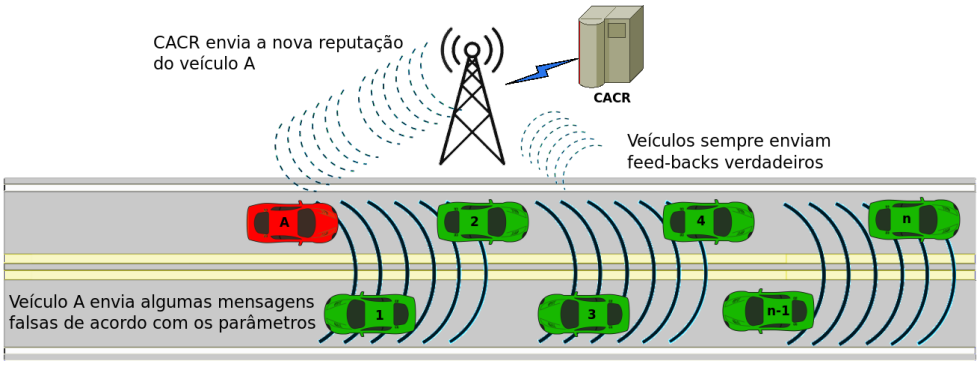


Figura 1. Comportamento do ataque de inconsistência

Ataques de conluio por *bad-mouthing*: os atacantes maliciosos agem em grupo e arbitrariamente emitem um *feedback* positivo ou negativo sobre um veículo na rede, a fim de alterar sua reputação, tal que os outros veículos tomem decisões incorretas a seu respeito [Banković et al. 2011]. No ataque mostrado na Figura 2, o veículo azul (`A`) que envia mensagens na rede, sempre o faz de forma idônea, isto é, sempre envia mensagens verdadeiras na rede. Já os veículos que opinam (`1..n`), são quem fazem os ataques contra a reputação do veículo que enviou a mensagem, ora opinando positivamente (verde) ora negativamente (vermelho). Os subgrupos para esses ataques são:

(i) **ataques de conluio por *bad-mouthing* restrito**: os veículos que possuem uma certa reputação, abaixo da taxa especificada, sempre enviam *feedbacks* negativos, por exemplo: veículos com reputação abaixo de 0,3 sempre enviam *feedbacks* negativos;

(ii) **ataques de conluio por *bad-mouthing* distribuído**: neste ataque durante toda a simulação, os veículos que opinam têm uma probabilidade de enviar *feedbacks* negativos incorretamente, por exemplo: de todos os veículos que opinam, 20% o fazem de forma incorreta, isto é, enviando *feedbacks* negativos.

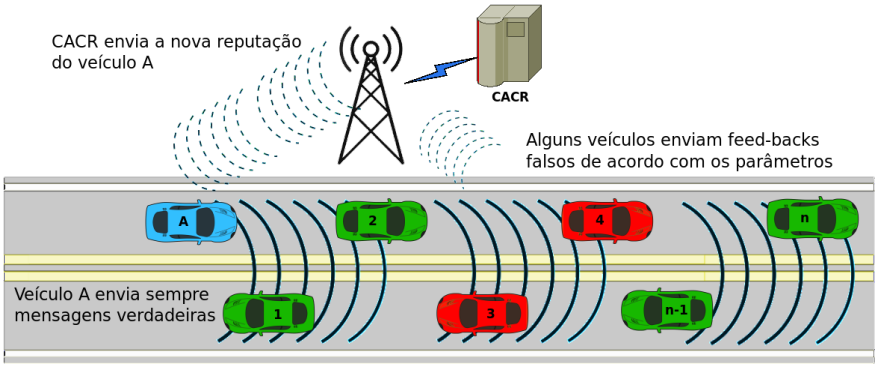


Figura 2. Operação do ataque de conluio por bad-mouthing

As simulações no RVV são realizadas em três etapas, como mostrado na Figura 3. Na etapa de Configuração, deve-se escolher os algoritmos que serão comparados, os tipos de ataques, os parâmetros de reputação, a porcentagem de veículos atacantes e a probabilidade de ataques. A definição do cenário com a quantidade de veículos honestos e atacantes e o número de iterações da simulação também são definidos na etapa de Configuração. Em seguida, inicia-se a fase de Execução dos testes propriamente ditos. Nesta fase um veículo escolhido (A) inicia com a reputação recebida dos parâmetros da simulação. Os demais veículos recebem uma reputação aleatória. O veículo A, então envia uma mensagem e os demais recebem e emitem seus *feedbacks* para o CACR, que agrega os *feedbacks* recebidos, calcula a nova reputação e a entrega para o veículo A. Este ciclo se repete por um número de vezes definidos nos parâmetros recebidos na etapa de Configuração, para cada algoritmo de reputação selecionado.

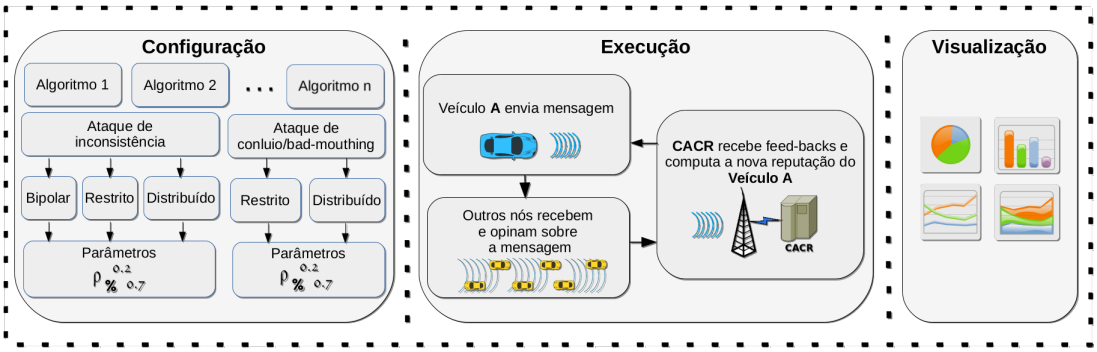


Figura 3. Arquitetura do Framework: componentes e interação

Vários arquivos de *log* são gerados contendo a nova reputação do veículo A coletada a cada iteração, para enfim serem lidos e plotados em um gráfico na etapa de Visualização. Todos os algoritmos selecionados são mostrados em um mesmo gráfico, e com o nível de confiança selecionado. O objetivo do gráfico é apresentar uma visão geral da reputação do veículo A ao longo do tempo, para cada um dos algoritmos de reputação testados. Com isso, a reputação do veículo A aumenta ou diminui, conforme seu comportamento em caso de ataque de inconsistência, ou de acordo com o comportamento dos demais veículos da rede no caso de ataque de conluio por *bad-mouthing*. A reputação dos veículos é definida pelo parâmetro ρ, tal que $\{\rho \in \mathbb{R}; 0 < \rho < 1\}$, e quanto mais próximo de 0, menor a reputação e quanto mais próximo de 1, maior.

O *framework* RVV atualmente inclui a implementação de alguns algoritmos utilizados em sistemas de reputação para redes veiculares, como o ARS [Jaimes et al. 2016], o BYOR e sua variação [Mühlbauer and Kleinschmidt 2018], além do algoritmo proposto LETICIA. Devido a modularidade do *framework* RVV, outros algoritmos de reputação também podem ser incluídos.

4. Algoritmo de reputação contra falsificação de dados em VANET

O algoritmo LETICIA - *Lightweight and EfficienT Information exChange In Ad-hoc network* - foi desenvolvido para avaliar a reputação dos veículos que trocam mensagens na VANET. O algoritmo proposto reduz drasticamente a reputação de um veículo que esteja enviando mensagens falsas na rede, e aumenta gradativamente a sua reputação quando envia mensagens verdadeiras. Esta estratégia visa reduzir os ataques de inconsistência, evitando que o veículo aumente rapidamente a sua reputação. Para o cálculo da reputação são levados em conta as opiniões ou *feedbacks* dos veículos e o tempo decorrido entre o envio da mensagem e entrega dos *feedbacks* para o servidor.

O CACR agrega e armazena as opiniões emitidas sobre cada veículo em dois contadores de *feedback*: um para contar as reputações positivas e outro para as reputações negativas. Cada *feedback* recebido, seja positivo ou negativo é calculado de acordo com a Equação 1. A Tabela 1, exibe todas as variáveis utilizadas nos cálculos de agregação de *feedbacks* e reputação dos veículos no algoritmo LETICIA.

$$\begin{cases} F^{+} = \sum_{i=1}^{m} \frac{\rho_{fb_i} + (1 - \frac{T_{fb_i}}{\epsilon})}{2} \\ F^{-} = \sum_{i=1}^{n} \frac{\rho_{fb_i} + (1 - \frac{T_{fb_i}}{\epsilon})}{2} \end{cases} \tag{1}$$

Nesta equação, F^{+} é o contador que recebe o somatório de *feedbacks* positivos e F^{-} é o que recebe o somatório de negativos. ρ_{fb_i} é a reputação do veículo que enviou o *feedback*, T_{fb_i} é o tempo desde a criação da mensagem e o momento em que a mesma foi recebida pelo veículo que enviou o *feedback* e ϵ é tempo limite de duração de uma mensagem.

Tabela 1. Variáveis utilizadas nos cálculos do algoritmo LETICIA

Variável	Descrição
F^{+}	somatório de *feedbacks* positivos
F^{-}	somatório de *feedbacks* negativos
m	número de veículos que enviaram *feed-backs* positivos
n	número de veículos que enviaram *feed-backs* negativos
ρ_{fb_i}	reputação do veículo que enviou *feedback*
T_{fb_i}	tempo da mensagem em relação ao veículo que enviou *feedback* (em segundos)
ϵ	tempo limite de uma mensagem na rede
A_{fb}	*feedbacks* agregados
α	*feedbacks* positivos + 1
β	*feedbacks* negativos + 1
ρ_0	reputação antiga do veículo avaliado
ρ	nova reputação do veículo avaliado

O cálculo de agregação dos *feedbacks* é dado pela Equação 2, que utiliza a função de distribuição de Probabilidade Beta, como em [Cervantes et al. 2014]. A_{fb} é a agregação dos *feedbacks* positivos e negativos, α é o somatório dos *feedbacks* positivos (F^+) + 1 e β, os negativos (F^-) + 1.

$$A_{fb} = \frac{\alpha}{(\alpha + \beta)} \tag{2}$$

Quando a agregação dos *feed-backs* (A_{fb}) recebidos é maior que 0,5, a função de probabilidade beta é dada pela Equação 2. Esse valor (A_{fb}) indica que, naquela iteração, a maioria das opiniões sobre o veículo foi positiva e que o valor da sua reputação deve incrementar, como mostra a Equação 3. Esse incremento é amortizado por um fator quadrático que eleva suavemente a reputação do veículo.

$$\rho = \rho_0 + \rho_0 * A_{fb} - {\rho_0}^2 * A_{fb} \tag{3}$$

Se a agregação dos *feed-backs* é menor ou igual a 0,5, o valor de A_{fb} indica que a maioria das opiniões sobre o veículo foi negativa e que seu valor da sua reputação deve ser drasticamente reduzido, dado pela Equação 4. Essa redução é extrema uma vez que além da dependência do cálculo dos valores da reputação anterior e do valor da agregação, o valor ainda é reduzido pela metade.

$$\rho = \frac{\rho_0 + \rho_0 * A_{fb}}{2} \tag{4}$$

5. Avaliação e Resultados

Esta seção avalia a reputação dos veículos de uma rede veicular que sofre ataques de inconsistência, conluio por *bad-mouthing* e suas variações. São avaliados e comparados os algoritmos `ARS`, `BYOR`, `BYOR-LF` e `LETICIA` quanto à influência dos ataques no cálculo da reputação do veículo honesto. O simulador auto-desenvolvido, `RVV`, foi utilizado para gerar a rede veicular, adicionar os módulos com os algoritmos de reputação, prover os veículos atacantes na rede e apresentar como resultado o comportamento dos algoritmos na presença de ataques efetuados na rede.

Tabela 2. Equações dos algoritmos

Algoritmo	**Equação**
`ARS`	$a = 0,8$ $\rho = \rho_0 * (1 - a) + (F^+ + F^-) * a$
`BYOR`	$\alpha = F^+;\ \beta = F^-$ $\rho = \alpha/(\alpha + \beta)$
`BYOR-LF`	$f = 25$ $\alpha = F^+;\ \beta = F^-$ $\alpha = F(\alpha, f);\ \beta = F(\beta, f)$ $\rho = \alpha/(\alpha + \beta)$
`LETICIA`	$\alpha = F^+;\ \beta = F^-; r = \alpha/(\alpha + \beta)$ se $r > 0,5 \rightarrow \rho = \rho_0 + \rho_0 * r - {\rho_0}^2 * r$ se $r \leq 0,5 \rightarrow \rho = (\rho_0 + \rho_0 * r)/2$

O cenário de simulação foi configurado para uma rede com 50 veículos que enviam *feedbacks* para cada uma das 100 mensagens enviadas pelo veículo que está sendo avaliado. O veículo avaliado inicia a simulação com uma reputação de $0,6$. Cada algoritmo é testado 100 vezes com sementes diferentes, para o cálculo de intervalo de confiança. A reputação dos veículos que emitem opinião é aleatória, variando no intervalo de $0,1$ a $0,99$. O tempo da mensagem é gerado aleatoriamente entre 0 e 600 segundos. Todos esses valores são parametrizáveis. As Tabela 2 e 3 apresentam as equações dos algoritmos e sumarizam a configuração das simulações, respectivamente.

Tabela 3. Parâmetros da simulação

Parâmetros	**Valor**
Número de veículos	50
Mensagens enviadas	100
Repetição de cada teste	100
Nível de confiança	95%
Reputação inicial do veículo	$0,6$
Reputações (aleatórias)	de $0,1$ a $0,99$
Tempos de mensagens	de 0 a 600

5.1. Ataques de Inconsistência

Os algoritmos de reputação foram avaliados no *framework* RVV contra ataques de inconsistência, no qual um atacante alterna enviando mensagens verdadeiras e falsas para os veículos da rede. Foram avaliados os subgrupos de ataques de inconsistência bipolar, restrito e distribuído.

Ataque de inconsistência bipolar: neste ataque um veículo da rede envia alternadamente mensagens verdadeiras e falsas para os veículos da rede. A Figura 4, apresenta os resultados das simulações para o ataque de Inconsistência Bipolar. O algoritmo `ARS` foi o mais instável variando a reputação do veículo malicioso entre 0,15 a 0,85, sendo classificada como ora "boa"(acima de 0,60) e ora "ruim", seguindo o comportamento do atacante. Os `BYOR` e `BYOR-LF` tiveram comportamentos semelhantes, a reputação do veículo ficou estabilizada em 0,50 após a quinta iteração. Apesar desses algoritmos reputarem o veículo negativamente, eles reagiram de modo complacente com os ataques e não reduziram a reputação do veículos à medida que o número de iterações aumentaram. O `LETICIA` reputou o veículo malicioso negativamente, reagindo mais rapidamente contra o ataque e reduzindo sua reputação à medida que o número de iterações aumentou.

Ataque de inconsistência restrito: para este ataque o veículo malicioso alterna o envio de mensagens verdadeiras e falsas a uma taxa fixa. Nesta simulação para um total de 100 mensagens, o veículo malicioso enviou 10% ou 20% de mensagens falsas, seguido de 10% ou 20% de mensagens verdadeiras, repetindo este comportamento até o final da simulação. A Figura 5 mostra o resultado do ataque de Inconsistência Restrito para todos os algoritmos. O `ARS` segue o comportamento do veículo atacante alternando entre as reputações negativas e positivas de acordo a taxa de envio de mensagens falsas. Os `BYOR` e `BYOR-LF` tiveram comportamentos similares para as duas taxas, reputando negativamente o veículo malicioso próximo a 20ª iteração. Para um percentual de 10%, tem-se

uma clara visão de que o LETICIA mantém a reputação do veículo abaixo dos demais com pequenos picos de recuperação, mas em seguida cai novamente chegando próximo a zero. Já com 20%, o veículo apresenta picos mais elevados, mas se mantém com uma reputação relativamente alta por pouco tempo em relação aos demais algoritmos, permanecendo a maior parte do tempo com a reputação próxima a zero, o que é desejável.

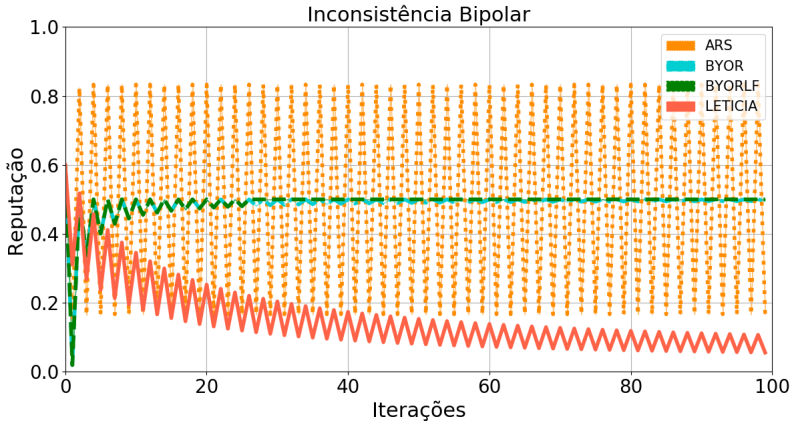


Figura 4. Ataque de Inconsistência Bipolar, com o veículo alternando entre mensagens verdadeiras e falsas

Ataque de inconsistência distribuído: Para simular este ataque o veículo malicioso envia mensagens falsas de maneira probabilística, seguindo uma distribuição de 10%, 30%, 60% e 70%. A Figura 6 apresenta os resultados da simulação para todos os algoritmos. Para a distribuição de 10%, os resultados são semelhantes para o LETICIA, ARS e BYOR, que mantém a reputação do veículo malicioso a uma média de 0,90. Entretanto, o BYOR−LF consegue reduzir a reputação mais drasticamente para aproximadamente 0,70 ao final de 100 iterações. Já para a distribuição de 30% de mensagens falsas, o LETICIA reputou negativamente o veículo malicioso mais rapidamente em relação aos demais, exceto do BYOR−LF que atinge um reputação abaixo de 50%, contra os 65% do LETICIA. Entretanto, nos testes de inconsistência, com taxas mais altas de envio de mensagens falsas, o LETICIA obteve os melhores resultados, como mostrado nos gráficos de 60% e 70%. Como pode ser observado, no ataque com 70% de mensagens falsas, LETICIA mantém a reputação do veículo malicioso próximo a zero, contra 0,30 dos demais.

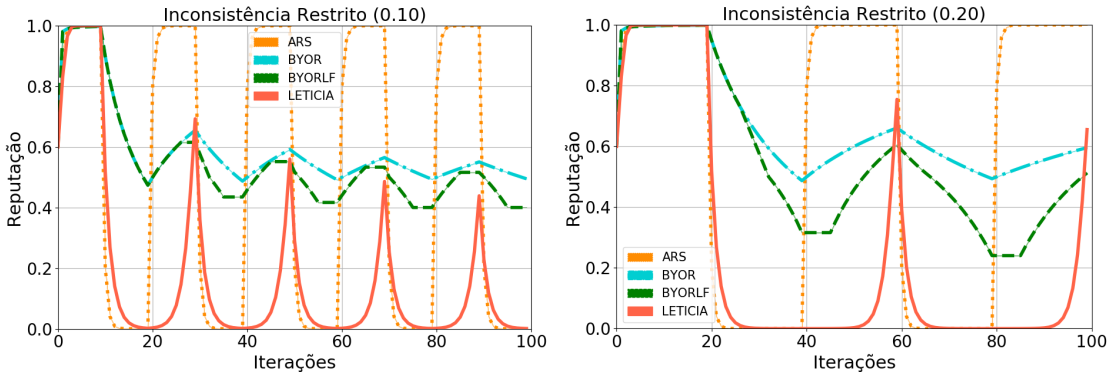


Figura 5. Ataque de Inconsistência Restrito com o veículo atacando em 10% e 20% do tempo de forma alternada, respectivamente

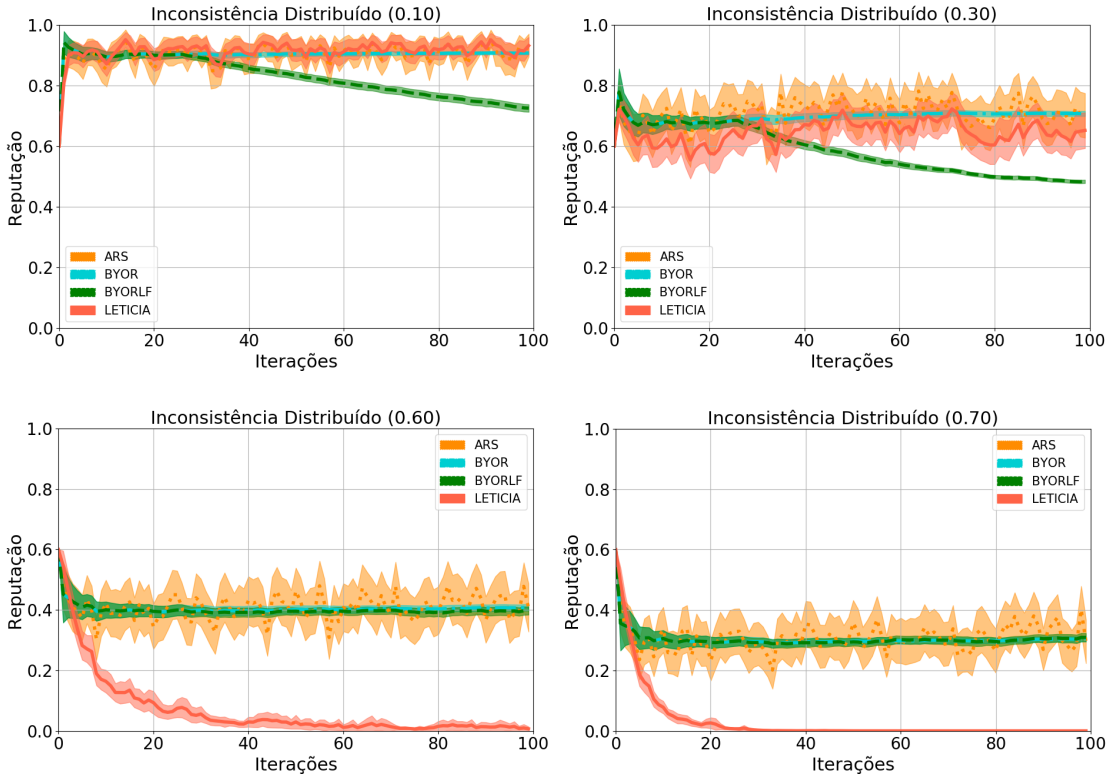


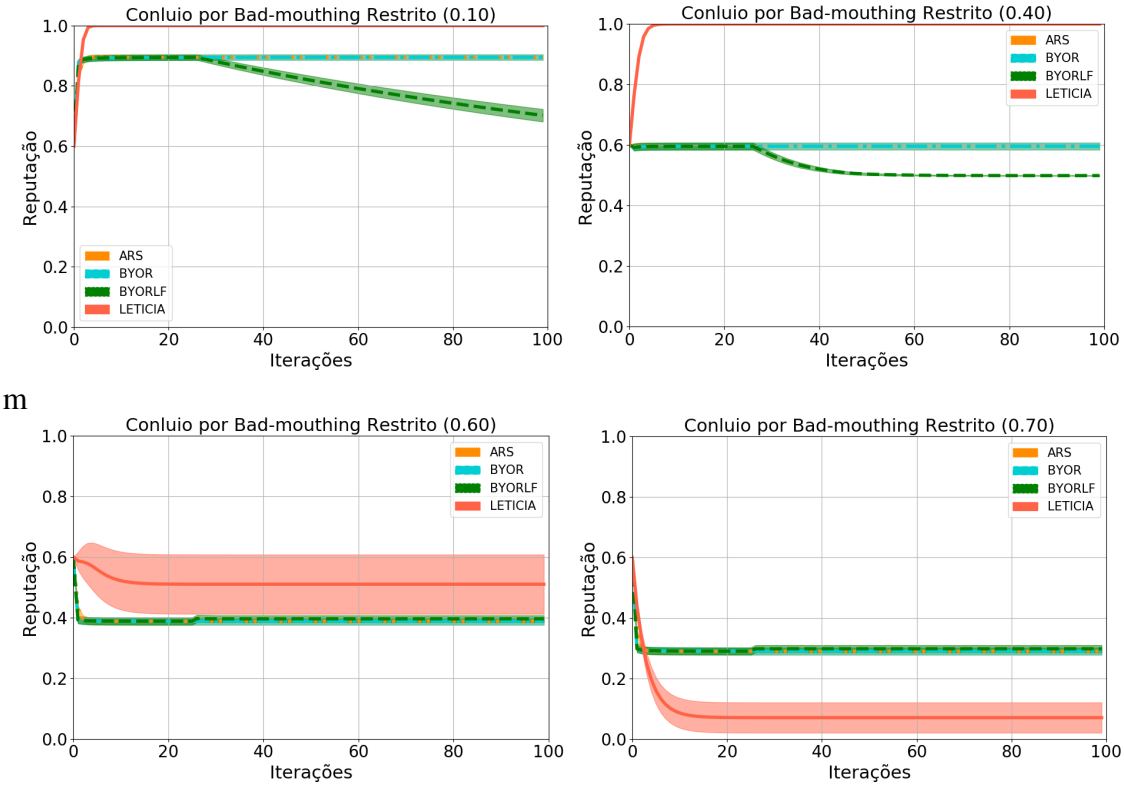
Figura 6. Ataque de Inconsistência Distribuído com o veículo enviando mensagens falsas em 10%, 30%, 60% e 70% do tempo, respectivamente

5.2. Ataques de Conluio por *bad-mouthing*

Os algoritmos de reputação foram avaliados na presença de ataques de Conluio por *bad-mouthing*. Neste tipo de ataque os veículos maliciosos se agrupam para manipular a reputação de um determinado veículo na rede. A consequência é que os outros veículos da rede avaliam de forma errada o veículo atacado, subestimando sua reputação. Foram avaliados os subgrupos de ataques de conluio por *bad-mouthing* restrito e distribuído.

Ataque de conluio por *bad-mouthing* restrito: Neste ataque os veículos da rede com reputações de 0,10; 0,40; 0,60 e 0,70 se agrupam enviando *feedbacks* negativos de um veículo honesto. Para veículos com reputações de 0,10 e 0,40, o algoritmo `LETICIA` manteve a reputação positiva do veículo avaliado próximo a 1,00, contornando o ataque de conluio por *bad-mouthing*. Os algoritmos `ARS` e `BYOR` mantiveram a reputação do veículo abaixo do `LETICIA`. O algoritmo `BYOR-LF` obteve o pior resultado, sendo totalmente afetado pelo ataque. Na simulação com veículos atacantes com reputação de 0,60, os algoritmos `ARS`, `BYOR` e `BYOR-LF` mantêm a reputação do veículo honesto em torno de 0,40, enquanto o `LETICIA` mantém em média a reputação acima dos 0,50. Já nas simulações com veículos com reputação de 0,70, o `LETICIA` não consegue manter a reputação do veículo honesto, caindo drasticamente, como pode ser visto no gráfico. Para os ataques de conluio por *bad-mouthing* restrito com veículos com reputação acima de 0,70, todos os algoritmos foram afetados pelo ataque, uma vez que trata-se de um ataque em que a maioria dos veículos reputam negativamente o veículo honesto.

Ataque de conluio por *bad-mouthing* distribuído: Neste ataque os veículos se agrupam, independentemente de suas reputações e enviam de forma incorreta *feed-bakcs* negativos seguindo uma taxa de distribuição de probabilidades de 10%, 30%, 40% ou 50%. A Figura 8 mostra o resultado do ataque de Conluio por *Bad-mouthing* Distribuído para todos os algoritmos. Para as simulações com taxas de 10% e 30 % os algoritmos mantiveram a reputação do veículo honesto próximo a 0,90 e 0,70, respectivamente. O `LETICIA` manteve a reputação do veículo honesto próximo de 1,00, enquanto que o `BYOR-LF` reduziu a reputação do veículo honesto, a partir da iteração 30 para as taxas de 10% e 30%.



m

Figura 7. Ataque de Conluio por *Bad-mouthing* Restrito com veículos com 0,1, 0,4, 0,5 e 0,6 de reputação fazendo ataques, respectivamente

Para a taxa de distribuição de 60%, os algoritmos `ARS` e `BYOR`, mantiveram a reputação do veículo honesto em 0,60. O `BYOR-LF` reduziu a reputação do veículo honesto para próximo de 0,50, enquanto o `LETICIA` manteve a reputação do veículo honesto próximo de 0,90. Todos os algoritmos na taxa de 70% reduziram a reputação do veículo honesto para próximo de 0,50. A exceção foi o algoritmo `LETICIA` que reduziu a reputação do veículo honesto para valores inferiores aos outros algoritmos, abaixo de 0,40. Isso é justificado, uma vez que, mais da metade dos veículos da rede são atacantes e este comportamento condiz com o esperado. Neste trabalho assumimos que a maioria dos veículos da rede veicular é honesta. Essa hipótese tem sido utilizada para as VANET e divulgado amplamente na literatura atual [Ghaleb et al. 2019].

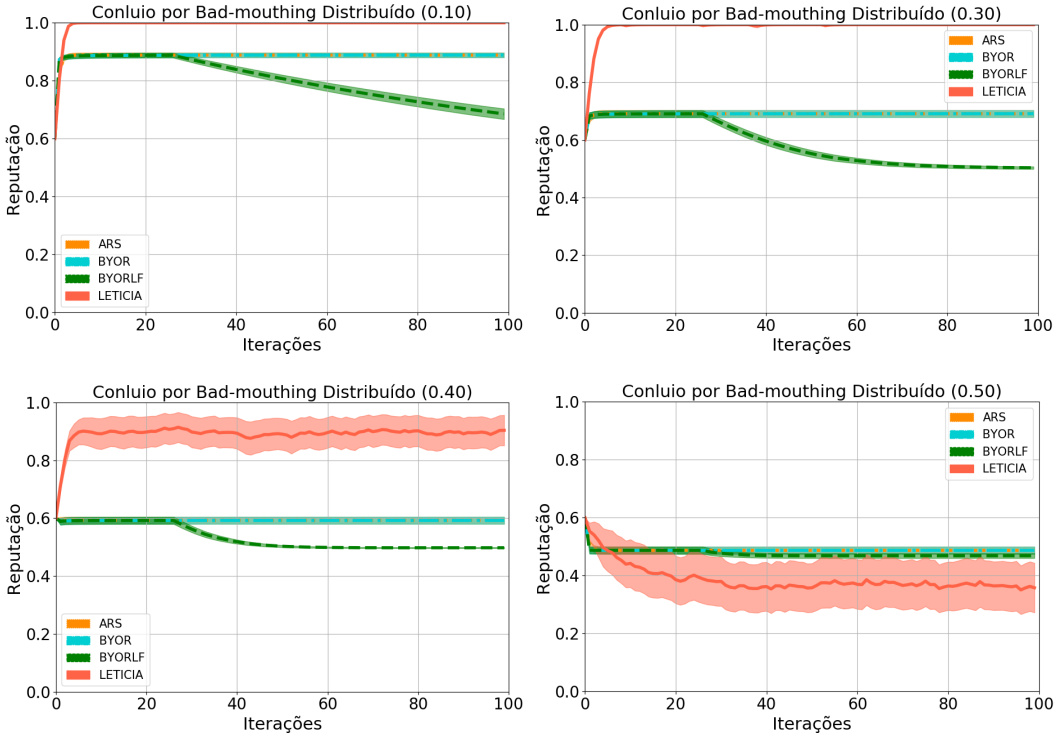


Figura 8. Ataque Conluio por *Bad-mouthing* Distribuído com 10%, 20%, 30% e 40%

6. Conclusões e Trabalhos Futuros

Este artigo apresentou um algoritmo leve para o cálculo de reputação centralizado e eficiente para lidar com ataques de inconsistência e de conluio por *bad-mouthing* em VANET, chamado `LETICIA`. Este algoritmo decrementa rapidamente a reputação de veículos maliciosos e incrementa suavemente a sua reputação, mantendo a estabilidade da decisão. Simulações para ataques de inconsistência mostraram que o `LETICIA` reduziu drasticamente a reputação do veículo malicioso com o menor número de iterações, quando comparado aos algoritmos `ARS`, `BYOR` e `BYOR-LF`. Outra vantagem é que o `LETICIA` recuperou a reputação do veículo malicioso mais lentamente. Nos ataques de conluio por *bad-mouthing* todos os algoritmos reduziram a reputação do veículo honesto. A reputação é afetada à medida que o número de veículos atacantes aumenta na rede ou a maioria dos veículos atacantes possuem uma maior reputação. O `LETICIA` reagiu de forma mais eficiente, pois manteve a reputação do veículo atacado até um limiar. Como trabalhos futuros, pretende-se realizar os testes em um ambiente mais realístico, utilizando os simuladores OMNeT++ e SUMO, e o *framework* Veins. Pretende-se ainda integrar o `RVV` com o VEINS, a fim de facilitar as aplicações com reputação neste *framework*.

AGRADECIMENTOS

Os autores agradecem ao apoio financeiro da agência CAPES, FAPEMIG e CNPq.

Referências

Banković, Z., Vallejo, J. C., Fraga, D., and Moya, J. M. (2011). Detecting bad-mouthing attacks on reputation systems using self-organizing maps. In *Computational Intelligence in Security for Information Systems*, pages 9–16, Berlin, Heidelberg.

Cervantes, C., Poplade, D., Nogueira, M., and Santos, A. (2014). Um sistema de detecção de ataques sinkhole sobre 6lowpan para internet das coisas. *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 153–166.

Dotzer, F., Fischer, L., and Magiera, P. (2005). Vars: a vehicle ad-hoc network reputation system. In *6º IEEE Internat. Symposium on a World of Wireless Mobile and Multimedia Networks*, pages 454–456.

Engoulou, R. G., Bellaiche, M., Halabi, T., and Pierre, S. (2019). A decentralized reputation management system for securing the internet of vehicles. In *2019 International Conference on Computing, Networking and Communications (ICNC)*, pages 900–904.

Ghaleb, F. A., Maarof, M. A., Zainal, A., Rassam, M. A., Saeed, F., and Alsaedi, M. (2019). Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages. *Vehicular Communications*, 20.

Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2017). Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7 – 20.

Hussain, R., Nawaz, W., Lee, J., Son, J., and Seo, J. T. (2016). A hybrid trust management framework for vehicular social networks. In *Internat. Conference on Computational Social Networks*, pages 214–225.

Jaimes, L. M. S., Ullah, K., and dos Santos Moreira, E. (2016). Ars: Anonymous reputation system for vehicular ad hoc networks. In *8th IEEE LatinCom*, pages 1–6.

Jøsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618 – 644.

Li, X., Liu, J., Li, X., and Sun, W. (2013). RGTE: A Reputation-Based Global Trust Establishment in VANETs. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pages 210–214.

Mühlbauer, R. and Kleinschmidt, J. H. (2018). Bring your own reputation: A feasible trust system for vehicular ad hoc networks. *Journal of Sensor and Actuator Networks*, 7(3).

Pedroso, C., Gielow, F., Santos, A., and Nogueira, M. (2019). Mitigação de Ataques IDFs no Serviço de Agrupamento de Disseminação de Dados em Redes IoT Densas. In *Anais SBSeg 2019*, Porto Alegre, RS, Brasil. SBC.

RoselinMary, S., Maheshwari, M., and Thamaraiselvan, M. (2013). Early detection of dos attacks in vanet using attacked packet detection algorithm (apda). In *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, pages 237–240.

Ruohomaa, S., Kutvonen, L., and Koutrouli, E. (2007). Reputation management survey. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 103–111.

Su, S., Tian, Z., Liang, S., Li, S., Du, S., and Guizani, N. (2020). A Reputation Management Scheme for Efficient Malicious Vehicle Identification over 5G Networks. *IEEE Wireless Communications*, 27(3):46–52.

Trček, D. (2017). *Trust and Reputation Management Systems: An e-Business Perspective*. Springer International Publishing.

Zhang, J. (2011). A survey on trust management for vanets. In *2011 IEEE International Conference on Advanced Information Networking and Applications*, pages 105–112.