



UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
NÚCLEO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA
COMPUTAÇÃO

GEORGE LEITE JUNIOR

I9Vanets: um modelo de arquitetura de
software para rede veicular

São Cristóvão

2016

GEORGE LEITE JUNIOR

**I9Vanets: um modelo de arquitetura de software para
rede veicular**

Versão original

Dissertação apresentada à Pró-Reitoria de Pós-Graduação e Pesquisa da Universidade Federal de Sergipe para obtenção do título de Mestre em Ciência da Computação pelo Programa de Pós-graduação em Ciência da Computação.

Área de concentração: Redes de Computadores e Sistemas Distribuídos

Orientador: Prof.^a Dr.^a Douglas D. J. de Macedo

Coorientador: Prof. Dr. Rogério Patrício Chagas do Nascimento

São Cristóvão

2016

Dissertação de autoria de George Leite Junior, sob o título **“I9Vanets: um modelo de arquitetura de software para rede veicular”**, apresentada à Pró-Reitoria de Pós-Graduação e Pesquisa da Universidade Federal de Sergipe, para obtenção do título de Mestre em Ciência da Computação pelo Programa de Pós-graduação em Ciência da Computação, na área de concentração Redes de Computadores e Sistemas Distribuídos, aprovada em ____ de _____ de _____ pela comissão julgadora constituída pelos doutores:

Prof.^a Dr.^a _____

Presidente

Instituição: _____

Prof. Dr. _____

Instituição: _____

Prof. Dr. _____

Instituição: _____

Resumo

LEITE, George Junior. **i9Vanets: um modelo de arquitetura de software para rede veicular**. 2016. 73 f. Dissertação (Mestrado em Ciência da Computação) – Pró-Reitoria de Pós-Graduação e Pesquisa, Universidade Federal de Sergipe, Sergipe, 2016.

Em consequência do crescimento populacional, as grandes cidades enfrentam problemas cotidianos relacionados à mobilidade urbana tais como: congestionamentos, baixa qualidade das rodovias, ineficiência de transportes públicos, entre outros. Iniciativas de sistemas de transportes inteligentes (STI) agem como uma solução eficiente para melhorar o funcionamento e desempenho dos sistemas de tráfego, reduzindo congestionamentos e aumentando a segurança para os cidadãos. Atualmente, pesquisadores vem buscando nas redes veiculares ad-hoc (VANET) uma possível solução para os problemas referentes à mobilidade urbana. Contudo, VANETs ainda apresenta uma série de desafios que devem ser resolvidos para que seu uso seja consolidado. Deste modo, o presente trabalho apresenta uma arquitetura denominada i9Vanets, cujo intuito é o gerenciamento virtualizado por meio de uma rede veicular para auxiliar nas soluções dos principais desafios relacionados à VANETs. Também é apresentado uma análise, dos testes realizados em laboratório, com objetivo de avaliar seu desempenho e capacidade operacional. Sendo assim, a conclusão deste trabalho, foi apresentar a viabilidade técnica da arquitetura i9Vanets bem como suas possíveis aplicações.

Palavras-chaves: Rede Veicular. Computação em Nuvem.

Abstract

LEITE, George Junior. **I9Vanets: a software architecture model for a vehicular network**. 2016. 73 p. Dissertation (Master of Science of Computer) – Dean of Graduate Studies and Research, Federal University of Sergipe, Sergipe, 2016.

Bla bla bla bla bla bla Bla bla bla bla bla blaBla bla bla bla blaBla bla bla
bla bla bla bla Bla bla bla bla bla bla Bla bla bla bla bla blaBla bla bla bla bla
blaBla bla bla bla bla bla blaBla bla bla bla bla bla Bla bla bla bla bla blaBla bla
bla bla bla bla blaBla bla bla bla bla blaBla bla bla bla bla bla Bla bla bla bla bla
bla blaBla bla bla bla bla bla blaBla bla bla bla bla blaBla bla bla bla bla bla Bla
bla bla bla bla bla blaBla bla bla bla bla blaBla bla bla bla bla blaBla bla bla bla
bla bla bla Bla bla bla bla bla bla blaBla bla bla bla bla blaBla bla bla bla bla bla
blaBla bla bla bla bla bla bla Bla bla bla bla bla bla blaBla bla bla bla bla blaBla bla
bla bla bla bla bla.

Keywords: Vehicle Network. Cloud Computing.

Lista de figuras

Figura 1 – Imagem do trânsito (DANTAS, 2011)	13
Figura 2 – Modelo do VNC (LEE et al., 2014)	17
Figura 3 – Arquitetura de referência para aplicações ITS baseadas em WSN. (LO-SILLA et al., 2011)	21
Figura 4 – Arquiteturas de redes veiculares(LUÍS, 2009)	27
Figura 5 – Ataque DDOS (WANGHAM et al.,).	29
Figura 6 – Ataque Buraco Negro (WANGHAM et al.,).	30
Figura 7 – Ataque social (WANGHAM et al.,).	31
Figura 8 – Ataque demodificação de mensagem (WANGHAM et al.,).	32
Figura 9 – Exemplo de aplicação VANET (QIAN; LU; MOAYERI, 2008).	40
Figura 10 – Módulos definidos para a arquitetura I9Vanet.	41
Figura 11 – Modelo de comunicação V2A, I2A, AI2AI e AV2AI.	44
Figura 12 – Exemplo de domínios.	46
Figura 13 – Organização dos servidores na nuvem.	48
Figura 14 – Modelo de processo de negócio da arquitetura I9Vanet com criptografia.	50
Figura 15 – Modelo de processo de negócio da arquitetura I9Vanet sem criptografia.	51
Figura 16 – Coniguração do ambiente utilizado para a realização dos experimentos. Fonte: Criada pelo autor.	55
Figura 17 – Tela de monitoramento do Sistema TaxiFast.	55
Figura 18 – Análise de Histograma de Frequência do Teste com 50 veículos.	61
Figura 19 – Análise de Histograma de Frequência do Teste com 100 veículos.	62
Figura 20 – Análise de Histograma de Frequência do Teste com 200 veículos.	63
Figura 21 – Análise de Histograma de Frequência do Teste com 400 veículos.	63
Figura 22 – Gráfico comparativo dos tempos mínimos entres os cenários.	64
Figura 23 – Gráfico comparativo dos tempos médios entres os cenários.	64
Figura 24 – Gráfico comparativo dos tempos máximos entres os cenários.	65

Lista de algoritmos

Lista de tabelas

Tabela 1 – Protocolos de roteamento aplicados a redes veiculares (LUÍS, 2009) . . .	39
Tabela 2 – Colunas das tabelas <i>Server</i>	47
Tabela 3 – Colunas da tabela <i>Device</i>	48
Tabela 4 – Características das aplicações veiculares.	53
Tabela 5 – Linhas do arquivo de movimentação.	56
Tabela 6 – Configuração dos computadores utilizados no experimento.	58
Tabela 7 – Configuração dos computadores utilizados no experimento em cada cenário.	59
Tabela 8 – Resultado do teste de análise de distribuição normal dos dados para cada quantidade de veículos e velocidades de acesso.	60
Tabela 9 – Resultado do teste de análise dos coeficientes de variação.	60
Tabela 10 – Velocidade de cada link por veículo.	62

Lista de abreviaturas e siglas

ITS	Intelligent Transport System
VANET	Vehicle Network Ad-hoc
VCC	Vehicle Cloud Computing
VNC	Vehicular Cloud Networking
V2V	Veículo para Veículo
V2I	Veículo para Infra-estrutura
AV2AV	Agente do Veículo para outro Agente do Veículo
AV2AI	Agente do Veículo para Agente da Infra-estrutura
AI2AI	Agente da Infra-estrutura para outro Agente da Infra-estrutura
AVC	Nuvens Veiculares Autônomas
SDN	Software-Defined Networking

Sumário

1	Introdução	12
1.1	Justificativa, Problemática e Hipótese	13
1.1.1	Justificativa	13
1.1.2	Problemática	17
1.1.3	Hipótese	17
1.2	Objetivos da Dissertação	17
1.2.1	Objetivos Específicos	17
1.2.2	Metodologia	18
1.2.3	Contribuições	19
1.3	Organização do Trabalho	19
2	Rede de Sensores sem Fio	20
2.1	Definição	20
2.2	Arquitetura de Rede e Topologia	20
2.2.1	Subsistema de Sensores	21
2.2.2	Subsistema de Distribuição	22
2.2.3	Subsistema de Tomada de Decisão	23
2.2.4	Subsistema de Execução	24
3	Sistemas Distribuídos	25
3.1	Definição	25
3.2	Características e Desafios	25
3.3	Aplicações	25
3.4	Protocolos	25
4	Redes Veiculares	26
4.1	Definição	26
4.2	Características e Desafios	27
4.3	Segurança	28
4.3.1	Ataques contra a Disponibilidade	28
4.3.2	Ataques contra a Autenticidade e a Identificação	30

4.3.3	Ataques contra a Integridade e Confiança dos Dados . . .	30
4.3.4	Ataques contra a Confidencialidade	32
4.3.5	Outros Ataques	32
4.4	Algoritmos de Roteamento	33
4.4.1	Protocolos Ad-hoc	34
4.4.2	Protocolos Baseados em Localização	35
4.4.3	Protocolos Baseado em <i>Clusters</i>	36
4.4.4	Protocolos por Broadcast	37
4.4.5	Protocolos <i>Geocast</i>	37
4.4.6	Comparação dos Protocolos de Roteamentos	38
4.5	Aplicações	39
5	Arquitetura I9Vanet	41
5.1	Visão Geral	41
5.2	Módulo da Arquitetura I9Vanets	41
5.2.1	Módulo de Comunicação	42
5.2.1.1	Comunicação Infra-Cloud	42
5.2.1.2	Comunicação Veículo-Cloud	43
5.2.2	Módulo de Segurança	45
5.2.3	Módulo de Gerenciamento dos Servidores	46
5.2.4	Módulo de Roteamento	49
5.2.5	Módulo de Aplicações	50
5.3	Processo de Negócio	50
6	Avaliação da Arquitetura	52
6.0.1	Definição	52
6.0.2	Planejamento	52
6.1	Cenário Proposto	54
6.2	Experimentos	58
6.3	Resultados	59
6.3.1	Taxa de Transferência	61
6.3.2	Processamento	62
7	Conclusão e Trabalhos Futuros	66

7.1	Conclusões deste Trabalho	66
7.2	Trabalhos Futuros	67
	Referências	68

1 Introdução

A conectividade inerente às cidades inteligentes abre uma fronteira bastante promissora no que se refere ao controle de acesso às informações (LI, 2010) (ZHU; LIU, 2015) e arquiteturas distribuídas para sistemas inteligentes de transporte (ICE et al., 2001).

Um sistema inteligente de transporte ou *Intelligent Transportation System* (ITS) representa “a aplicação de sensores avançados, computadores, dispositivos eletrônicos e tecnologias de comunicação e gerenciamento estratégico integrado visando melhorar a segurança e a eficiência do sistema de gerenciamento de tráfego” (NASIM; KASSLER, 2012).

Os Sistemas Inteligentes de Transporte (ITS), são actualmente a mais importante aplicação de uma rede veicular, fornecendo serviços de segurança rodoviários (XU et al., 2003) ou informações relativas às situações de tráfego. Dito por Sumra (2011) (SUMRA; HASBULLAH; MANAN, 2011) e Luís (2009) (LUÍS, 2009), o principal objetivo de uma VANET é prover segurança aos passageiros nas estradas.

Também de acordo com Ball e Dulay (2010) e Losilla et al. (LOSILLA et al., 2011), a segurança no trânsito é a motivação principal para as pesquisas no âmbito das redes veiculares. Da mesma maneira, conforme a Organização Mundial da Saúde (OMS), acidentes acometidos por veículos são responsáveis por mais de um milhão de mortes e 50 milhões de feridos anualmente em todo o mundo (PEDEN et al., 2004). Nos Estados Unidos e no Brasil, acidentes realacionados a veículos são a terceira maior causa de mortalidade evitável e incapacitação profissional precoce (SYSTEMATICS; MEYER, 2011) (DIB et al., 2007).

Ainda afirmado por Losilla et al. (LOSILLA et al., 2011), congestionamento também é uma grande preocupação como mostra a figura 1. Só nos EUA, o congestionamento representa 115 bilhões de dólares em custos de combustível (TTI, 2014), com números semelhantes em outros países desenvolvidos. As baixas de tráfego no mundo ascendem a 1,17 milhões por ano. Neste contexto, os Sistemas de Transporte Inteligentes visam melhorar a eficiência e a segurança dos transportes através do uso avançado de processamento de informação, comunicações, controle, bem como de novas tecnologias eletrônicas.

Segundo o IPEA (Instituto de Pesquisa Econômica Aplicada do Brasil), a mobilidade urbana, nos dias atuais, é um dos principais problemas dos grandes centros. Os reflexos sobre o transporte urbano são evidentes, caracterizados principalmente pelo aumento do

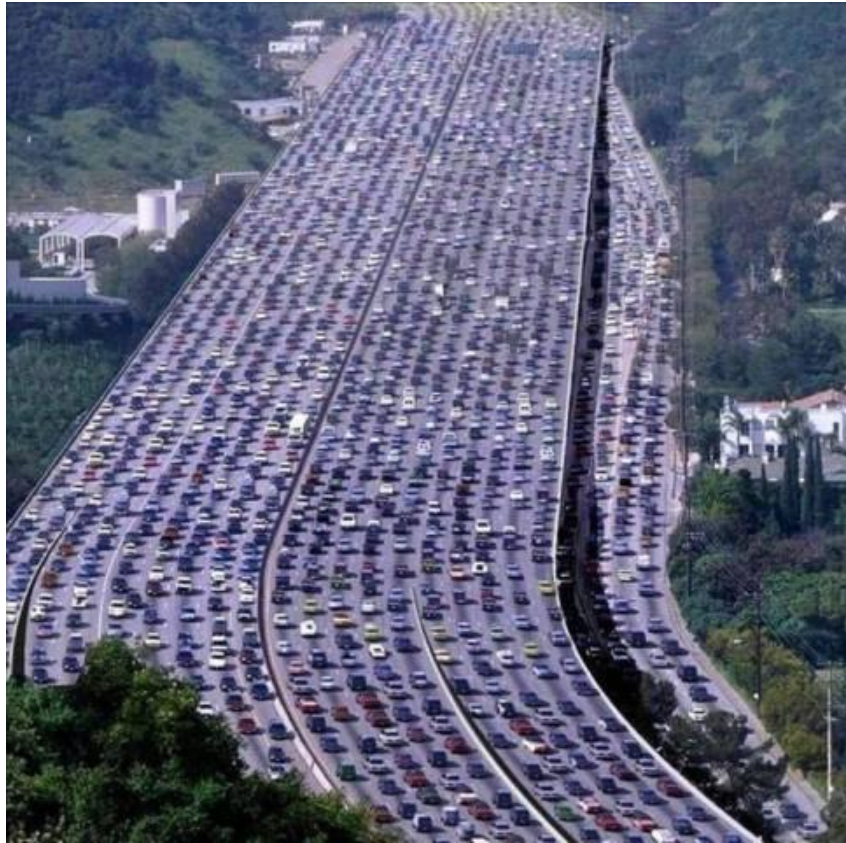


Figura 1 – Imagem do trânsito ([DANTAS, 2011](#))

tráfego nas vias e consequentemente dos congestionamentos ([CARVALHO et al., 2010](#)). Porém, baseado em Gupte and Younis (2012) , é possível gerir o tráfego de forma eficiente utilizando redes de veículos ad-hoc (VANET) de maneira eficiente e autonoma.

Segundo Cavalcanti (2008) ([CAVALCANTI, 2008](#)), a crescente quantidade de dispositivos eletrônicos que podem ser embarcados em veículos automotores como DVD, TV, GPS e telefone celular, faz com que os veículos deixem de ser apenas um meio de transporte e passem a oferecer uma rede de serviços e entretenimento para os condutores e/ou passageiros.

1.1 Justificativa, Problemática e Hipótese

1.1.1 Justificativa

É crescente o número de pesquisas sobre VANETs com intuito de aumentar a segurança viária, bem como ofertar e comercializar novos serviços a motoristas e passageiros. VANETs que usam veículos como nós móveis, são uma subclasse de rede móveis ad hoc

chamadas de MANETs (*Mobile Ad hoc Network*), elas fornecem comunicação entre os veículos próximos e entre veículos e equipamentos à beira da rodovia mas, aparentemente difere de outras redes por suas próprias características do ambiente.

Diante da evolução das redes veiculares e da necessidade de garantir o táfego dos dados dentro da alta mobilidade dos nós numa VANET, vê-se a importância de utilizar tecnologias que permitam auxiliar na solução dos principais desafios relacionados a este tipo de rede.

O uso de VANETs representa uma oportunidade para melhora na segurança, eficiência e conforto relacionados ao trânsito nas grandes cidades, porém, possui características específicas que apresentam obstáculos a serem contornados.

Os nós numa rede VANET são muito dinâmicos pois os veículos possuem velocidade e direção variável. A alta mobilidade dos nós conduz a uma topologia de rede dinâmica caracterizada pela constante perda de comunicação fazendo com que os algoritmos de roteamentos tornem-se complexos e limitados. Normalmente, VANETs apresentam três aspectos para pesquisas: roteamento, segurança e privacidade, bem como suas aplicações (LIANG et al., 2015).

O roteamento em VANETs é baseada na comunicação sem fio e devido à topologia dinâmica e conectividade intermitente, a maioria dos algoritmos em MANETs não estão disponíveis para os vários cenários VANETs, tornando o tema ainda em aberto e sendo foco de várias pesquisas na atualidade com objetivo de dar confiabilidade na comunicação levando em consideração número de emissores e receptores e tipos de roteamento.

Comentado por Cavalcanti(2008), os nós de uma rede veicular apresentam como principal característica, a alta mobilidade, por serem dinâmicos e apresentarem rápidas variações das condições do meio sem fio são os principais geradores de desafios. O alto dinamismo representa um contratempo para as comunicações, visto que nem sempre o tempo de contato dos veículos é suficiente para estabelecer uma comunicação efetiva.

Trabalhos como , Nandan et al. (2005), Chen (2006) e Hadaller (2007) , apresentam propostas que vão desde a implementação de uma infra-estrutura fixa até definir esquemas de agrupamento de nós, visando reduzir a latência de entrega de mensagens para sistemas de segurança. Nandan et al. (2005), propuseram uma comunicação eficiente para sistemas P2P com disponibilização de conteúdo utilizando um mecanismo de partição dos arquivos disponíveis em pequenos pedaços. Este particionamento visa promover uma forma de transferência distribuída, na qual é possível que um nó esteja recebendo dois pedaços

distintos do mesmo arquivo de duas fontes distintas e simultaneamente. Cabe ressaltar que em grande parte as propostas visam agilizar o processo de transferência de dados em VANETs e implementam mecanismos específicos para minimizar os problemas gerados pela alta mobilidade dos nós.

Dentro desse contexto, este artigo apresenta como principal contribuição, um modelo de arquitetura de software flexível e extensível, que utiliza rede veicular e Computação em Nuvem, com a finalidade de proporcionar uma alternativa para os principais desafios relacionados à VANETs tais como:

- **meio físico:** interferências devido à prédios, árvores e outros obstáculos;
- **alta mobilidade:** dificulta a troca de informações mais completas;
- **topologia:** VANET possui uma característica dinâmica, devido à velocidade que os veículos se movimentam;
- **baixa densidade:** quando a densidade de tráfego é baixa e os veículos estão distantes uns dos outros;
- **alta densidade:** muitos veículos em uma pequena área faz com que a quantidade de mensagens trocadas seja um problema;
- **segurança:** como as VANETs suportam aplicações de emergência em tempo real e lidam com informações críticas de segurança no trânsito, estas devem satisfazer os seguintes requisitos de segurança: confidencialidade, integridade, disponibilidade, autenticidade, privacidade e não repudição para prover segurança na comunicação dos dados ([SAMARA; AL-SALIH; SURES, 2010](#)) ([MATOS et al., 2013](#)).

Segundo Falchetti et al, os principais desafios técnicos que são abordadas pela maioria dos pesquisadores, podem ser agrupados em seis categorias: mobilidade, latência, confiabilidade, criticidade(prioridade das mensagens), topologia e segurança.

Portanto, pesquisar sobre redes veiculares e computação em nuvem, traz a possibilidade de construção de uma plataforma capaz de criar uma VANET virtualizada facilitando a comunicação entre os nós virtuais da rede e simplificando a implementação dos algoritmos de roteamento, segurança e aplicações.

Com o uso da computação em nuvem, os autores Liu et al. utilizaram um controlador SDN (*Networking Defined Software*) para enviar mensagens para os veículos a partir de um RSU conectados ao controlador, porém, os veículos deveriam pertencer à mesma geolocalização.

Foi criado por Hajji e Bargaoui , a plataforma Testbed que serve para testar a implementação real dos roteadores móveis em uma rede veicular virtualizado. A característica principal consiste na sua capacidade em satisfazer ao mesmo tempo as exigências de mobilidade do veículo e o número elástico de roteadores Móveis aplicados.

Olariu et al pela primeira vez realizou uma mudança de paradigma imaginado para o ambiente de VANET tradicional para VANET baseado em nuvem. Eles vieram com uma nova noção de VANET chamado AVC (*Autónomas Vehiculares Nuvens*). Yan et al. delineou os desafios de segurança e privacidade nas nuvens veiculares. No entanto, Olariu et al. discutiu sobre nuvens veiculares de maneira abstrata, sem mencionar uma arquitetura em particular.

Recentemente, Hussain et al. propôs três quadros de arquitetura para VANETs baseados em nuvem ou seja VC (*Vehicular Clouds*), VUC (textitVANET using Clouds)), e HVC (*Hybrid Vehicular Clouds*) e propôs um esquema conhecido como TIaaS (*Information of traffic as Service*), onde a infraestrutura de nuvem atua para fornecer informações de tráfego para os veículos que se deslocam sobre a estrada.

Qin et al. (QIN; HUANG; ZHANG, 2012) propôs um esquema de roteamento, para VANETs, baseado em nuvem chamado VehiCloud que fornece serviços de roteamento através da infraestrutura de nuvem. Veículos compartilham a sua actual e futuras informações de localização na forma de *waypoints*) com infraestrutura de nuvem e, em seguida, a nuvem lhes proporciona uma melhor informação de roteamento.

De acordo com Falchetti et al. , a integração de VANETs com a nuvem aumenta a utilização das capacidades computacionais que são subutilizados por aplicações de segurança e supera os problemas de roteamento em comunicação V2V (*Vehicle to Vehicle*).

Lee et al (2014). visam interligar recursos OBU (*On Board Unit*) e RSU (*Road Side Unit*) em nuvem para tarefas cooperativas sensoriais, de armazenamento e de computação, enquanto outros (HUSSAIN et al., 2012) (MERSHAD; ARTAIL, 2013) propõem que as RSUs ajam como gateways para as OBUs para acesso às nuvens tradicionais.

Foi proposto por Lee et al.(LEE et al., 2014) o VCN (*Vehicular Cloud Networking*) que está sendo visto como uma revolução para modernizar a tradicional VANET, que integra informações de redes e Cloud Computing com VANETs tradicionais. No VCN, veículos e RSU compartilham seus recursos em uma plataforma virtual como ilustrado na figura 2.

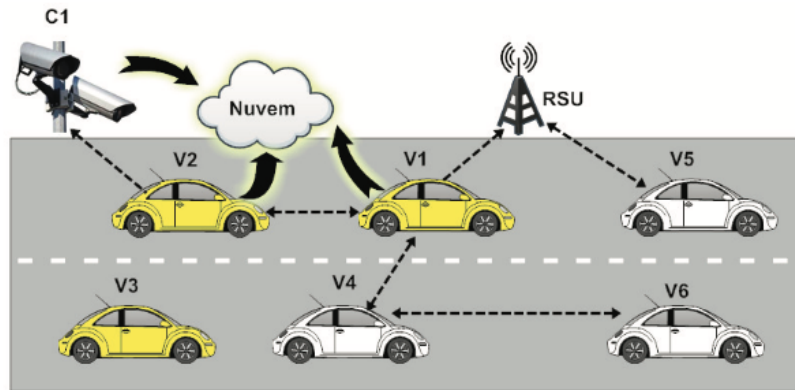


Figura 2 – Modelo do VNC (LEE et al., 2014)

1.1.2 Problemática

Como criar uma plataforma em nuvem capaz de permitir a construção de aplicações voltadas para VANETs, considerando o desenvolvimento simplificado e extensível de maneira que o cerne principal da plataforma seja abstraído das novas funcionalidades e mantendo o foco nos principais desafios atualmente encontrados em redes veiculares.

1.1.3 Hipótese

Avaliar se o tempo de resposta da arquitetura proposta permite os mais variados tipos de aplicações em VANETs, dada a particularidade deste tipo de rede.

1.2 Objetivos da Dissertação

O objetivo principal desta dissertação é apresentar uma arquitetura de software flexível e extensível, com capacidade de virtualizar nós de uma rede VANET, realizando a comunicação entre os elementos de forma virtual na tentativa de corroborar com a solução de alguns dos principais desafios relacionados à rede veiculares.

1.2.1 Objetivos Específicos

Para alcançar a integração anterior, alguns objetivos específicos devem ser atendidos, a saber:

- Definir a arquitetura de software de maneira que permita a extensibilidade e flexibilidade;
- Construir a arquitetura utilizando a linguagem Java;
- Implementar uma versão para cada camada da arquitetura para realização de testes;
- Construir uma aplicação como prova de conceito;
- Realizar testes simulados para avaliar seu desempenho e capacidade.

1.2.2 Metodologia

No desenvolvimento desta dissertação foram empregadas a pesquisa bibliográfica, pesquisa quantitativa e a pesquisa experimental.

Na pesquisa bibliográfica foi verificado o estado da arte sobre redes veiculares e seus principais desafios. A pesquisa quantitativa foi utilizada para poder quantificar dentre as aplicações relacionadas à VANETs quais os tempos de comunicação necessários para viabilidade da solução. E por fim, a pesquisa experimental, pois foram realizados experimentos na arquitetura e gerados dados em um ambiente real para responder a hipótese levantada na problemática.

Na definição do escopo e das metas desta pesquisa, ficou estabelecido definir e construir uma arquitetura de software modular de maneira que cada módulo abstraia detalhes de implementação dos demais, permitindo usufruir de “contratos” no uso efetivo dos módulos.

Os cenários para os experimentos foram definidos utilizando movimentações reais dentro da cidade de Aracaju-Sergipe Brasil, os quais foram extraídos de uma empresa de taxi gerando 12 milhões de movimentações.

Para alcançar os resultados foi necessário estabelecer conexões entre os nós de uma rede VANETs, permitindo a criação de rede de maneira dinâmica e “aleatória” mantendo a integridade dos dados.

A métrica e a técnica de avaliação desta pesquisa foi o tempo de processamento de cada mensagem enviada ao servidor como também o tempo de comunicação entre os veículos e os servidores em nuvem contrapondo entre as velocidades do 2G, 3G, 4G e 5G, permitindo avaliar se as velocidades atuais da telefonia móvel suportam a solução.

1.2.3 Contribuições

A computação veicular em nuvem é um novo campo de pesquisa com o potencial de mudar a vida das pessoas. Ele traz a eficiência, segurança e conforto para motoristas e passageiros (FALCHETTI; AZURDIA-MEZA; CESPEDES, 2015). Sendo a principal contribuição deste trabalho a construção de uma arquitetura para criação de redes veiculares em nuvem como também a análise dos dados coletados a partir dos experimentos. Nesse sentido, este estudo mostra que também é válido o uso de VCN no auxílio das soluções para os principais desafios relacionados à VANETs.

Outra contribuição importante foi poder instalar e analisar aspectos de segurança nas redes veiculares podendo apenas assinar a mensagem ou criptografá-la, seguindo com análise de viabilidade. Conclui-se que o desempenho e eficiência da arquitetura atendem aos requisitos relacionados à VANETs. E assim, demonstrar que o tempo de conexão e processamento em uma rede VCN em ambiente de simulação atende às necessidades de vários tipos de aplicações relacionadas a VANETs.

Dentro desse contexto, este trabalho apresenta como principal contribuição, um modelo de arquitetura de software flexível e extensível, que utiliza rede veicular ad-hoc (VANET) e Computação em Nuvem, com a finalidade de proporcionar uma alternativa para os principais desafios relacionados à VANETs .

1.3 Organização do Trabalho

Os demais capítulos da dissertação estão organizados da seguinte forma: O capítulo 2 aborda de maneira geral as redes veiculares, as suas aplicações, conceitos de internet das coisas e sistemas distribuídos. No capítulo 3 é apresentado a arquitetura I9Vanet, seus módulos e detalhes da tecnologia utilizada na construção. Já o capítulo 4, apresenta o processo de avaliação realizado na arquitetura I9Vanet bem como a análise dos resultados. O capítulo 5 apresenta as conclusões, destacando as principais contribuições, o resultado da análise dos dados e sugestão para os possíveis trabalhos futuros.

2 Rede de Sensores sem Fio

As Redes de Sensores ou WSN (*Wireless Sensor Network*) estão emergindo como uma nova ferramenta para aplicações importantes em diversos campos como vigilância militar, monitoramento de ambiente, e coleta de informações em ambiente hostil, vigilância de edifícios, entre outros.

2.1 Definição

Uma rede de sensores sem fio é uma tecnologia específica que ajuda na criação de aplicações com foco em cidades inteligentes. O seu objectivo consiste em criar uma rede que contenha muitos nós de sensores “inteligentes” que possam detectar múltiplos parâmetros de interesse para uma melhor gestão da cidade.

Para realizar tarefas de detecção, a maioria dos Sistemas de Transporte Inteligentes (ITS) atuais contam com sensores caros, que oferecem apenas funcionalidade limitada. Uma tendência mais recente consiste em utilizar WSN para tal finalidade, o que reduz o investimento necessário e permite o desenvolvimento de novas aplicações colaborativas e inteligentes que contribuem ainda mais para melhorar tanto a segurança de condução como a eficiência do tráfego ([LOSILLA et al., 2011](#)).

Da mesma forma que em redes de sensores sem fio, os nós de uma rede VANET necessitam trocar informações com outros nós próximos o que torna técnicas de WSN aplicáveis à redes veiculares entretanto, há o desafio da alta mobilidade dos nós em uma rede VANET.

2.2 Arquitetura de Rede e Topologia

Uma aplicação ITS baseada em WSN distribuída, realiza quatro tarefas principais distintas: (i) aquisição de informação, (ii) distribuição de dados, (iii) processamento de dados para planejar as ações necessárias e, finalmente, (iv) execução das ações apropriadas ([LOSILLA et al., 2011](#)). Uma vez que estas tarefas podem ser realizadas de forma independente, pode considerar-se que definem correspondentemente quatro subsistemas diferenciados que estão presentes nos sistemas ITS, como mostrado na figura 3, nomeada-

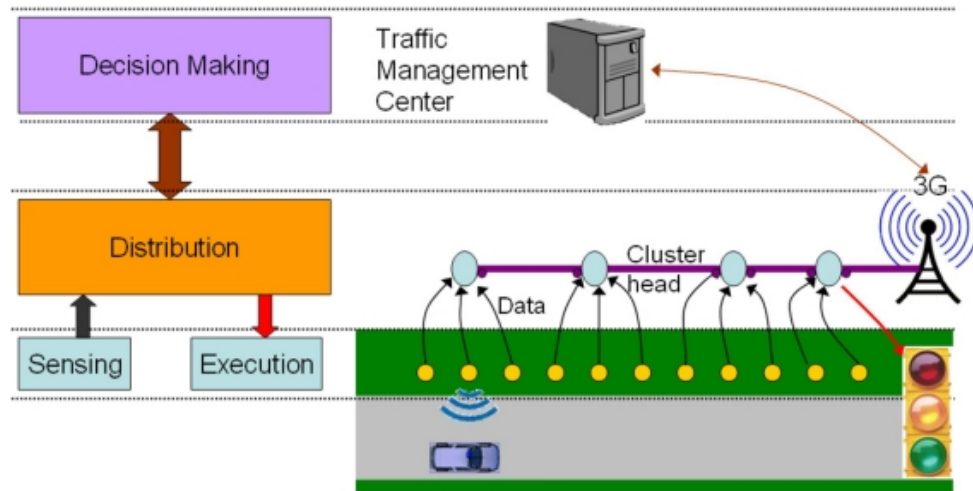


Figura 3 – Arquitetura de referência para aplicações ITS baseadas em WSN. (LOSILLA et al., 2011)

mente o subsistema «Sensores», o subsistema «Distribuição», o subsistema «Tomada de decisões» e o subsistema «Execução».

2.2.1 Subsistema de Sensores

Este subsistema é composto pela aquisição das informações relevantes, principalmente em relação ao tráfego e estados da rodovia. Numa aplicação ITS baseada em WSN, não necessariamente todos os dispositivos utilizam a tecnologia WSN, permitindo uma distribuição de tarefas entre dispositivos que utilizam tecnologias diferentes. A implantação do subsistema de sensores consiste na implantação de um ou mais WSNs em toda a área de observação (estradas ou parques de estacionamento), que detectam veículos através dos seus sensores e, opcionalmente, comunicam-se sem fios com eles. Os nós WSN são divididos em grupos seguindo um esquema semelhante, e a implantação consiste em uma composição, tipicamente homogênea, desses grupos de nós. Portanto, eles podem ser considerados como os blocos de construção do subsistema de detecção. Deve-se notar que, além disso, os nós que formam esses blocos podem propagar informações dentro deles, mas isso não deve ser confundido com o subsistema de Distribuição. A propagação de dados no subsistema de sensores é restrita a áreas locais, visando extrair informações do bloco / grupo (para um nó coletor) ou ativar o processamento colaborativo com nós próximos. Se for necessária a disseminação de dados através de áreas maiores, é necessário o uso do subsistema de distribuição.

2.2.2 Subsistema de Distribuição

O subsistema de distribuição é responsável pela troca de informações entre os diferentes subsistemas de uma aplicação ITS. Numa arquitectura em camadas tal como a da Figura 3, ela é colocada numa posição central, recebendo pedidos de comunicação de todos os outros subsistemas e servindo-os em conformidade. É responsável pela transmissão dos dados detectados para o subsistema «tomada de decisões» e, por outro lado, pela transmissão de comandos do subsistema «tomada de decisões» para os subsistemas «detecção e execução» (SUNG; YOO; KIM, 2007). Da mesma forma, interconecta os diferentes grupos de sensores de uma rede. Isso resulta em uma rede escalável criada pela composição desses grupos. A este respeito, o subsistema de distribuição pode igualmente interligar grupos fisicamente isolados de nós ou veículos, permitindo assim a interconexão de ilhas WSN desdobradas em diferentes partes ao longo da estrada (WEINGÄRTNER; KARGL, 2007) ou de agrupamentos de veículos que de outra maneira formariam VANETs não ligados (BARBA; AGUIRRE; IGARTUA, 2010) .

O subsistema de distribuição consome uma quantidade significativa de energia devido às exigências impostas aos seus dispositivos. Eles são encarregados de encaminhar cada evento relatado por cada nó do subsistema de sensores, que pode ocorrer em uma alta taxa de frequência. Além disso, deve ser feito sob as restrições de tempo definidas pela aplicação. Isto requer nós muito ativos para garantir a entrega de informações em tempo hábil, comprometendo a economia de energia. Portanto, os dispositivos usados neste subsistema precisam de um orçamento de energia mais generoso do que os nós de sensores, tornando necessárias fontes de energia adicionais (LOSILLA et al., 2011).

Existem diferentes formas de implementar o subsistema de distribuição. Uma delas consiste em empregar redes veiculares para disseminar informações. Dispositivos utilizados nos veículos não têm restrições de energia, uma vez que podem ser alimentados por instalações do próprio veículo. Além disso, a mobilidade de veículos, que é um fator limitante para outros tipos de aplicações, ajuda a espalhar dados em veículos e nós estáticos ao longo da rodovia, e alivia os nós estáticos das tarefas de distribuição. O esquema mais simples envolve a utilização de transmissão directa entre veículos, isto é, uma rede de um salto que permite a partilha de dados de um veículo de origem para cada veículo que se aproxima (LI; LIU; TANG, 2007) (MIURA; ZHAN; KURODA, 2006). A segunda alternativa baseia-se na utilização de uma rede de distribuição VANET multi-salto

(QIN et al., 2010). Esta opção requer mais recursos do sistema, mas também facilita a disseminação mais rápida de dados e escalas muito melhor à medida que o número de veículos tecnologicamente equipados cresce.

De acordo com Losilla et al. (LOSILLA et al., 2011), um subsistema de distribuição baseado em redes celulares é uma opção atraente, não apenas por sua alta disponibilidade, mas também pelo custo de implantação. Mesmo gateways são dispositivos caros que requerem interfaces de rede celular, apenas alguns deles são necessários para serem colocados perto de estações de base celulares (BS) e alguns nós mais baratos que conectam os nós de detecção com os gateways devem ser implantados. Por outro lado, os custos de exploração também devem ser levados em conta, uma vez que os operadores celulares cobram a utilização da BS. Isso pode levar a uma outra escolha, quer quando não está planejado para pagar o uso de BS ou não estão disponíveis, que consiste em usar IMS (Internet Multimedia Subsystems) (BIRK; OSIPOV; ELIASSON, 2009) que fornecem acesso ao Sistema de Distribuição através de diferentes tecnologias (2G, 2.5G, 3G, 4G, 5G, WLAN) independentemente do operador.

2.2.3 Subsistema de Tomada de Decisão

Subsistema de tomada de decisão é também conhecido por DMS (*Decision Making subsystem*), é responsável pelo planejamento das ações necessárias para alcançar os objetivos do sistema. As tarefas atribuídas a este subsistema podem ser divididas em três grupos diferentes. O primeiro deles inclui tarefas destinadas ao armazenamento e ao pré-processamento de dados. Trata-se da enorme quantidade de dados que chega ao subsistema, filtrando e armazenando apenas informações relevantes e subsequentemente acessando-a. O segundo grupo trata as informações de tráfego de diferentes fontes e as processa de acordo com o objetivo da aplicação. Finalmente, o terceiro grupo de tarefas é responsável por endereçar comandos de controle, bem como para gerenciamento da rede.

O DMS pode ser executado em diferentes níveis. Em um nível superior, ele pode ser implementado em centrais de monitoramento de tráfego. Isto implica que todos os dados recolhidos pelo subsistema de sensores são enviados, através do subsistema de distribuição, para o DMS, que deve suportar um fluxo de dados assimétrico. A principal vantagem desta abordagem é a possibilidade de realizar cálculos complexos sobre uma grande quantidade de informação. Inversamente, se apenas o processamento simples for aplicado, o DMS pode

ser distribuído entre os nós . Isso permite executar algoritmos colaborativos simples entre nós vizinhos que permitem a execução de aplicações de segurança de tráfego em tempo real. Finalmente, uma outra solução é a utilização de dispositivos inteligentes (smartphones, etc.) em veículos, que podem receber dados brutos de redes rodoviárias e usá-los, por exemplo, para planejar rotas (LOSILLA et al., 2011).

2.2.4 Subsistema de Execução

Este subsistema é responsável por executar ações necessárias que promovam mudanças no fluxo de tráfego de acordo com o objetivo da aplicação ITS. É composto principalmente por dispositivos que fornecem estímulos visuais e acústicos aos condutores, embora outros destinados à automação de veículos também pertençam a este subsistema. Podem ser utilizados equipamentos diferentes. Os semáforos ou os sinais de mensagem variável instalados ao longo das estradas são opções atrativas que proporcionam um controlo rigoroso e adaptabilidade a diferentes situações, respectivamente. Eles oferecem a vantagem de serem infra-estruturas rodoviárias amplamente adotadas, adequadas para reutilização em aplicações para ITS, o que ajudaria a reduzir os custos de implantação (LOSILLA et al., 2011).

O emprego de sistemas no veículo oferece, por um lado, a possibilidade de apresentar informação personalizada para cada veículo e, por outro lado, a possibilidade de utilizar sinais acústicos e mensagens que diminuem as distrações durante a condução. Além disso, as informações provenientes dos sistemas rodoviários podem ser integradas nos sistemas de informações no veículo, o IVI (*In-Vehicle Infotainment*), por exemplo, para a sua fusão com mapas digitais ou outros serviços de informação (horários de transporte, previsões meteorológicas, etc.). Atualmente, o número considerável e crescente de smartphones, navegadores ou tablets abre o caminho para a adoção de sistemas dentro do veículo. No entanto, há um interesse crescente dos fabricantes de veículos em incorporar sistemas IVI em seus produtos como um diferencial competitivo. A este respeito, novos modelos de automóveis de empresas importantes estão equipados com sistemas como o iDrive da BMW (NIEDERMAIER et al., 2009), o Audi MMI [44], a Ford SYNC [45] ou GENIVI Apollo da aliança GENIVI apud Losilla et al (LOSILLA et al., 2011), que visam facilitar o desenvolvimento Das aplicações IVI.

3 Sistemas Distribuídos

3.1 Definição

3.2 Características e Desafios

3.3 Aplicações

3.4 Protocolos

4 Redes Veiculares

4.1 Definição

As VANETs que usam veículos como nós móveis são uma subclasse de rede móveis ad hoc chamadas de MANETs. Elas fornecem comunicação entre os veículos próximos e entre veículos e equipamentos à beira da rodovia. Os nós numa rede VANET são muito mais dinâmicos, pois os veículos possuem velocidade e direção variável. A alta mobilidade dos nós conduz a uma topologia de rede dinâmica caracterizada pela constante perda de comunicação (BUBENIKOVA; DURECH; FRANEKOVA, 2014) (JAKUBIAK; KOUCHERYAVY, 2008). E podem ser categorizadas segundo o tipo de ligações existentes. Dessa maneira, consideremos as três arquiteturas de redes veiculares (LUÍS, 2009), como mostra a figura 4:

- **Arquitetura WLAN ou celular:** baseada na utilização de antenas fixas, colocadas ao longo da rodovia funcionando como pontos de acesso à rede. Não existe qualquer ligação direta entre os veículos. Em um cenário de auto-estrada, a implantação dos equipamentos à beira da rodovia de maneira suficiente para permitir a cobertura necessária pode tornar uma solução bastante dispendiosa.
- **Arquitetura ad-hoc:** é considerada uma arquitetura ad-hoc quando não há qualquer uso de infra-estruturas para realizar a comunicação, sendo as ligações feitas diretamente entre os nós envolvidos. Fatores como velocidade ou densidade dos nós podem pôr em *check* o desempenho deste tipo de rede.
- **Arquitetura híbrida:** tem objetivo de retificar as falhas existentes nas duas arquiteturas anteriores, utilizando concomitantemente as arquiteturas ad-hoc e WLAN

As comunicações em VANETs são categorizadas em 4 tipos:

- Em veículos: pode ser utilizado para detectar a fadiga e/ou sonolência de um motorista que representa risco na segurança;
- Entre veículos: a comunicação V2V (veículo para veículo) pode fornecer uma plataforma de intercâmbio de dados para compartilhamento de informações de advertência de modo a alertar o motorista;
- Entre veículos e rodovia (V2I): permite atualização em tempo real do tráfego e fornece detecção e monitoramento do ambiente;

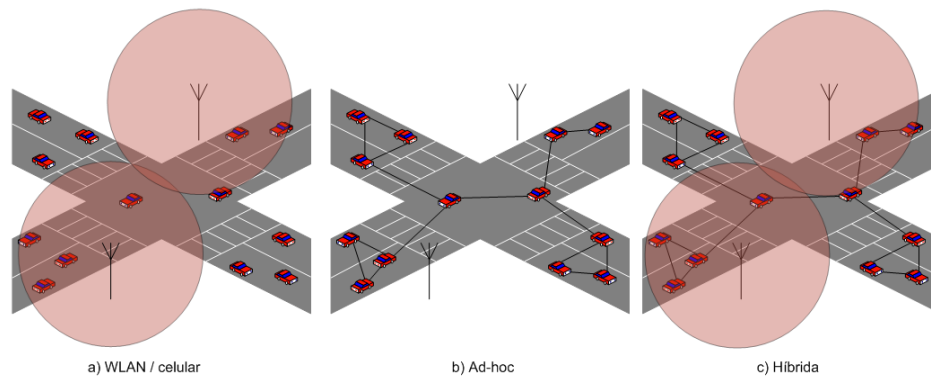


Figura 4 – Arquiteturas de redes veiculares(LUÍS, 2009)

- Entre veículo e nuvem: os veículos podem comunicar-se através da banda larga sem fio tais como 3G, 4G ou WIMAX podendo enviar dados para uma central, o que permitiria um controle mais abrangente do tráfego e assistência ao motorista

As aplicações VANETs podem ser divididas em 3 classes: segurança, entretenimento e assistência ao motorista. O principal desafio relacionado à segurança, está ligado à velocidade de alerta ao condutor, para que possa ter tempo hábil de reação. Nas aplicações de entretenimento, destacam-se os sistemas de compartilhamento de conteúdo e jogos. Já sobre a assistência ao motorista, são aquelas que auxiliam o condutor como por exemplo, através do uso de informações sobre as condições do trânsito (SOUZA RONIEL DE; SOARES, 2014).

4.2 Características e Desafios

Como mencionado anteriormente, as redes veiculares apresentam como principal característica a sua alta mobilidade e é justamente por isso que surge uma série de desafios a serem tratados. Dentre os maiores desafios encontram-se:

- **meio físico:** interferências devido à prédios, árvores e outros obstáculos;
- **alta mobilidade:** dificulta a troca de informações mais completas;
- **topologia:** VANET possui uma característica dinâmica, devido à velocidade que os veículos se movimentam;
- **baixa densidade:** quando a densidade de tráfego é baixa e os veículos estão distantes uns dos outros;

- **alta densidade:** muitos veículos em uma pequena área faz com que a quantidade de mensagens trocadas torne-se um problema;
- **segurança:** como as VANETs suportam aplicações de emergência em tempo real e lidam com informações críticas de segurança no trânsito, estas devem satisfazer os seguintes requisitos de segurança: confidencialidade, integridade, disponibilidade, autenticidade e não repudição para prover segurança na comunicação dos dados (SAMARA; AL-SALIH; SURES, 2010) (MATOS et al., 2013).

Cada um dos desafios relacionados está sendo tratado na arquitetura I9Vanet, uma vez que o objetivo da arquitetura é justamente ajudar a resolver tais problemas.

4.3 Segurança

Dito por Wingham et al , a segurança em redes veiculares é um fator crucial que precisa ser levado em consideração, pois a falta desta pode afetar a vida das pessoas. Como quaisquer redes de computadores sem fio e redes *ad-hoc*, estas estão sensíveis a ataques, tais como: negação de serviço, alteração de mensagens (RAYA; PAPADIMITRATOS; HUBAUX, 2006).

Para construir uma arquitetura de segurança robusta para redes veiculares, é necessário estudar as peculiaridades dos ataques que podem ocorrer. Do mesmo modo que as redes clássicas, as VANETs são vulneráveis a muitos ataques. Alguns destes ataques são encontrados e soluções são concebidas, considerando que um dia estes ataques podem ser lançados sobre a rede (ENGOULOU et al., 2014). De acordo com Wingham et al., os principais ataques analisados na literatura são: ataques contra a disponibilidade; ataques contra a autenticidade e a identificação; ataques contra a integridade e confiança dos dados; ataques contra a confidencialidade; entre outros.

4.3.1 Ataques contra a Disponibilidade

- **Negação de serviço (DoS):** este ataque tem como objetivo evitar que veículos autênticos acessem aos recursos da rede não permitindo a troca de informação. Um atacante pode proceder de 3 maneiras: sobrecarregando um nó específico da rede com informações deixando-o extremamente ocupado; atacando o canal de comunicação

gerando altas frequências adicionando ruído e impossibilitando a troca de informações entre os veículos; o não repasse de pacotes para outros veículos da rede, fazendo com que a informação não seja propagada para os outros nós.

- **Negação de serviço distribuída (DDoS):** possui o mesmo objetivo do DoS, ou seja, indisponibilidade de recursos porém, o ataque parte de diferentes localizações e em horários distintos como mostra a figura 5, onde veículos (B, C e D) enviam uma grande quantidade de pacotes contra uma unidade RSU ocasionando sua indisponibilidade.

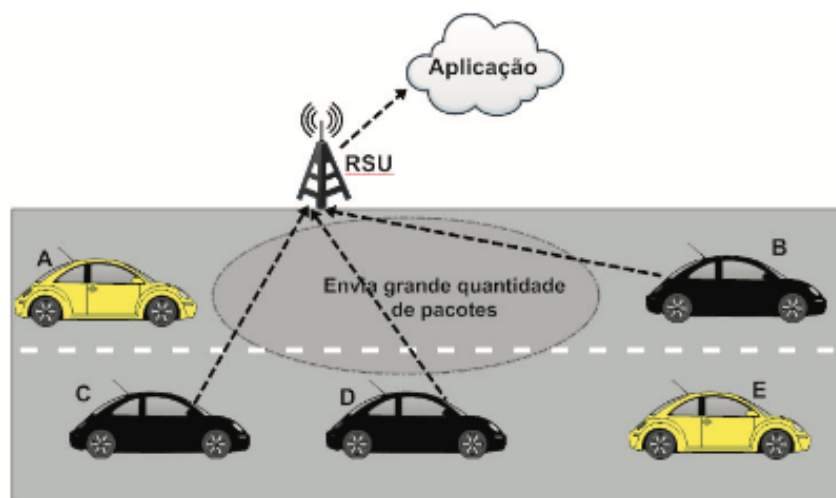


Figura 5 – Ataque DDOS (WANGHAM et al.,).

- **Supressão de mensagem:** o atacante recebe e não repassa pacotes da rede com objetivo de impedir que veículos seguintes possam saber de alguma ocorrência, por exemplo, um aviso de congestionamento, acidentes (TANGADE; MANVI, 2013).
- **Buraco Negro (black hole):** é uma área onde o tráfego de rede é redirecionado, contudo, ou não há veículos neste local ou nós maliciosos que estão nesta área se recusam a participar, fazendo com que os pacotes da rede não se propaguem. A figura 6 ilustra o ataque onde veículos se recusam a transmitir a mensagem recebida pelo veículo C.
- **Jamming:** é um ataque de negação de serviço através do meio físico, onde o atacante transmite um sinal para perturbar o canal de comunicação o que reduz a relação sinal ruído SNR (Signal to Noise Ratio) para o receptor. Segundo Avelar (AVELAR et al., 2015), o impacto com esse tipo de ataque é devastador.

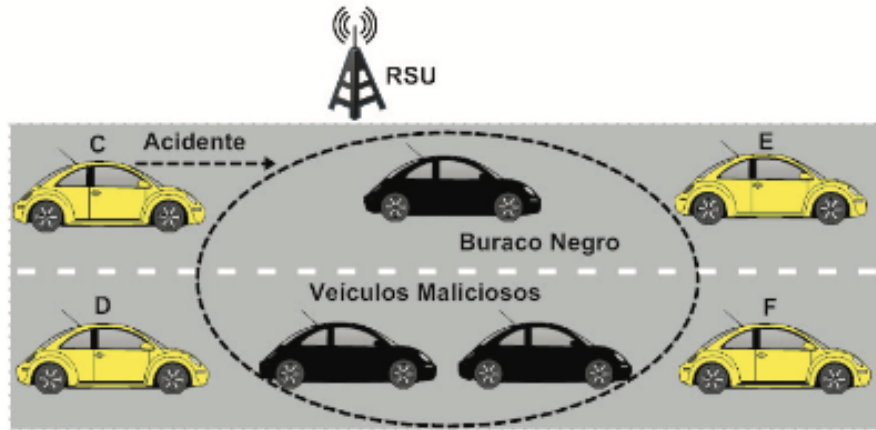


Figura 6 – Ataque Buraco Negro (WANGHAM et al.,).

4.3.2 Ataques contra a Autenticidade e a Identificação

- **Falsificação de endereço (*address spoofing*)**: o atacante cria um endereço falso de origem, fazendo com que o nó atacado confie no remetente achando que o mesmo possui permissão para conectar-se à rede (AL-KAHTANI, 2012).
- **Mascaramento**: ocorre quando um veículo malicioso falsifica sua identidade para se passar por outro com intuito de ter acesso a recursos restritos. Por exemplo, se passar por uma ambulância e ter vantagem no trânsito.
- **Replicação do certificado ou chave**: consiste em utilizar certificados ou chaves duplicados, que são usados como prova de identificação com objetivo de criar ambiguidade dificultando assim, a identificação de um veículo pelas autoridades (MEJRI; BEN-OTHTMAN; HAMDI, 2014).
- **Sybil**: é gerado múltiplas identidades por um atacante, para simular vários veículos e cada nó transmite mensagens com múltiplas identidades e assim sucessivamente. Desta maneira, um único veículo pode parecer centenas fazendo que com veículos reais mudem a rota achando que ali há um congestionamento (TANGADE; MANVI, 2013).

4.3.3 Ataques contra a Integridade e Confiança dos Dados

- **Falsificação nos dados de GPS (*GPS spoofing*)**: o atacante utiliza simulador de satélite GPS para gerar sinais mais fortes que o sinal originado de um satélite

real de maneira a enganar os sensores de GPS introduzindo um alocalização falsa (RAWAT; SHARMA; SUSHIL, 2012).

- **Ilusão (ataque contra os sensores do veículo):** Issac et al. (ISAAC; ZEADALLY; CAMARA, 2010) e Al-Kahtani (AL-KAHTANI, 2012) disseram que esse é um novo tipo de ameaça em aplicações VANET onde o atacante interfere intencionalmente nos sensores do seu próprio veículo gerando valores errados com objetivo de criar mensagens de aviso de tráfego incorretas na rede, assim, é criada uma condição de ilusão em VANET. Os métodos tradicionais de autenticação e integridade utilizados em redes sem fio são inadequados contra este tipo de ataque.
- **Injeção de informação falsa (*bogus information*):** neste tipo de ataque o atacante pode ser um usuário real ou um intruso que transmite informações falsas na rede para obter vantagens ou afetar decisão de outros veículos. Pode ser chamado de também de ataque social, onde o atacante procura confundir e distrair a vítima com envio de mensagens antiéticas para o motorista ficar confuso e distraído podendo causar um acidente como mostra a figura 7.

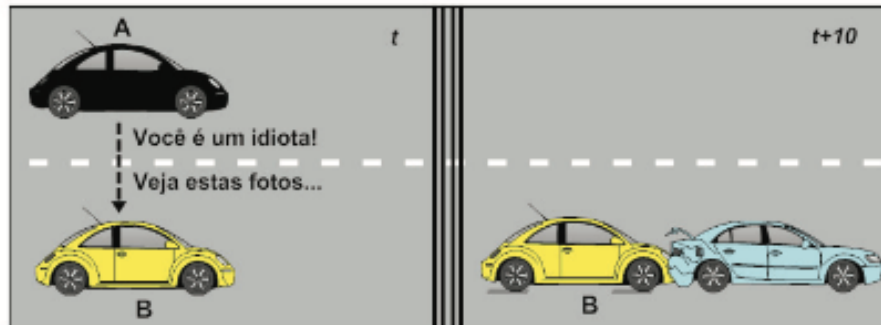


Figura 7 – Ataque social (WANGHAM et al.,).

- **Modificação de mensagem (*man in the middle*):** de acordo com Mejri et. al. (MEJRI; BEN-OTHMAN; HAMDI, 2014), este ataque a autenticidade do remetente e a integridade das mensagens onde o veículo atacante fica inserido entre dois veículos reais que se comunicam então, o atacante faz o intermédio entre a comunicação interceptando as mensagens enquanto estes acreditam estarem se comunicando diretamente. A figura 8 mostra o veículo malicioso M escutando a comunicação entre os veículos A e B, modifica um alerta recebido e propaga uma informação falsa, para os veículos B e C)

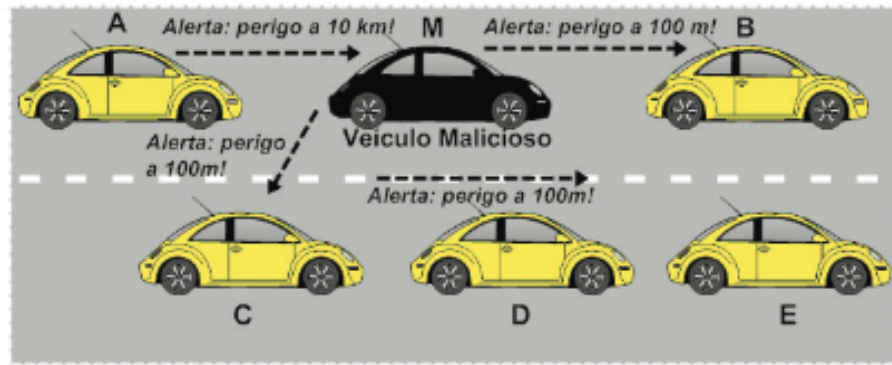


Figura 8 – Ataque demodificação de mensagem (WANGHAM et al.,).

4.3.4 Ataques contra a Confidencialidade

- **Análise de tráfego:** segundo Issac et. al. (ISAAC; ZEADALLY; CAMARA, 2010). esse é um ataque passivo utilizado em redes *ad-hoc*, onde o atacante que tenha acesso à rede pode interceptar o tráfego de pacotes coletando dados que estejam sendo transmitidos sem o uso de criptografia.
- **Força bruta:** tem como foco capturar mensagens trocadas ou ainda o processo de identificação e autenticação. Esse ataque não é trivial já que o tempo de comunicação entre os veículos é relativamente curto e esse ataque consome muito tempo (PATHRE, 2013).
- **Revelação de identidade:** normalmente, o motorista é o dono do veículo, então, o atacante pode obter a identidade do proprietário de um veículo violando sua privacidade (TANGADE; MANVI, 2013) e utilizá-lo para compor informações para um ataque social.

4.3.5 Outros Ataques

- **Ataques contra não repúdio (*accountability*):** consiste em tomar medidas para permitir ao atacante negar a realização de uma ou mais ação (WANGHAM et al.,). Apesar disso, Mejri et. al. (MEJRI; BEN-OTHTMAN; HAMDI, 2014), não foi encontrando na literaturam um documento afirmando a possibilidade desse ataque.
- **Ataques contra a privacidade:** estes tidos de ataques violam a privacidade dos usuários e condutores em redes veiculares. Segundo Wangharam et. al. (WANGHAM et al.,), estudos na literaturam classificam esses tipos de ataques como uma categoria

separada para VANETs e cita dois exemplos: rastreamento de veículo durante sua viagem e engenharia social, verificando se o veículos encontra-se em deslocamento ou parado (MEJRI; BEN-OTHMAN; HAMDI, 2014).

- **Conluio:** é o ataque que se utiliza de vários nós da rede com um objetivo comum, de realizar o vandalismo ou terrorismo, tendo como resultado a indisponibilidade da rede ou de algum serviço ou denegrir a reputação de confiança de um veículo (ZHANG, 2011).

As aplicações suportadas por VANETs com foco em segurança, permite a tomada de decisão por um condutor com base em informações enviadas por outros veículos. Entretanto, se um veículo malicioso cria ou altera mensagens, este pode colocar o motorista em situação de risco (WASEF et al., 2010). Dessa forma, a autenticidade das mensagens é fundamental para segurança das redes veiculares e dependendo da aplicabilidade, é necessário ainda fazer uso da criptografia (WANGHAM et al.,). Pensando nisso, vários autores (RAYA; PAPADIMITRATOS; HUBAUX, 2006) (MEJRI; BEN-OTHMAN; HAMDI, 2014) escolheram a assinatura digital como solução para autenticação das mensagens contidas nas redes veiculares.

O método mais simples e eficiente para assinatura digital, é atribuir, a cada veículo, um par chaves possibilitando assinar digitalmente as mensagens. Assim, é necessário utilizar uma autoridade certificadora confiável implicando no uso de uma Infraestrutura de Chaves Públicas (ICP) veicular (WASEF et al., 2010).

4.4 Algoritmos de Roteamento

Os algoritmos de roteamento em redes veiculares é um dos desafios estabelecidos, já que não existe rotas pré-definidas e nem estimativos da quantidade de nós de uma rede e o fator primordial que é a alta mobilidade dos nós. Então, como calcular as rotas necessárias para encaminhar os pacotes com sucesso, desde a origem até ao destino?

Foram realizados diversos estudos com a finalidade de comparar o desempenho dos algoritmos aplicados para redes móveis, de modo a corrigir as suas limitações, alguns sofreram adaptações, enquanto outros foram criados (LUÍS, 2009).

Dentre os principais algoritmos de roteamento, com foco nas redes veiculares, temos os protocolos: ad-hoc, baseados em localização, baseado em *clusters*, por *broadcast* e geocast

4.4.1 Protocolos Ad-hoc

As redes ad-hoc é caracterizada por ser um tipo de rede que não utiliza infra-estruturas e permite a mobilidade dos nós. Ao contrário dos outros protocolos de roteamento infra-estruturados, os quais não apresentam um desempenho aceitável para redes VANETs.

São tradicionalmente divididos em duas grandes categorias: reativos e pró-ativos. Os Reativos caracterizam-se pelo fato de nem sempre possuírem as rotas para todos os nós da rede. Quando um nó precisa de uma rota para um certo destino na rede, inicia o processo de descoberta de rota e é finalizado quando a rota é calculada com êxito ou não exista uma rota disponível. As rotas já descobertas são utilizadas enquanto o nó de destino permanecer alcançável ou não ser mais necessário. Os protocolos reativos mais conhecidos são AODV (*Ad hoc On Demand Distance Vector*) e o DSR (*Dynamic Source Routing*). Em contra partida, Boukerche ([BOUKERCHE, 2004](#)), afirmou que o desempenho dos protocolos AODV e DSR é bastante prejudicado pela constante alteração topológica da rede.

Os protocolos pro-ativos (*table-driven*) caracterizam-se por ter conhecimento das rotas para todos os nós existentes. Esse protocolo possui a vantagem de ter um reduzido atraso inicial, pois as rotas já estão estabelecidas. Não obstante, a metodologia dos protocolos pró-ativos implica na existência de um tráfego adicional para controle da topologia, uma vez que é preciso manter as rotas existentes sempre atualizadas, consumindo uma maior largura de banda. São exemplos de protocolos pró-ativos: DSDV (*Destination Sequenced Distance Vector*) e o WRP (Wireless Routing Protocol).

Os protocolos PRAODV (*PREemptive AODV*) e PRAODV-M (*PREemptive AODV - Maximum*) foram criados em cima do protocolo AODV, oferecendo uma componente baseado na velocidade, na localização e na predição. A diferença é que no PRAODV, é estabelecida uma ligação alternativa entre dois nós, antes da principal expirar, e a PRAODV-M, escolhe uma rota que prevê ficar ativa por mais tempo, ao contrário da AODV, que escolhe a rota mais curta ([LUÍS, 2009](#)).

O protocolo OLSR (Optimized Link State Routing), realiza uma otimização da topologia, sendo este, o algoritmo mais utilizado em redes ad-hoc (JACQUET et al., 2001). Possui um modo de funcionamento bastante característico, pois cada nó, seleciona dentre seus vizinhos, uma quantidade de nós suficientes de maneira a cobrir toda a vizinhança a dois saltos do nó, com objetivo de realizar o roteamento e retransmitir as mensagens.

4.4.2 Protocolos Baseados em Localização

Um dos primeiros protocolos baseados em localização foi o GPSR (Greedy Perimeter Stateless Routing), no qual baseia-se na informação geográfica em relação aos vizinhos. A vantagem deste protocolo está em manter a informação apenas sobre a topologia local, permitindo uma maior escalabilidade e um menor tempo para criação de novas rotas. Entretanto, o desempenho do GPSR é comprometido em ambiente reais, apresentando obstáculos e distribuição aleatória dos veículos.

O protocolo GSR (*Global State Routing*) foi criado com objetivo de corrigir a limitação do GPSR de modo a utilizar o *link-state* de forma que cada nó mantém uma tabela de conectividade, contendo todas as ligações existentes entre os diversos nós da rede, otimizando as decisões a nível de roteamento local. Avaliação feita por Füssler (FÜSSLER et al., 2003), indica que o GSR apresentou melhor desempenho em relação ao GPSR e melhora no atraso comparado ao DSR, do mesmo modo que, uma melhor taxa de sucesso de entrega e menor ocupação da largura de banda se comparado com o AODV (LI; WANG, 2007).

O protocolo A-STAR é baseado no GSP e GPSR e incorpora um sistema de sensibilização de tráfego (*traffic awareness*) fazendo uso de mapas das estradas ordenados por utilização, de forma a poder definir suas rotas pelas estradas com maior conectividade, na tentativa de aumentar a probabilidade de sucesso na entrega dos pacotes. Devido à sensibilização de tráfego aplicado ao A-STAR, há um melhor desempenho, entorno de 40%, na entrega de pacotes em relação ao protocolo GSR.

Foi proposto por Leontiadis et al (LEONTIADIS; MASCOLO, 2007), o protocolo de roteamento denominado GeOpps (*Geographical Opportunistic routing for vehicular networks*), ele assume que todos os nós estão munidos com sistemas de posicionamento de maneira a encaminhar um pacote para um nó que está, teoricamente, em melhores condições de poder entregar ao seu destino final. Segundo Karp et al. (KARP; KUNG,

2000), os resultados mostraram que o protocolo GeOpps tem um melhor comportamento do que o GPSR.

4.4.3 Protocolos Baseado em *Clusters*

Os protocolos de roteamento baseados em *Clusters*, representam uma rede virtual criada por meio de nós de uma rede física, onde o grupo criado, por um conjunto de nós interligados de maneira lógica, tem tendência a alterar rapidamente a sua composição.

Cada *cluster* pode apresentar um nó como líder, denominado *cluster-head*, que é incumbido de pela coordenação da comunicação dos nós da rede. Os nós de um cluster podem se comunicar diretamente porém, a comunicação extra grupo deve ser feita somente pelo líder. A criação dos *clusters* é de suma importância para aumentar a escalabilidade dos protocolos de roteamento e está na estabilidade a chave para o desempenho destes algoritmos (LUÍS, 2009).

Em redes veiculares, a aleatoriedade da movimentação dos veículos torna os protocolos de roteamento baseado em cluster para redes móveis frustrados tais como: *Adaptative Clustering* e o MCDS *Minimum Connected Dominating Set* (DAS; BHARGHAVAN, 1997).

Como dito anteriormente, o sucesso de um cluster está na estabilidade consequentemente, muitas pesquisas foram realizadas com objetivo de tornar o grupo o mais estável possível a exemplo do protocolo COIN *Clustering for Open IVC Networks* que utiliza informações sobre mobilidade para para formação do *cluster*. Entretanto, são adicionados ao algoritmo as intenções do motorista do veículo como também a dinâmica veicular. De acordo com Blum et al. (BLUM; ESKANDARIAN; HOFFMAN, 2003), resultados demonstram que as otimizações feitas molhoram o desempenho do protocolo, identificando um aumento de 192% no tempo médio de vida de um *cluster* e uma redução de 42% no número de alterações dos integrantes do grupo.

O protocolo CBLR (*Cluster-Based Location Routing algorithm*) apresentado por Santos et al. (SANTOS; EDWARDS; EDWARDS, 2004), utiliza conceitos de *cluster* juntamente com informações de localização. Este protocolo, se comparado ao AODV e DSR, desmostrou um desempenho superior ao atraso *end-to-end* e à taxa de sucesso de entrega.

4.4.4 Protocolos por Broadcast

Os protocolos de roteamento baseados em broadcast, consistem em transmitir informações por todos os nós que façam parte da rede. Em VANETs, este tipo de defusão é muito utilizado para compartilhar informações sobre o tráfego, condições da estrada, condição do clima, entre outros (LUÍS, 2009). Assim, fica garantido que todos receberam a informação. Entretanto, o funcionamento destes protocolos não é indicado para redes consideravelmente grandes, podendo gerar um efeito de tempestade de broadcast (broadcast storm), aumentando a probabilidade de colisões de pacotes e o consumo da largura de banda, comprometendo o desempenho.

O protocolo BROADCAST COMM (*BROADCAST COMMUNICATIONS*) apresenta algumas semelhanças com os protocolos baseados em clusters ao dividir a auto-estrada em células e utilizar o conceito de *cluster-head*, aqui chamando de *cell-reflectors* (DURRESI; DURRESI; BAROLLI, 2005). Neste caso, a diferença é que as *cell-reflectors* devem ficar geometricamente no centro da célula. A função do *cell-reflectors* é difundir as informações de emergências entre as células. Contudo, este protocolo funciona apenas para ambiente de auto-estrada.

4.4.5 Protocolos Geocast

O protocolo de *Geocast* (*Geocast Routing*) leva em consideração a posição/localização, e seu objetivo é entregar um pacote a nós que estão em uma determinada região denominada ZOR (*Zone of Relevance*). A implementação deste protocolo deve levar em consideração, a integração de um serviço de multidifusão em conjunto com o agrupamento dos nós conforme seu posicionamento geográfico, criando assim as ZORs.

Uma implementação do algoritmo *Geocast* foi utilizado na construção do protocolo *Message Dissemination Process* proposto por Briesemeister et al. (BRIESEMEISTER; SCHAFERS; HOMMEL, 2000), cuja objetivo é evita colisão de pacotes e diminuir o número de retransmissões. No momento que um nó recebe um pacote, ele não o encaminha imediatamente esperando um tempo de modo a poder tomar uma decisão referente à retransmissão. O tempo de espera é baseado na distância do nó que lhe enviou o pacote, ou seja, quanto maior a distância menor é o tempo de espera. Quando o período de tempo expira, o pacote somente é retransmitido se a informação não tiver sido recebida novamente.

Esse controle no envio dos pacotes faz com que seja menos provável a existência de *broadcast storms* e a propagação de pacotes seja mais eficiente.

Os protocolos DRG (*Distributed Robust Geocast*) e ROVER (*RObust Vehicular Routing*) projetados por Kihl et al. (KIHL; SICHITIU; JOSHI, 2008), sendo o DRG um protocolo com foco em grandes cenários, adaptável às constantes mudanças da topologia das redes veiculares e fornece um sistema de encaminhamento rápido e confiável. Em contra partida, o protocolo ROVER oferece uma difusão *multicast* confiável, tendo como base, um processo de descoberta de rotas dentro da ZOR.

4.4.6 Comparação dos Protocolos de Roteamentos

Ainda não foi encontrada a melhor forma de se criar um protocolo de roteamento para VANETs, porém, há autores que consideram um roteamento baseado em cluster mais viável em relação aos outros modelos (LUÍS, 2009). A aplicabilidade do protocolo faz aumentar o número de pesquisas existentes sendo que, se há alguns protocolos que possuem desempenho favorável em cenários urbanos, isso já não acontece em ambientes de alta mobilidade, e vice-versa. A tabela 1 faz um apanhado geral sobre os protocolos de roteamento e os cenários mais indicados.

Protocolo de Roteamento	Tipo Protocolo	Informação Sobre Estrutura Hierárquica	Cenário de Mobilidade
AODV	Unicast	Não	—
DSR	Unicast	Não	—
OLSR	Unicast	Não	—
PRAODV-M	Unicast	Seleção de rotas	Auto-estrada
GPSR	Unicast	Encaminhamento de Pacotes	—
GSR	Unicast	Encaminhamento de Pacotes	Urbano
A-STAR	Unicast	Encaminhamento de Pacotes	Urbano
GeOpps	Unicast	Encaminhamento de Pacotes	Urbano

COIN	Unicast	Formação de Cluster	Sim	Auto-estrada
CBLR	Unicast	Encaminhamento de Pacotes	Sim	Circuito circular e quadrangular
BROADCOM	Broadcast	Formação de células	Sim	Auto-estrada
Msg. Proc.	Diss. Geocast	Encaminhamento de Pacotes	Não	Auto-estrada
DRG	Geocast	Encaminhamento de Pacotes	Não	Auto-estrada
ROVER	Geocast	Encaminhamento de Pacotes	Sim	Auto-estrada

Tabela 1 – Protocolos de roteamento aplicados a redes veiculares (LUÍS, 2009)

4.5 Aplicações

Há uma série de aplicações que as redes veiculares podem atuar porém, para cada aplicação é necessário conhecer as características que as cercam, tais como: segurança da informação; tempo de resposta; garantia na entrega; entre outros.

Segundo Dantas (2011) (DANTAS, 2011), há uma relação entre velocidade dos veículos e a distância entre eles, esta relação é diretamente proporcional indicando que quanto maior a velocidade, maior deve ser a distância entre os veículos. Isto ocorre naturalmente, pois o motorista precisa considerar-se seguro no trânsito. Porém, esta condição é dinâmica variando a cada instante, e para agravar, a relação entre velocidade do fluxo e a distância dos veículos relaciona um fator de realimentação positiva, e sistemas com esta característica, tendem à instabilidade, gerando transtornos no trânsito. Então, um sistema capaz de alertar o motorista caso o mesmo esteja a distância “não segura” do veículo da frente, pode ser alcançado com sistemas baseados em VANETs.

Outra aplicação, com foco em redes veiculares, pode ser produzida por meio de alertas de colisão em uma via de fluxo intenso, o condutor possui um tempo de percepção mais um tempo de reação e somente após a soma dos tempos, poderá executar uma reação.

Esta situação mostra a importância de agregar aos veículos uma rede de comunicação no qual os mesmos e seus motoristas, poderão trocar informações de ocorrências emergenciais e preventivas no trânsito. Esta situação fica claramente evidenciada na figura 9.

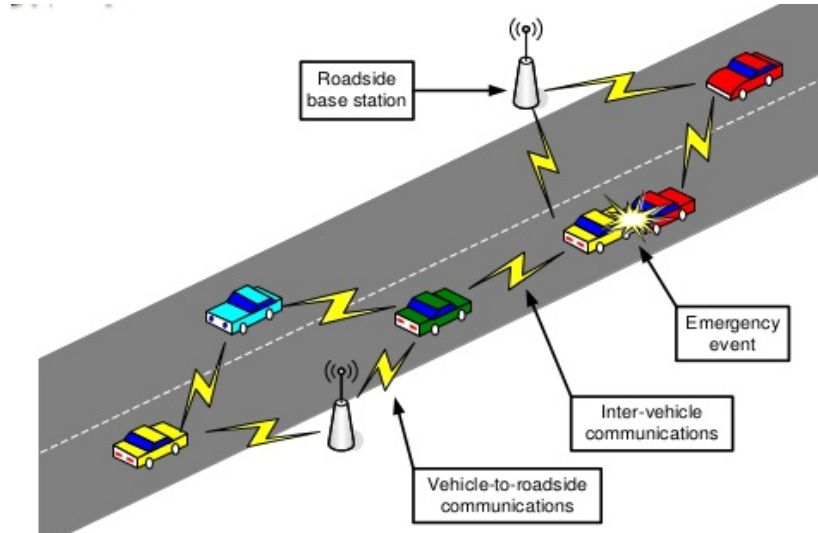


Figura 9 – Exemplo de aplicação VANET (QIAN; LU; MOAYERI, 2008).

Há também a possibilidade de aplicações voltadas para o entretenimento com o uso de *chats* ou até mesmo propagandas comerciais nas proximidades do veículos.

Por ser uma área crescente, as redes veiculares tem atraído empresas automobilísticas e órgãos controladores a exemplo do órgão americano de pesquisa de inovação tecnológica, RITA (*Research and Innovative Technology Administration*) o qual é coordenado pelo departamento de transporte dos EUA. O projeto Car 2 Car (*Communication Consortium*), criado por cinco fabricantes de automóveis europeus (BMW, Volvo, Volkswagen, Honda, e Audi) e apoiada por fornecedores de equipamentos, organizações de pesquisa e outros parceiros, tendo como objetivo aumentar ainda mais a segurança e a eficiência do tráfego rodoviário através de Sistemas de Transporte Inteligente (C-ITS) cooperativos com a comunicação veículo para veículo (V2V) suportada pela comunicação veículo infraestrutura (V2I) .

5 Arquitetura I9Vanet

5.1 Visão Geral

A arquitetura proposta tem a finalidade de criar redes veiculares virtuais em nuvem com foco no auxílio dos principais desafios relacionados à VANETs tais como: alta densidade, baixa densidade, alta mobilidade, segurança e privacidade, entre outros.

A arquitetura consiste em um modelo aberto, dividido em módulos com funções bem definidas. Cada módulo possui funcionalidades específicas e padrões de comportamentos. Sendo possível estender suas operações ou até mesmo substituí-las de maneira que atenda às novas necessidades.

5.2 Módulo da Arquitetura I9Vanets

A Figura 10 mostra os módulos necessários da arquitetura I9VANETS: *Applications*, *Server Management Cloud*, *Routing between Nodes*, *Security OBU/RSU*, *Infra-Cloud Communication* e *Vehicle-Cloud Communication*. Sendo que cada módulo segue um modelo de arquitetura com objetivos bem definidos, sendo que suas interfaces de comunicação são padronizadas, permitindo substituir um módulo por outro, com a mesma característica, sem que interfira no modelo.

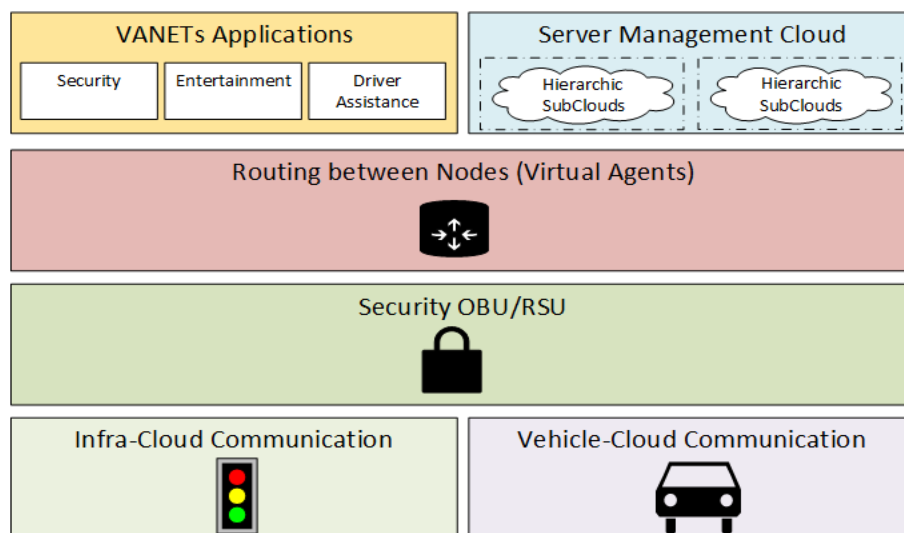


Figura 10 – Módulos definidos para a arquitetura I9Vanet.

Todas as classes que podem ser customizadas tais como: a tecnologia de comunicação; algoritmo de roteamento; modelo de segurança; implementação de eventos, devem estar definidas no arquivo de configuração **idclassload.properties** como os itens abaixo.

- **ICommunication:**

br.com.virtualVanets.infraVehicle.communication.CommunicationWebSocketImpl

- **CommunicationV2A:**

br.com.virtualVanets.infracloud.communication.impl.CommunicationI2AImpl

- **CommunicationI2A:**

br.com.virtualVanets.infracloud.communication.impl.CommunicationI2AImpl

- **ListenerInfraEquipament:**

br.com.virtualVanets.applicationModel.listener.DefaultListenerInfraEquipament

- **ListenerVehicle:**

br.com.virtualVanets.applicationModel.listener.DefaultListenerVehicle

- **EventInfraEquipament:**

br.com.virtualVanets.infracloud.listener.SVVEventInfraEquipament

- **EventVehicle:**

br.com.virtualVanets.vehiclecloud.listener.SVVEventVehicle

- **SecurityModel:**

br.com.virtualVanets.security.I9Security

- **RouterNetwork:**

br.com.virtualVanets.infraVehicle.communication.CommunicationWebSocketImpl

5.2.1 Módulo de Comunicação

O módulo de comunicação é responsável por definir o modelo de troca de mensagens entre os servidores e os dispositivos OBU e RSU. Dessa forma, é possível mudar o protocolo de comunicação sem interferir na arquitetura.

5.2.1.1 Comunicação Infra-Cloud

A forma como a comunicação será efetivamente implementada, não é preocupação da arquitetura, cabe ao desenvolvedor utilizar a tecnologia (socket, webservices, websocket,

push, etc) que mais se adequa à sua necessidade e/ou região. As informações trocadas são de entrada e saída, portanto, os equipamentos RSU podem enviar como também receber informações dos servidores. Em VANETs, pode existir a comunicação entre veículos e dispositivos à beira da rodovia (V2I), todavia, não é o propósito desta arquitetura realizar, de forma direta, a comunicação entre os equipamentos contudo, será realizada entre os respectivos agentes virtuais .

Todos os equipamentos RSU serão virtualizados e representados por agentes virtuais. Sendo assim, pode haver a comunicação entre agente RSU e o agente do veículo (AV2AI), como também entre agentes RSUs (AI2AI), como mostrado na Figura 11.

Os dispositivos RSUs disponibilizam as seguintes informações: identificação, latitude, longitude, altitude, temperatura, pressão, umidade relativa do ar e um campo textual para informações extras. A plataforma prevê 3 operações:

- **Conectar:** realiza a conexão com o servidor, informando identificador do dispositivo, a latitude e longitude;
- **Enviar Mensagem:** envia mensagens para rede. O conteúdo das mensagens variam de acordo com a aplicação;
- **Disconectar:** fecha a conexão com o servidor.

Para implementar a comunicação entre o agente e o veículo (I2AI), é necessário implementar a classe abstrata **CommunicationI2A** e sobrescrever o método **sendMsg**. Esse método é executado pela arquitetura de maneira transparente e deve enviar o comando para o dispositivo.

5.2.1.2 Comunicação Veículo-Cloud

Define a comunicação entre os servidores e os equipamentos instalados nos veículos (OBU). Os detalhes da implementação podem ser substituídos permitindo utilizar a melhor tecnologia do momento. Assim como no módulo de Comunicação Infra-Cloud, a comunicação V2V não ocorrerá diretamente, como ocorre nos modelos tradicionais, ela será reatada através dos agentes virtuais, que nada mais são do que a representação virtual dos veículos. Desta forma, a comunicação se dará entre os agentes (AV2AV) e entre o agente e o veículo físico (V2A) este processo é exemplificado na Figura 11.

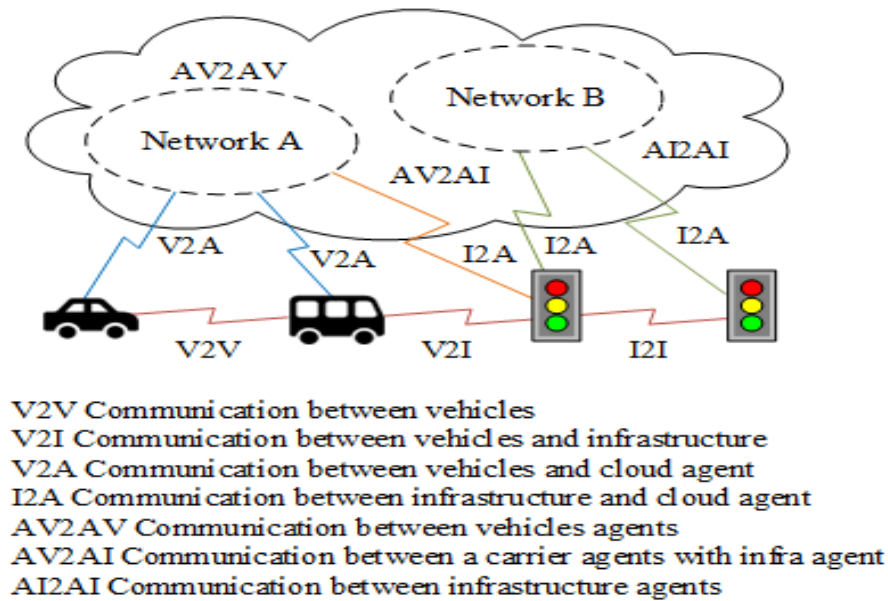


Figura 11 – Modelo de comunicação V2A, I2A, AI2AI e AV2AI.

O veículo deve disponibilizar as seguintes informações: identificação, latitude, longitude, altitude, velocidade, direção, tipo operação e um campo textual. A plataforma prevê 4 operações que podem ser extendidas, são elas:

- **Conectar** (CONNECT_CODE): realiza a conexão com o servidor, informando identificador do dispositivo, a latitude e longitude;
- **Movimentar** (MOVIMENTATION_CODE): este comando é executado a cada 10 segundos, com o intuito de informar a geolocalização, velocidade e direção do mesmo;
- **Enviar Mensagem** (SEND_BROADCAST_CODE): envia mensagens para os veículos da rede, sendo que o conteúdo das informações variam de acordo com a aplicação;
- **Desconectar** (DISCONNECT_CODE): fecha a conexão com o servidor removendo-o da rede.

Para implementar a comunicação entre o agente e o veículo (V2AV), é necessário implementar a classe abstrata **CommunicationV2A** e sobrescrever o método **sendMsg**. Este método é responsável por chamar a classe responsável pela conexão efetivamente definida.

5.2.2 Módulo de Segurança

A segurança na troca de informações em redes veiculares é um dos desafios que devem ser solucionado antes mesmo da implantação de uma solução VANET ser posta no mercado, então, como garantir os princípios da autenticidade, integridade, confidencialidade e não repúdio na troca de mensagens entre os veículos? Já que é inviável fornecer as chaves de segurança de todos os veículos durante a comunicação.

Na arquitetura I9Vanet, foi pensado em um processo de comunicação entre os equipamentos, OBU e RSU, e os servidores em Nuvem, de forma que deva garantir os princípios da autenticidade, integridade, confidencialidade e não repúdio através do uso de assinatura digital baseado em algoritmos assimétricos e criptografia dos dados toda via, este último foi definido de forma parametrizada para que fosse feito análise comparativo entre a comunicação aberta e criptografada.

A geração das chaves para cada equipamento deve ser controlado pelo órgão responsável pelos veículos, a exemplo, o DENATRAN (Departamento Nacional de Trânsito). Quando um novo veículo for cadastrado em sua base, “veículo zero quilômetro”, deve ser gerado as chave pública e privada, sendo que a pública deva ser enviada para os servidores em nuvem responsáveis pelo gerenciamento da arquitetura I9Vanets e a privada, inserida no equipamento.

A cada renovação de licenciamento, um novo token deve ser gerado e fornecido ao equipamento e publicado nos servidores. Como também, em caso de venda de um veículo, ao passar para o nome do novo proprietário, deve ser gerado um novo token.

Se o parametro de criptografia estiver habilitado, o primeiro passo no momento da conexão é a troca de chave secreta para que toda comunicação seja segura. Para isso, assim que o comando *onConnection* for executado, o servidor enviará o comando *createSecretKey* com a chave secreta criptografada com a chave pública do veículo assim, o mesmo poderá descriptografar com sua chave privada e utilizá-la na criptografia de cada mensagem de agora em diante.

No momento que um equipamento desejar enviar uma mensagem para seu agente em nuvem, ela deve ser asinada com sua chave privada, assim, através da verificação da assinatura com a chave pública, o agente poderá conviar no remetente. Porém, a mensgaem será asinada com a chave secreta do servidor para que o equipamento, OBU ou RSU, possa validar através da chave pública do servidor.

Alterar o modelo de segurança adicionando novas regras, é possível através da implementação da classe **ASecurityModel** e dos métodos **verifySign**, **sign**, **encrypt** e **decrypt**. A chamada dos métodos é feita pela arquitetura de maneira transparente, não sendo necessário intervenção do usuário.

5.2.3 Módulo de Gerenciamento dos Servidores

Não é possível prever a quantidade de veículos conectados a um servidor, e isto criou a necessidade de construir uma plataforma de gerenciamento com objetivo de aumentar a capacidade de dispositivos conectados à arquitetura. Então, pensando nisso, foi definido que os servidores devem ser distribuídos hierarquicamente de forma que permita controlar regiões, denominadas domínio, separadamente e independentemente. Cada servidor deverá conter informações do servidor pai, no caso, o servidor nível 0, o qual não possui pai. A figura 12 mostra como um exemplo de domínio, onde cada cerca representa um servidor.

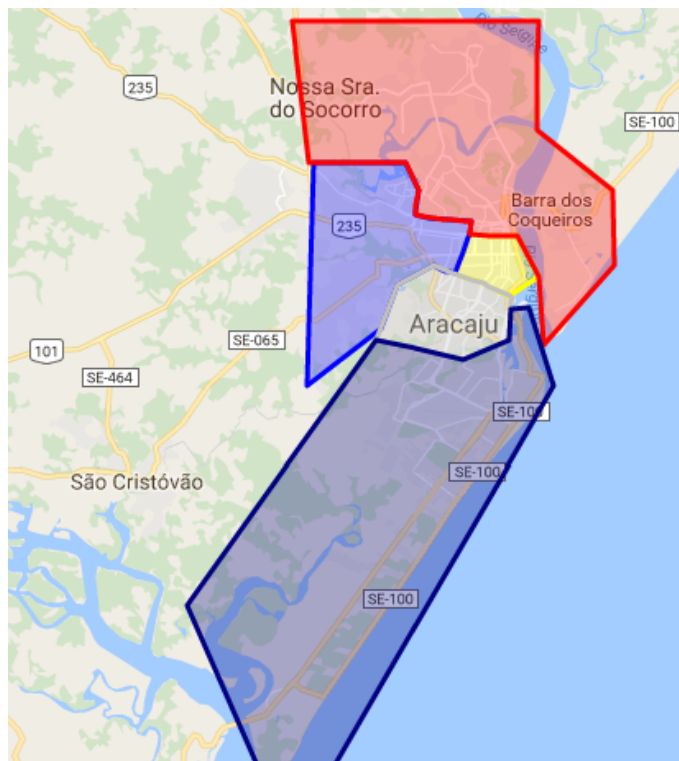


Figura 12 – Exemplo de domínios.

Quando um veículo iniciar a transmissão, será conectado automaticamente ao servidor Nível 0, informando o comando *StartConnection*, o qual realizará uma busca pela coordenada GPS enviada pelo veículo para localizar o servidor responsável pelo domínio onde encontra-se o veículo, podendo ocorrer duas situações:

1. O veículo apresenta-se em uma área sem cobertura de cerca virtual, assim, o próprio servidor raiz será responsável por gerenciar a rede VANET deste veículo;
2. O veículo encontra-se em uma domínio válido que é de responsabilidade de algum servidor filho. Então o servidor nível 0 irá passar o comando, *ChangeServer*, informando o ip do servidor que deve ser responsável pela rede dessa domínio, e assim o veículo faz uma nova conexão para o novo servidor.

Cada movimentação do veículo deve ser transmitida para o servidor do domínio, pelo comando *SendMoviment*, o qual verificará se o veículo ainda está em sua região, de acordo com a cerca virtual. Caso não esteja mais sob seu domínio, o servidor irá enviar o comando *ChangeServer* com o endereço do servidor Pai. Assim, o veículo poderá refazer a conexão com este novo servidor, através do comando *StartConnection*, o qual deverá verificar se a coordenada pertence a este servidor ou de algum de seus filhos, este processo é realizado para todos os níveis da hierarquia.

Em todos os servidores deve existir uma base de dados para definir a hierarquia, os domínios geográficos como também o cadastro dos dispositivos. As tabelas 2 e 3 mostram respectivamente o dicionário de dados da tabela *server* e *device* utilizadas no sistema.

Tabela <i>Server</i>		
Coluna	Tipo do Dado	Descrição
server_id	<i>integer</i>	Identificador único no sistema
address	<i>varchar</i>	Endereço Ip do servidor
server_idsuper	<i>integer</i>	Identificador do servidor pai
dominio	<i>polygon</i>	Cerca virtual de responsabilidade do servidor

Tabela 2 – Colunas das tabelas *Server*.

Tabela <i>Device</i>		
Coluna	Tipo do Dado	Descrição
device_id	<i>integer</i>	Identificador único no sistema
identification	<i>varchar</i>	Identificador do dispositivo (Imei, Mac Address, etc.)

type	<i>char</i>	Tipo do dispositivo (OBU ou RSU)
public_key	<i>byte[]</i>	Chave pública do dispositivo
	<i>integer</i>	

Tabela 3 – Colunas da tabela *Device*.

A Figura 13 mostra como os servidores devem ser organizados para melhor controle. O servidor nível 0 é a raiz da árvore e responsável por gerenciar os nós abaixo dele. A estrutura não é um uma árvore binária e sim uma formação em árvore com N nós filhos. Quando um veículo que está conectado a um servidor precisar conectar-se a outro, a mudança deve ser solicitada ao servidor pai imediato, caso este não seja o de destino, deve perguntar ao pai deste e assim sucessivamente até encontrar o servidor responsável pelo domínio de destino ou o servidor nível 0 será responsável por este gerenciamento. .

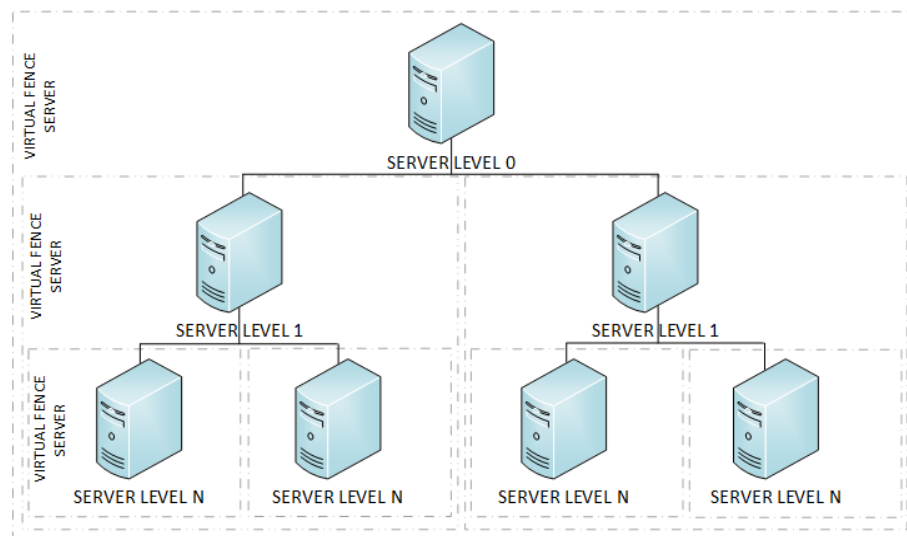


Figura 13 – Organização dos servidores na nuvem.

A cada envio do comando *SendMoviment* pelos veículos, o servidor deve verificar se o mesmo ainda encontra-se no mesmo domínio, como este processo é executado a cada 10 segundos por cada veículo, foi necessário realizar essa consulta em memória ao invés de ir no banco. Para isso, foi utilizado a API GEOTools.

O GeoTools é uma biblioteca feita em Java *open source* que provê ferramentas para manipulação de dados geoespacial em memória. O objetivo da biblioteca é permitir que programadores que estejam desenvolvendo aplicações geoespaciais se concentrem na

construção do negócio fim, enquanto reutilizam ferramentas genéricas para funções básicas (HALL; LEAHY, 2008).

A mesma funcionalidade do GeoTools poderia ser atingida com o as funções do Postgis porém, ao realizar pequenos testes, foi percebido que o tempo da consulta é 10 vezes maior que a do GeoTools, o que poderia comprometer a avaliação da arquitetura.

5.2.4 Módulo de Roteamento

O módulo de roteamento em ma rede veicular é um dos grandes desafios e por isto, é foco de estudos na busca de soluções que viabilizem a rede. Na arquitetura I9Vanet proposta, essa preocupação está presente porém, a plataforma permite criar novos algoritmos sem a necessidade de preocupar-se com detalhes como, segurança, protocolo de comunicação ou quantidade de veículos.

Toda comunicação entre os nós é realizado entre os agentes virtuais da rede (AV2AV e AV2AI e AI2AI). As regras de roteamento podem ser substituídas ou expandidas, basta implementar novos algoritmos seguindo o modelo da arquitetura do módulo. Quando houver a necessidade de enviar algo para algum nó físico da rede, esta mensagem deve ser enviada através do Módulo Comunicação Veículo-Cloud ou Infra-Cloud e eles se responsabilizarão pela entrega.

O módulo e roteamento pode ser definido de acordo com a necessidade, bastando implementar a classe **RouterNetwork** porém, para fins de avaliação da arquitetura, foi construído o algoritmo conhecido como *geocast routing*, no qual o objetivo é entregar um pacote aos nós que pertencam a uma certa região, denominada *Zone of Relevance* que utiliza um OBU como nó cabeça de uma rede veicular.

Os veículos quando iniciam o processo de conexão com o servidor, buscam uma rede já existente para se conectar. O veículo “cabeça” desta rede, deve estar a uma distância máxima de 1 KM e seguir na mesma direção na via, caso contrário, este veículo criará uma nova rede esperando que novos veículos solicitem acesso.

A cada transmissão de um veículo, através da operação **MOVIMENTATION_CODE**, o algoritmo de roteamento seguirá uma dentre três opções, são elas: permanecer na rede atual; entrará em uma nova; criará uma nova rede veicular.

**** Adicionar Figuras mostrando as 3 possibilidades da rede

5.2.5 Módulo de Aplicações

Permite adicionar novas aplicações tendo como base os recursos disponibilizados pelos outros módulos. Porém, para que as aplicações possam enviar e receber informações da arquitetura, é necessário definir um contrato com as classes da arquitetura, através do uso de interfaces e classes abstratas. Sendo assim, quando um veículo enviar uma informação para seu agente virtual, a arquitetura irá executar um método padronizado de uma classe da aplicação, fazendo com que os dados sejam entregues corretamente.

Podem ser implementados vários tipos de aplicações com os dados que a arquitetura já disponibiliza porém, caso seja necessário que uma aplicação possa modificar os dados de entrada e saída da arquitetura, é possível utilizar o campo mensagem para adicionar novas informações e assim atender às novas demandas.

5.3 Processo de Negócio

A figura 14 e 15 mostram os diagramas de processos de negócio da arquitetura I9Vanet com e sem criptografia respectivamente. No primeiro processo, o início, figura 14(1), se dar quando o veículo é ligado e abre a primeira conexão com o servidor raiz, figura 14(2). Em seguida, o processo de negociação da chave a ser utilizada na criptografia figura 14(3), a chave é criptografada, pelo servidor com a chave pública do veículo e enviada para o nó da rede, figura 14(4). A partir deste momento, toda comunicação será criptografada e em ambos os modelos, toda mensagem será assinada.

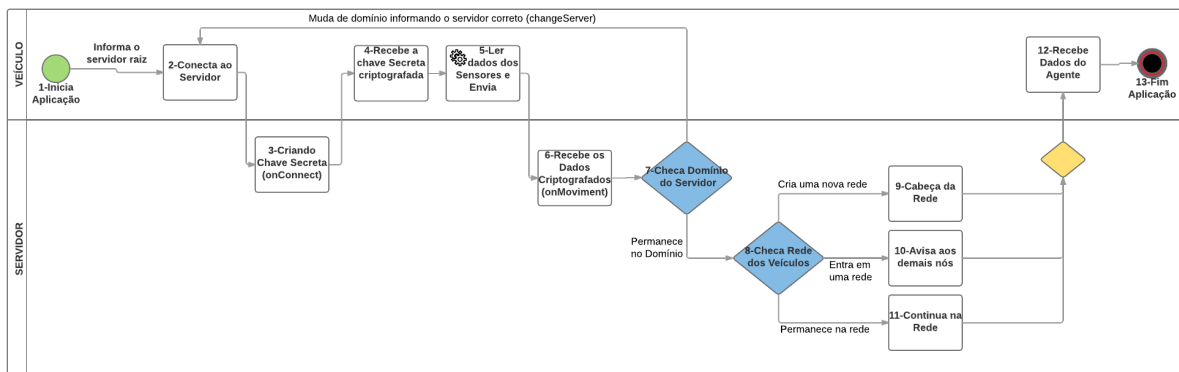


Figura 14 – Modelo de processo de negócio da arquitetura I9Vanet com criptografia.

Após estabelecido o canal seguro, é iniciada uma thread, figura 14(5), responsável por obter os dados dos sensores do veículo e enviá-los para o servidor, figura 14(6), dentre

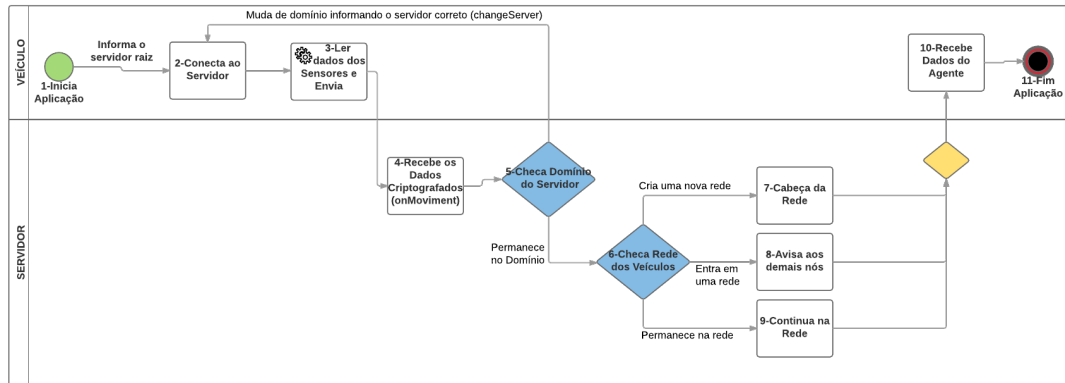


Figura 15 – Modelo de processo de negócio da arquitetura I9Vanet sem criptografia.

os dados estão a latitude, longitude, velocidade e direção. O recebimento dos dados é feito pelo método **onMovement** que irá verificar o em qual domínio o servidor deve ficar conectado, figura 14(7), se a coordenada geográfica indicar que o veículo deve mudar de servidor, então, o comando **changeServer** é acionado informando o endereço do servidor “pai”, voltando para o processo, figura 14(2), para recriar a conexão e segurança do canal. Caso permaneça no mesmo domínio, deve realizar uma análise sobre a rede que o veículo pertence, verificando se deve permanecer na rede atual, figura 14(11), cria uma nova rede, figura 14(9), ou entrar em uma outra, 14(10).

O processo de execução da rede em si, não está mapeado nesse fluxo de processos já que as mensagens a serem trocadas entre os nós da rede, depende da camada da aplicação que está sendo desenvolvida.

6 Avaliação da Arquitetura

Este capítulo visa avaliar a arquitetura I9Vanets, através do paradigma GQM (Goal-Question-Metric) muito usado para planejar medições em projetos de softwares (SOLINGEN et al., 2002). As seguintes fases foram analisadas durante o processo de avaliação: fase de planejamento, de coleta de dados e de interpretação dos resultados.

O processo de avaliação iniciou-se na fase de planejamento com o intuito de analisar a arquitetura com relação à eficácia e eficiência da solução. O experimento teve como público alvo os desenvolvedores de software interessados na arquitetura como gerenciamento de uma rede VANET para ITS no contexto de cidades inteligentes.

Com base na proposta da arquitetura i9Vanets, foram realizados dois tipos de testes. O primeiro, com o intuito de avaliar a sua aplicabilidade em ambientes de redes veiculares reais, teve objetivo de avaliar o fluxo de dados referentes à velocidade das tecnologias atualmente utilizados na telefonia móvel, sendo 2G, 3G, 4G e 5G. O segundo teste objetivou dimensionar a capacidade de operação e o comportamento da arquitetura proposta a partir de um excessivas requisições, sem limite de limite de velocidade. Ambos os testes extraíram dados estatísticos a partir de métricas pré-definidas e planejadas.

6.0.1 Definição

Analisar a arquitetura i9Vanets com finalidade de avaliar sua eficiência, a respeito do tempo de latência e capacidade de processamento, do ponto de vista de múltiplos acessos concorrentes no contexto de redes veiculares em nuvem.

6.0.2 Planejamento

O experimento tem como alvo os desenvolvedores de soluções que visam melhorar mobilidade urbana com o uso de VANETs. Onde o objetivo foi avaliar a capacidade de processamento do servidor e medir o tempo de latência das comunicações da telefonia móvel, através das seguintes perguntas:

- Qual a taxa de processamento por minuto?
- Qual a latência média de cada requisição?
- Qual a latência média de cada requisição para as velocidades de 2G, 3G, 4G e 5G?

- A latência média com a mensagem criptografada irá aumentar em relação à não criptografada?
- Qual a capacidade de processamento da arquitetura I9Vanet ?

Para isso, serão utilizadas as seguintes métricas:

- número Total de requisições por min (TR/min);
- tempo de latência da comunicação (Lat);
- tempo de processamento de cada requisição no servidor (PT).

O tempo de latência representa o tempo que uma mensagem sai do ponto A para o ponto B, sendo que o tempo calculado pelo experimento foi o RTT (round trip time), tempo que a mensagem foi enviada e recebida de volta pelo veículo sendo considerado como latência, a metade do RTT.

De acordo com Papadimitratos et al (2008) , as aplicações voltadas para as redes VANETs possui alguns requisitos que devem ser respeitados e estão relacionados ao tipo de comunicação, ao tipo de mensagem, ao tempo de entrega, à latência (tempo de atraso máximo requerido) e a outros requisitos como mostra a tabela 4. Então, o objetivo do experimento é avaliar se o tempo obtido se adequa ao requisitos mostrados.

Tabela 4 – Características das aplicações veiculares.

Aplicações	Tempo	Latência	Outros
Alerta de Veículo Lento	500ms	100ms	Alcance: 300m, alta prioridade
Alerta de Colisão em cruzamento	100ms	100ms	Posicionamento preciso em um mapa digital, alta prioridade
Pré Colisão	100ms	50ms	Alcance 50m, prioridade alta/média
Gerenciamento de Cruzamento	1000ms	50ms	Precisão de posicionamento menor que 5m
Download de Mídia	–	500ms	Acesso a internet e Gerência dos direitos
Assistência para direção ecológica	1000ms	500ms	Acesso a internet e disponibilidade do serviço

6.1 Cenário Proposto

O ambiente proposto para avaliação consiste em simular movimentações de veículos na cidade de Aracaju-SE Brasil transmitindo e recebendo informações dos servidores que compoem a arquitetura I9Vanets.

Cada teste realizado, levou em consideração quantidades diferentes de dispositivos representando os veículos, sendo da seguinte forma: 50, 100, 200 e 400. Para cada faixa, também foi ajustado a largura de banda para definir a velocidade máxima de comunicação de cada dispositivo, seguindo os modelos 2G, 3G, 4G e 5G.

Todo o ambiente, tanto o cliente quanto os servidores, foi montado em máquinas virtuais. No caso dos servidores, foram criados 4 máquinas com linux ubuntu server 16.04 com o postgresql 9.5 e plugin postgis 2.0 e Glassfish 4.1.1 como servidor de aplicação. Todos os servidores possuíam a mesma configuração, sendo 1 GB de Ram e 2 processadores virtuais e foram executados em uma única máquina física cuja configuração está presente na tabela 16. A disposição dos servidores virtuais foi definido em dois níveis hierárquicos, sendo o servidor nível 0, a raiz da hierarquia e, como filhos, 3 servidores no nível 1.

Para simulação dos clientes, os OBUs e RSUs, foi utilizado máquinas virtuais com linux ubuntu server 14.04 LTS 32 bits com o Mininet 2.2.1 configurado. Cada rede virtual Mininet instanciou entre 25 e 50 hosts, para que seu desempenho não fosse comprometido. Todas as máquinas com Mininet utilizaram a mesma configuração: 2GB de RAM e 2 processadores virtuais. O modelo do ambiente é mostrado na figura 16.

Foi criado um script em Python, conforme Código 6.1 com intuito de automatizar a criação dos hosts, limitar largura de banda entre 2G, 3G, 4G e 5G, iniciar a execução da aplicação responsável por simular as funcionalidades dos OBUs e RSUs, realizar a comunicação com a arquitetura I9Vanet e registrar em log, os dados referentes à comunicação de cada host, em arquivos individuais.

Um host virtual tem a função de representar um veículo real, inclusive com uso de movimentações reais, coletadas por 12 meses, de um sistema de monitoramento de veículos de uma empresa de taxi com 102 carros, totalizando mais de 12 milhões de movimentações. A figura 17 mostra o exemplo do monitoramento do sistema de taxi.

A base de movimentação foi extraída, separada por veículo e em seguida, armazenada em arquivo e colocada em cada máquina Mininet para que cada host pudesse simular uma movimentação real. Cada arquivo de movimentação recebeu um número, por exemplo:

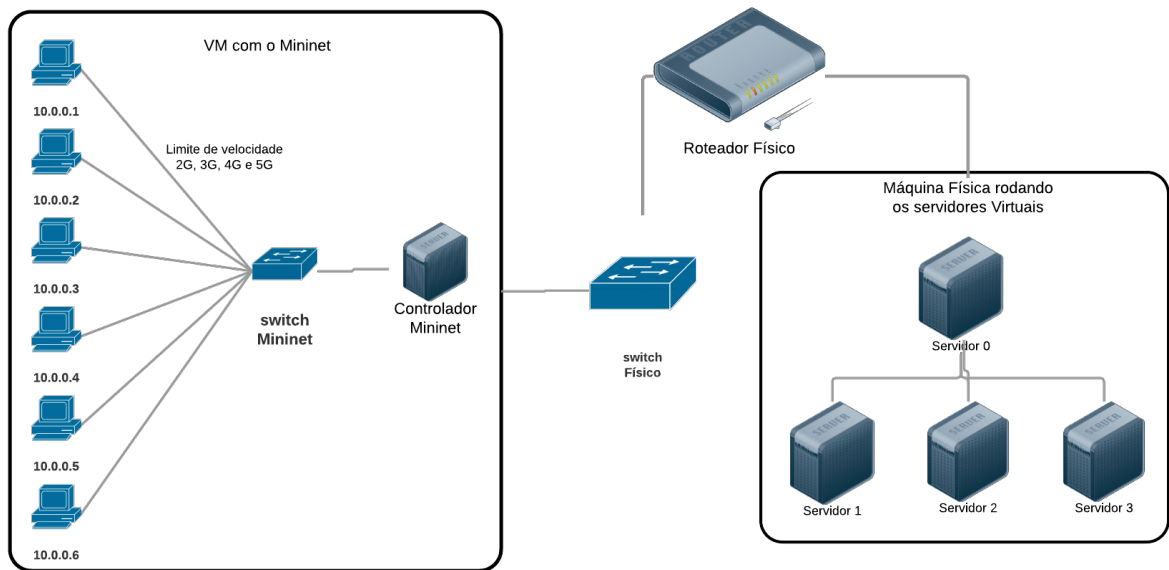


Figura 16 – Configuração do ambiente utilizado para a realização dos experimentos. Fonte: Criada pelo autor.

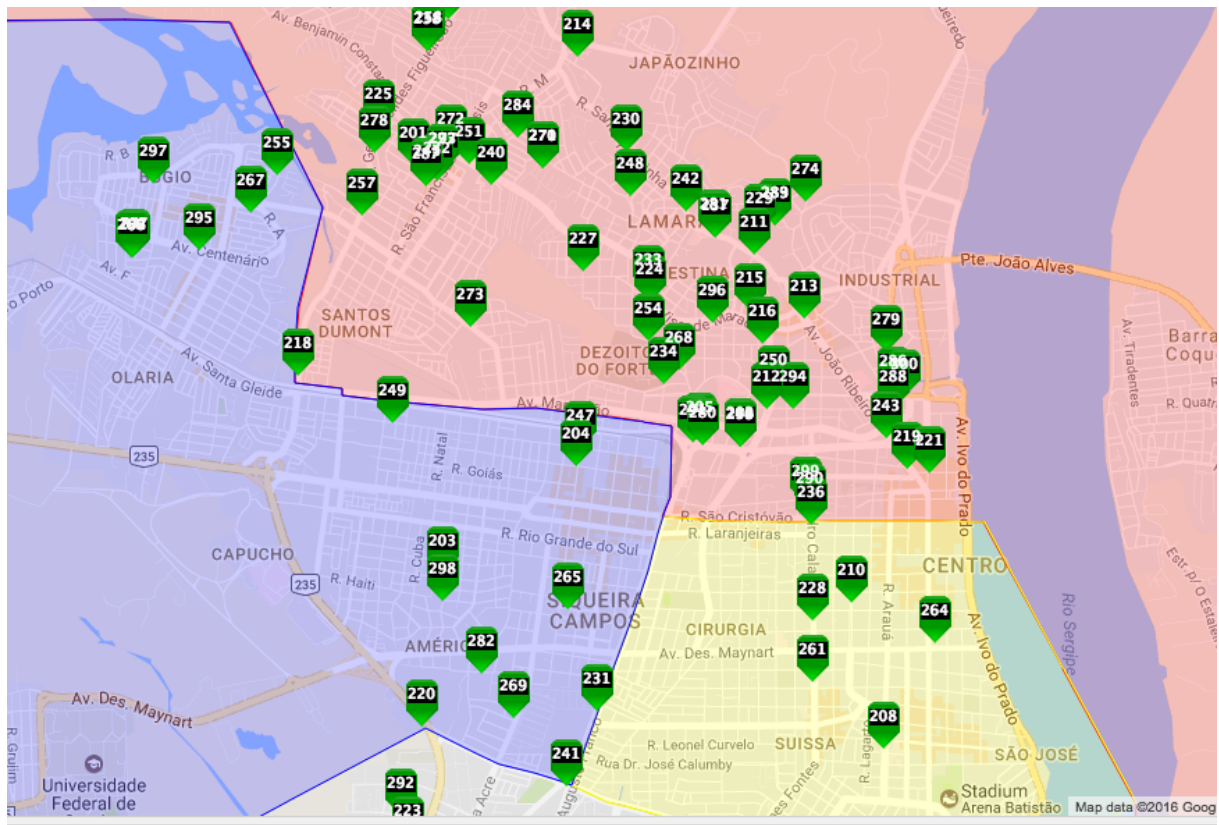


Figura 17 – Tela de monitoramento do Sistema TaxiFast.

1.csv, 2.csv e assim por diante. Assim, os host virtuais realizaram um sorteio entre os arquivos disponíveis para ler as informações de movimentação e transmiti-la para o servidor. A tabela 5 mostra exemplo do conteúdo de um arquivo de movimentação.

Latitude	Longitude	Velocidade
-10.9062183	-37.0619264	0
-10.906164143173685	-37.061813870099655	10.7
-10.904381347197752	-37.0671766923126	21.121
-10.904279005332516	-37.067784265675165	26.259
-10.904165425504841	-37.06846398328098	29.678

Tabela 5 – Linhas do arquivo de movimentação.

```

1  #!/usr/bin/python
2  ...
3  class SingleSwitchTopo(Topo):
4  def build(self, n=2):
5      switch = self.addSwitch('s1')
6      #Cria todos os hosts e conecta ao switch
7      for h in range(n):
8          host = self.addHost('h%s' % (h + 1))
9          self.addLink(host, switch)
10 def limit( bw=0.2, cpu=1 ):
11     intf = custom( TCIntf, bw=bw )
12     myTopo = SingleSwitchTopo(n=2)
13     for sched in 'rt', 'cfs':
14         if sched == 'rt':
15             release = quietRun( 'uname -r' ).strip('\r\n')
16             output = quietRun( 'grep CONFIG_RT_GROUP_SCHED /boot/config-%%
17                 s'
18             % release )
19             if output == '# CONFIG_RT_GROUP_SCHED is not set\n':
20                 continue
21             host = custom( CPULimitedHost, sched=sched, cpu=cpu )
22             net = Mininet( topo=myTopo, intf=intf, host=host)
23             net.addNAT().configDefault()
24             net.start()
25             # Para cada host criado, executa a aplicacao de simulacao
26             for host in net.hosts:
27                 if 'h' in host.name:
28                     host.cmd('java -jar SVVMMainTest.jar ' + str(host) + '.
29                         csv /home/mininet/vanet &')
30             CLI( net )
31 if __name__ == '__main__':
32     setLogLevel( 'info' )
33     limit()

```

Listing 6.1 – Script Python para criação dos hosts no mininet.

6.2 Experimentos

Ao iniciar cada teste do experimento, os hosts virtuais devem estabelecer a conexão com o servidor nível 0, contudo, se todos os "veículos" iniciarem a conexão ao "mesmo tempo" ocasionará uma sobrecarga tanto na máquina cliente quanto no servidor. Pensando nisso, foi implementando na aplicação cliente que antes de iniciar o processo de conexão, cada host obtém um número pseudo-aleatório entre 0 e 120000 (2 minutos), o qual será usado para dar uma pausa na aplicação pra depois iniciar o processo de conexão gerando assim, uma aleatoriedade inicial. Se por algum motivo a conexão do host cliente cair ou der *timeout*, ela será refeita automaticamente não considerando mais o tempo de pausa inicial.

***** Quais operações são realizadas a cada transmissão ver fluxo *****
Informar as velocidades de cada teste 2g, 3g, 4g, 5g

***** Por último foi executado o teste de stress sem o limite de banda - 800/10s=80/s
= 0,08s tempo médio de requisição, na prática o tempo ficou em 0,02s

As máquinas utilizadas no experimento pertenciam a um laboratório do Instituto Federal de Sergipe - Campus Lagarto e dois notebooks pertencente ao autor, cuja configurações estão presentes na tabela 6.

Maquina Cliente			
Sist Operacional.	Qnt.	Processador	Memória
Windows 7	12	AMD Phenom II X2 B57 3.20 GHz	4 GB
Mac OS Sierra	1	2,4 GHz Intel Core i5	8 GB
Maquina Servidora			
Sist Operacional.		Processador	Memória
Ubuntu 16.4	1	2,4 GHz Intel Core i7 GHz	8 GB

Tabela 6 – Configuração dos computadores utilizados no experimento.

Para cada cenário, 50,100,200 e 400 veículos, os *hosts* emulados seguiram a seguinte distribuição entre as máquinas clientes como mostra a tabela 7, tendo como preocupação o poder de processamento das máquinas físicas.

Cenário 50		
Máquina Física.	Qnt.	Nr Hosts Cada

Windows	2	25
Cenário 100		
Máquina Física.	Qnt.	Nr <i>Hosts</i> Cada
Windows	4	25
Cenário 200		
Máquina Física.	Qnt.	Nr <i>Hosts</i> Cada
Windows	6	25
Mac OS	1	50
Cenário 400		
Máquina Física.	Qnt.	Nr <i>Hosts</i> Cada
Windows	12	25
Mac OS	2	50

Tabela 7 – Configuração dos computadores utilizados no experimento em cada cenário.

Conforme dito anteriormente, foram definidos 48 cenários de testes levando em consideração quantidades de veículos, largura de banda da comunicação e a criptografia ou não dos dados.

6.3 Resultados

Inicialmente, os dados colhidos referentes à latência, foram avaliados quanto à sua normalidade, para verificar se a distribuição de probabilidade associada às amostras podem ser aproximada. Para tal, foi utilizado o Kolmogorov-Smirnov test (KS) tendo as seguintes hipóteses:

H0: Os dados seguem uma distribuição normal.

Ha: Os dados não seguem uma distribuição normal.

O resultado do teste KS aplicado às médias dos tempos de latência das requisições de cada *host*, indica que nenhuma das amostras apresentou uma distribuição normal a um nível de significância, comumente utilizado, de 0,05, rejeitando a hipótese H0, como mostrado na Tabela 8, apontando que a distribuição de probabilidade associada às médias das requisições não podem ser aproximadas.

Tabela 8 – Resultado do teste de análise de distribuição normal dos dados para cada quantidade de veículos e velocidades de acesso.

Qnt. Veículos	2G	3G	4G	5G
50	0,0	0,0	0,0	0,0
100	0,0	0,0	0,0	0,0
200	0,0	0,0	0,0	0,0
400	0,0	0,0	0,0	0,0
800	0,0	0,0	0,0	0,0
1600	0,0	0,0	0,0	0,0

Sob a ótica das variações entre as latências das requisições, podemos observar que nos cenários com 50 e 100 veículos, o coeficiente de variação foi baixa e acima de 200 veículos houve um crescimento no coeficiente. Isso aconteceu devido à maior quantidade de veículos presente nos testes e consequentemente, houve mais mudança de servidores, em média o tempo gasto para realizar a operação *changeServer* é de 2,5 segundos, conforme mostra a tabela 9.

Tabela 9 – Resultado do teste de análise dos coeficientes de variação.

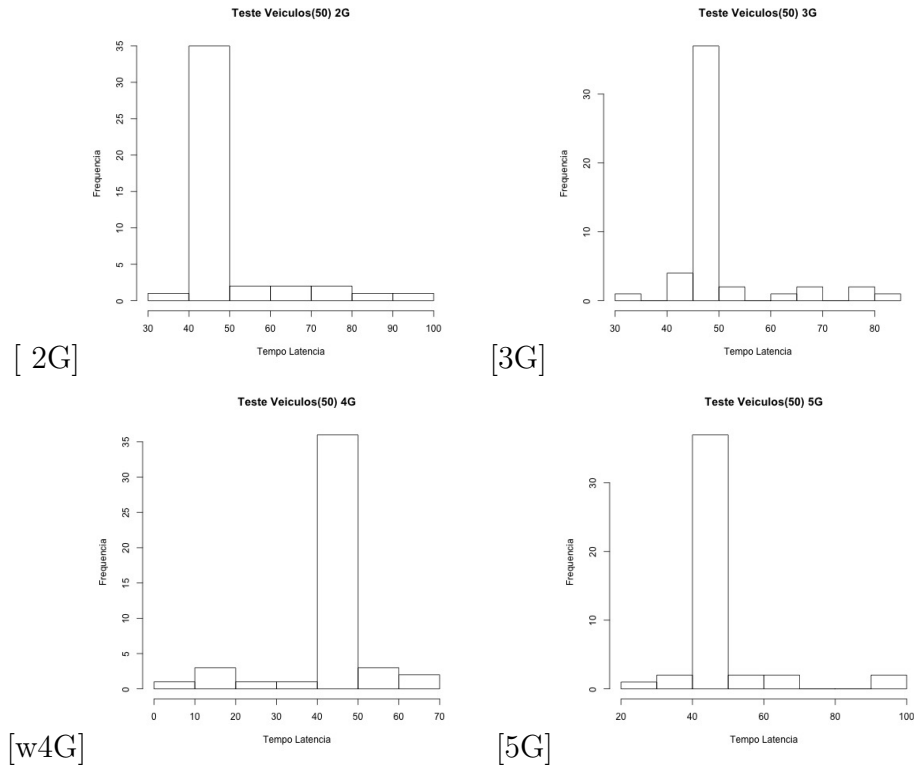
Qnt. Veículos	2G	3G	4G	5G
50	0.52360	0.5504	0.5751	0.5435
100	0.5340	0.5490	0.5630	0.5560
200	2.1970	2.5930	2.4360	2.3560
400	1.9220	2.1680	2.4270	2.5360

As imagens contidas na figura 18, mostram o histograma de frequência das médias das requisições para cada velocidade, 2G, 3G, 4G e 5G, para o teste com 50 veículos. Observou-se que não há uma relação de melhora nos tempos médios à medida que aumenta a velocidade de 2G para 5G. A concentração dos tempos permanecem na mesma referência, entre 40 e 50 milissegundos.

O cenário com 100 veículos apresentou gráficos semalhantes aos de 50, ou seja, o tempo médio das requisições não variou de acordo com o aumento da velocidade, conforme mostra a figura 19.

Entretanto, os testes com o cenário de 200 veículos, apresentou uma variação com a diferença de velocidades porém, de maneira inversamente proporcional, ou seja, de acordo com a figura 20, o teste com a velocidade 2G apresentou maior concentração entre o intervalo de 0 e 50 milissegundos. Com a velocidade de 3G a maior concentração dos tempos médios ficou entre 140 e 160 milissegundos.

Figura 18 – Análise de Histograma de Frequência do Teste com 50 veículos.



Da mesma maneira que o cenário com 200 veículos, o de 400 não apresentou uma relação lógica sendo que a velocidade 2G mostrou, de forma considerável, médias entre 600 e 700 milissegundos como mostra a figura 21.

Nas figuras 22, 23 e 24, é feito uma análise sobre os tempos mínimos, médios e máximos das médias das latências das requisições extraídas de casa cenário. Fica evidente que nos cenários de 50, 100 e 200 veículos simultâneos, os tempos mínimos, médios e máximos sofrem pequena variação porém, os tempos médios e máximos no cenário com 400 veículos com velocidade de 2G, há um aumento considerável em relação às outras velocidades, como mostra as figuras 23 e 24.

6.3.1 Taxa de Transferência

Os veículo enviam sua localização, através do comando *sendMoviment*, a cada 10 segundos sendo que a mensagem enviada variou entre 212 e 256 bytes e a média ficou em 233 bytes então, a tabela 10 mostra as velocidades de transmissão utilizadas em cada teste e a capacidade de operação de cada link testado.

Figura 19 – Análise de Histograma de Frequência do Teste com 100 veículos.

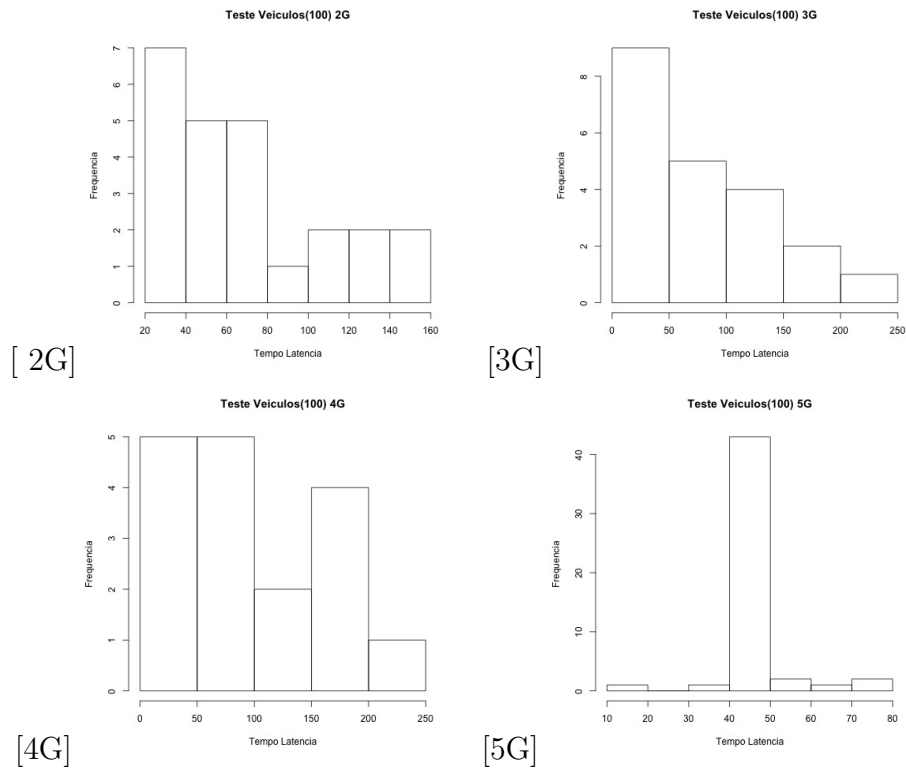


Tabela 10 – Velocidade de cada link por veículo.

Link	Lagura de Banda(kbps)
2G	400
3G	10.000
4G	100.000
5G	10.000.000

6.3.2 Processamento

Também foi avaliado o nível de processamento dos servidores, sendo que o servidor nível 0 chegou a 100% de processamento nos primeiros 2 minutos, no teste com 800 veículos, e depois reduziu para 20%, onde se manteve. Isso ocorreu devido à todas as conexões iniciais serem feitas para este servidor, como também quando há a necessidade de mudança de domínio, o servidor nível 0 é requisitado de acordo com a hierarquia estabelecida.

Figura 20 – Análise de Histograma de Frequência do Teste com 200 veículos.

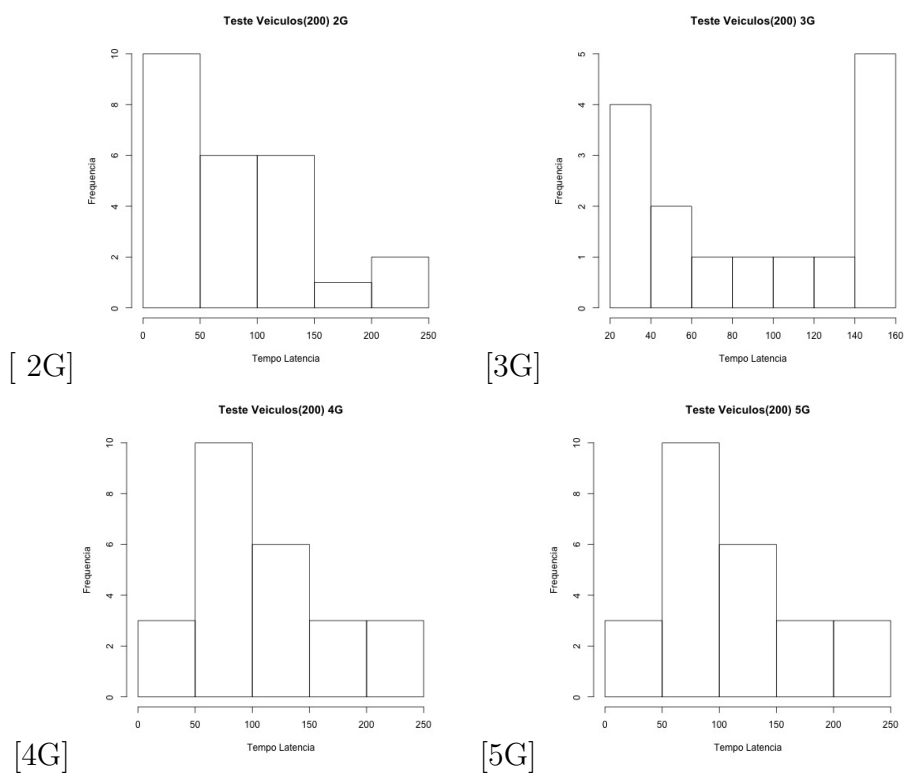
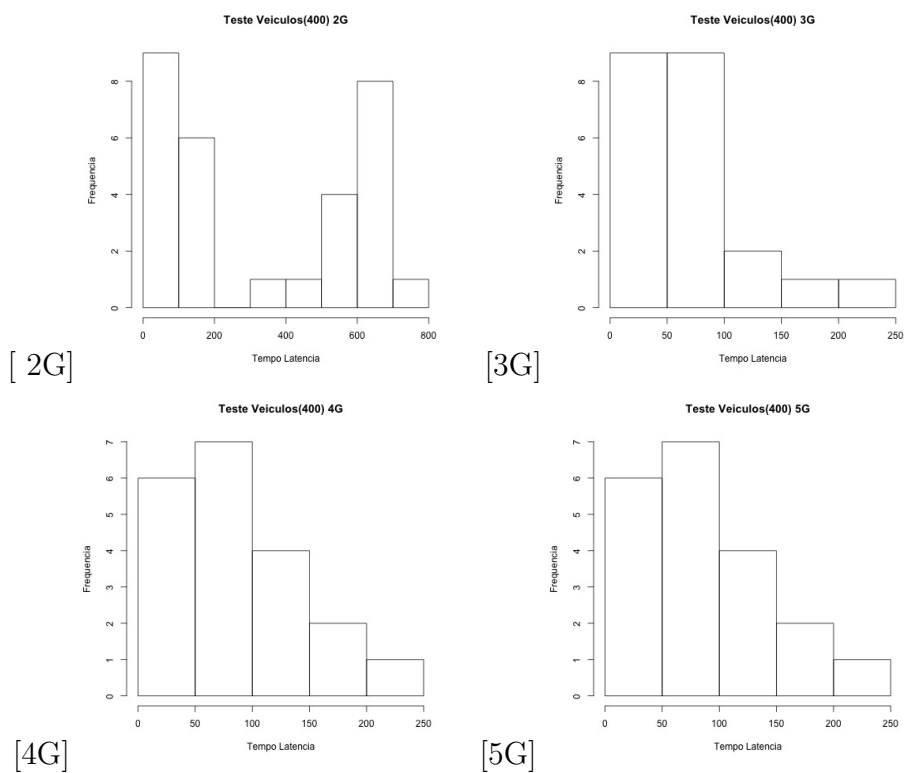


Figura 21 – Análise de Histograma de Frequência do Teste com 400 veículos.



Tempos Mínimos por Velocidade e Quantidade de Veículos

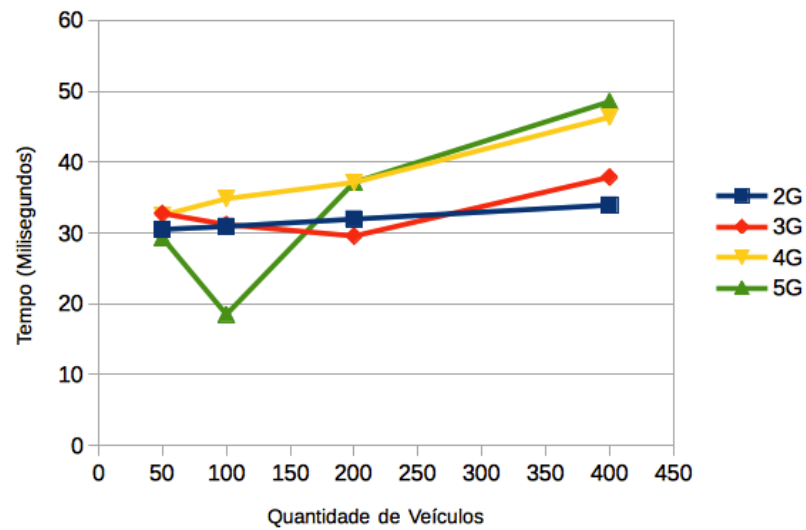


Figura 22 – Gráfico comparativo dos tempos mínimos entres os cenários.

Tempos Médios por Velocidade e Quantidade de Veículos

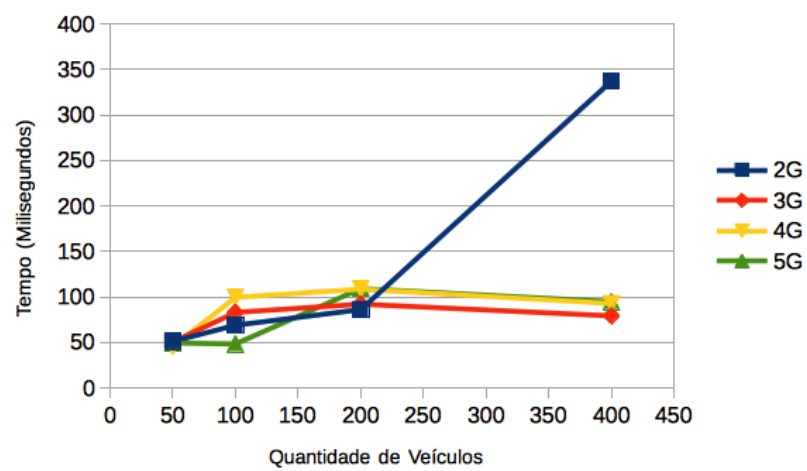


Figura 23 – Gráfico comparativo dos tempos médios entres os cenários.

Tempos Máximos por Velocidade e Quantidade de Veículos

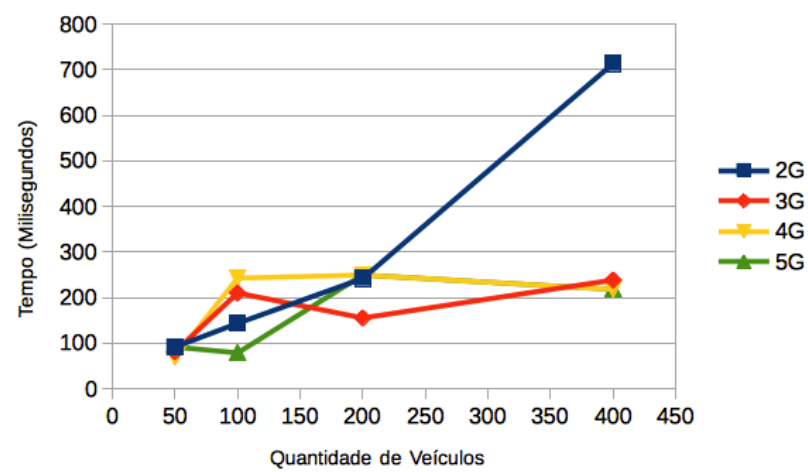


Figura 24 – Gráfico comparativo dos tempos máximos entres os cenários.

7 Conclusão e Trabalhos Futuros

7.1 Conclusões deste Trabalho

O presente trabalho apresentou o modelo de uma arquitetura para rede veiculares em nuvem, denominado i9Vanets, como também uma avaliação com intuito de medir a sua eficácia e eficiência, visando atender às demandas e desafios relacionados à VANETs. Este modelo permite montar uma rede veicular em nuvem e realizar todo gerenciamento e comunicação de maneira virtual, tornando os equipamentos OBUs e RSUs mais simples e baratos.

Foram realizados alguns testes estatísticos, com objetivo de analisar o comportamento da arquitetura. Sobre o teste da normalidade da distribuição, tanto no cliente quanto no servidor, foi constatado que distribuição de probabilidade associada às amostras não podem ser aproximada. Outra análise foi relacionado à dispersão dos dados através do coeficiente de variação, o qual avaliou, sobre as amostras de latência, que a dispersão em cada teste define um comportamento semelhante, porém, o coeficiente de variação medido em cima do tempo de processamento no servidor, mostrou que os testes 250, 500, 1000, 2000 e 2500 tiveram grande dispersão.

Em relação ao nível de processamento dos servidores, o servidor nível 0 é o responsável pelas primeiras conexões feitas pelos veículos e durante a mudança de domínios, pensando nisso, para uma melhor organização e diminuição de carga em um único servidor, é interessante que os domínios vizinhos fiquem, ao máximo, no mesmo nível de hierarquia tendo o mesmo servidor pai, assim, essa sub-árvore responderia de maneira mais eficiente ao comando *changeServer* e diminuindo a pressão sobre o servidor nível raiz.

Uma outra possibilidade é que o servidor nível 0 seja utilizado apenas para coordenar a estrutura retirando de si o papel de gerenciar os veículos, assim ele teria o papel de receber as primeiras conexões dos veículos e encaminhá-las para o servidor correspondente, o mesmo na operação *changeServer*.

* a velocidade 2G e 5G apresentam os mesmos tempos médios

7.2 Trabalhos Futuros

Como trabalhos futuros, é possível criar várias aplicações tais como: sistema de detecção e alerta de congestionamento de trânsito, permitindo um RSU avisar a outros RSU e/ou OBU; Controle de passagem livre para veículos de urgência e emergência; utilizar a arquitetura pra criar um simulador que possa simular toda uma cidade; Criar novos algoritmos de roteamento, segurança e comunicação.

Referências

- AL-KAHTANI, M. S. Survey on security attacks in vehicular ad hoc networks (vanets). In: IEEE. *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*. [S.l.], 2012. p. 1–9. Citado 2 vezes nas páginas 30 e 31.
- AVELAR, E. et al. Interoperability issues on heterogeneous wireless communication for smart cities. *Computer Communications*, Elsevier, v. 58, p. 4–15, 2015. Citado na página 29.
- BALL, R.; DULAY, N. Enhancing traffic intersection control with intelligent objects. *Urban Internet of Things Towards Programmable Realtime Cities*, 2010. Nenhuma citação no texto.
- BARBA, C. T.; AGUIRRE, K. O.; IGARTUA, M. A. Performance evaluation of a hybrid sensor and vehicular network to improve road safety. In: ACM. *Proceedings of the 7th ACM workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. [S.l.], 2010. p. 71–78. Citado na página 22.
- BIRK, W.; OSIPOV, E.; ELIASSON, J. iroad—cooperative road infrastructure systems for driver support. In: *Proceedings of the 16th ITS World Congress*. [S.l.: s.n.], 2009. Citado na página 23.
- BLUM, J.; ESKANDARIAN, A.; HOFFMAN, L. Mobility management in ivc networks. In: IEEE. *Intelligent Vehicles Symposium, 2003. Proceedings. IEEE*. [S.l.], 2003. p. 150–155. Citado na página 36.
- BOUKERCHE, A. Performance evaluation of routing protocols for ad hoc wireless networks. *Mobile Networks and Applications*, Springer-Verlag New York, Inc., v. 9, n. 4, p. 333–342, 2004. Citado na página 34.
- BRIESEMEISTER, L.; SCHAFERS, L.; HOMMEL, G. Disseminating messages among highly mobile hosts based on inter-vehicle communication. In: IEEE. *Intelligent Vehicles Symposium, 2000. IV 2000. Proceedings of the IEEE*. [S.l.], 2000. p. 522–527. Citado na página 37.
- BUBENIKOVA, E.; DURECH, J.; FRANEKOVA, M. Security solutions of intelligent transportation system's applications with using vanet networks. In: IEEE. *Control Conference (ICCC), 2014 15th International Carpathian*. [S.l.], 2014. p. 63–68. Citado na página 26.
- CARVALHO, C. H. R. d. et al. Mobilidade urbana e posse de veículos: análise da pnad 2009. Instituto de Pesquisa Econômica Aplicada (Ipea), 2010. Citado na página 13.
- CAVALCANTI, S. R. *Veer: Um algoritmo de seleção de pares em redes ad hoc veiculares*. Tese (Doutorado) — UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, 2008. Citado na página 13.
- CHEN, W. et al. Dynamic local peer group organizations for vehicle communications. In: IEEE. *Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on*. [S.l.], 2006. p. 1–8. Nenhuma citação no texto.

DANTAS, A. *TRÂNSITO: O JOGO DO CAOS*. 2011. Disponível em: <http://www.autoentusiastascClassic.com.br/2011/05/transito-o-jogo-do-caos.html>. Citado 3 vezes nas páginas 5, 13 e 39.

DAS, B.; BHARGHAVAN, V. Routing in ad-hoc networks using minimum connected dominating sets. In: IEEE. *Communications, 1997. ICC'97 Montreal, Towards the Knowledge Millennium. 1997 IEEE International Conference on*. [S.l.], 1997. v. 1, p. 376–380. Citado na página 36.

DIB, R. P. E. et al. A systematic review of the interventions to promote the wearing of hearing protection. *São Paulo Medical Journal*, SciELO Brasil, v. 125, n. 6, p. 359–361, 2007. Citado na página 12.

DURRESI, M.; DURRESI, A.; BAROLLI, L. Emergency broadcast protocol for inter-vehicle communications. In: IEEE. *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*. [S.l.], 2005. v. 2, p. 402–406. Citado na página 37.

ELTOWEISSY, M.; OLARIU, S.; YOUNIS, M. Towards autonomous vehicular clouds. In: SPRINGER. *International Conference on Ad Hoc Networks*. [S.l.], 2010. p. 1–16. Nenhuma citação no texto.

ENGOULOU, R. G. et al. Vanet security surveys. *Computer Communications*, Elsevier, v. 44, p. 1–13, 2014. Citado na página 28.

FALCHETTI, A.; AZURDIA-MEZA, C.; CESPEDES, S. Vehicular cloud computing in the dawn of 5g. In: IEEE. *2015 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*. [S.l.], 2015. p. 301–305. Citado na página 19.

FÜSSLER, H. et al. Mobicom poster: location-based routing for vehicular ad-hoc networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, ACM, v. 7, n. 1, p. 47–49, 2003. Citado na página 35.

GUPTE, S.; YOUNIS, M. Vehicular networking for intelligent and autonomous traffic management. In: IEEE. *Communications (ICC), 2012 IEEE International Conference on*. [S.l.], 2012. p. 5306–5310. Nenhuma citação no texto.

HADALLER, D. et al. Vehicular opportunistic communication under the microscope. In: ACM. *Proceedings of the 5th international conference on Mobile systems, applications and services*. [S.l.], 2007. p. 206–219. Nenhuma citação no texto.

HAJJI, T.; BARGAOUI, H. Design of a vanet testbed based on cloud computing. Nenhuma citação no texto.

HALL, G. B.; LEAHY, M. G. *Open source approaches in spatial data handling*. [S.l.]: Springer, 2008. v. 2. Citado na página 49.

HUSSAIN, R. et al. Rethinking vehicular communications: Merging vanet with cloud computing. In: IEEE. *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*. [S.l.], 2012. p. 606–609. Citado na página 16.

ICE, R. et al. *REGIONAL ITS ARCHITECTURE GUIDANCE: DEVELOPING, USING, AND MAINTAINING AN ITS ARCHITECTURE FOR YOUR REGION*. [S.l.], 2001. Citado na página 12.

ISAAC, J. T.; ZEADALLY, S.; CAMARA, J. S. Security attacks and solutions for vehicular ad hoc networks. *IET communications*, IET, v. 4, n. 7, p. 894–903, 2010. Citado 2 vezes nas páginas 31 e 32.

JACQUET, P. et al. Optimized link state routing protocol for ad hoc networks. In: IEEE. *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*. [S.l.], 2001. p. 62–68. Citado na página 35.

JAKUBIAK, J.; KOUCHERYAVY, Y. State of the art and research challenges for vanets. In: IEEE. *Consumer communications and networking conference, 2008. CCNC 2008. 5th IEEE*. [S.l.], 2008. p. 912–916. Citado na página 26.

KARP, B.; KUNG, H.-T. Gpsr: Greedy perimeter stateless routing for wireless networks. In: ACM. *Proceedings of the 6th annual international conference on Mobile computing and networking*. [S.l.], 2000. p. 243–254. Citado na página 36.

KIHL, M.; SICHITIU, M.; JOSHI, H. Design and evaluation of two geocast protocols for vehicular ad-hoc networks. *Journal of Internet Engineering*, Klidarithmos Press, 2008. Citado na página 38.

LEE, E. et al. Vehicular cloud networking: architecture and design principles. *IEEE Communications Magazine*, IEEE, v. 52, n. 2, p. 148–155, 2014. Citado 3 vezes nas páginas 5, 16 e 17.

LEONTIADIS, I.; MASCOLO, C. Geopps: Geographical opportunistic routing for vehicular networks. In: IEEE. *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*. [S.l.], 2007. p. 1–6. Citado na página 35.

LI, C. Travel information service system for public travel based on soa. In: IEEE. *Service Operations and Logistics and Informatics (SOLI), 2010 IEEE International Conference on*. [S.l.], 2010. p. 321–324. Citado na página 12.

LI, F.; WANG, Y. Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular technology magazine*, IEEE, v. 2, n. 2, p. 12–22, 2007. Citado na página 35.

LI, L.; LIU, Y.-A.; TANG, B.-H. Snms: an intelligent transportation system network architecture based on wsn and p2p network. *The journal of China universities of posts and telecommunications*, Elsevier, v. 14, n. 1, p. 65–70, 2007. Citado na página 22.

LIANG, W. et al. Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, Taylor & Francis, Inc., v. 2015, p. 17, 2015. Citado na página 14.

LIU, Y.-C.; CHEN, C.; CHAKRABORTY, S. A software defined network architecture for geobroadcast in vanets. In: IEEE. *2015 IEEE International Conference on Communications (ICC)*. [S.l.], 2015. p. 6559–6564. Nenhuma citação no texto.

LOSILLA, F. et al. A comprehensive approach to wsn-based its applications: A survey. *Sensors*, Molecular Diversity Preservation International, v. 11, n. 11, p. 10220–10265, 2011. Citado 7 vezes nas páginas 5, 12, 20, 21, 22, 23 e 24.

LUÍS, N. M. A. *Melhoria de protocolos de encaminhamento em VANETs de alta densidade*. Tese (Doutorado) — FCT-UNL, 2009. Citado 11 vezes nas páginas 5, 7, 12, 26, 27, 33, 34, 36, 37, 38 e 39.

MATOS, L. B. C. d. et al. Análise de desempenho de algoritmos criptográficos assimétricos em uma rede veicular (vanet). *Ciência da Computação*, 2013. Citado 2 vezes nas páginas 15 e 28.

MEJRI, M. N.; BEN-OTHTMAN, J.; HAMDI, M. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, Elsevier, v. 1, n. 2, p. 53–66, 2014. Citado 4 vezes nas páginas 30, 31, 32 e 33.

MERSHAD, K.; ARTAIL, H. Finding a star in a vehicular cloud. *IEEE Intelligent transportation systems magazine*, IEEE, v. 5, n. 2, p. 55–68, 2013. Citado na página 16.

MIURA, S.; ZHAN, Y.; KURODA, T. Evaluation of parking search using sensor network. In: IEEE. *2006 1st International Symposium on Wireless Pervasive Computing*. [S.l.], 2006. p. 6–pp. Citado na página 22.

NANDAN, A. et al. Co-operative downloading in vehicular ad-hoc wireless networks. In: IEEE. *Second Annual Conference on Wireless On-demand Network Systems and Services*. [S.l.], 2005. p. 32–41. Nenhuma citação no texto.

NASIM, R.; KASSLER, A. Distributed architectures for intelligent transport systems: A survey. In: IEEE. *Network Cloud Computing and Applications (NCCA), 2012 Second Symposium on*. [S.l.], 2012. p. 130–136. Citado na página 12.

NIEDERMAIER, B. et al. The new bmw idrive—applied processes and methods to assure high usability. In: SPRINGER. *International Conference on Digital Human Modeling*. [S.l.], 2009. p. 443–452. Citado na página 24.

PAPADIMITRATOS, P. et al. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, IEEE, v. 46, n. 11, p. 100–109, 2008. Nenhuma citação no texto.

PATHRE, A. Identification of malicious vehicle in vanet environment from ddos attack. *Journal of Global Research in Computer Science*, v. 4, n. 6, p. 30–34, 2013. Citado na página 32.

PEDEN, M. et al. *World report on road traffic injury prevention*. [S.l.]: World Health Organization Geneva, 2004. Citado na página 12.

QIAN, Y.; LU, K.; MOAYERI, N. A secure vanet mac protocol for dsrc applications. In: IEEE. *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. [S.l.], 2008. p. 1–5. Citado 2 vezes nas páginas 5 e 40.

QIN, H. et al. An integrated network of roadside sensors and vehicles for driving safety: Concept, design and experiments. In: IEEE. *Pervasive Computing and Communications (PerCom), 2010 IEEE International Conference on*. [S.l.], 2010. p. 79–87. Citado na página 23.

QIN, Y.; HUANG, D.; ZHANG, X. Vehicloud: Cloud computing facilitating routing in vehicular networks. In: IEEE. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. [S.l.], 2012. p. 1438–1445. Citado na página 16.

RAWAT, A.; SHARMA, S.; SUSHIL, R. Vanet: Security attacks and its possible solutions. *Journal of Information and Operations Management*, Bioinfo Publications, v. 3, n. 1, p. 301, 2012. Citado na página 31.

RAYA, M.; PAPADIMITRATOS, P.; HUBAUX, J.-P. Securing vehicular communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, v. 13, n. LCA-ARTICLE-2006-015, p. 8–15, 2006. Citado 2 vezes nas páginas 28 e 33.

SAMARA, G.; AL-SALIH, W. A.; SURES, R. Security issues and challenges of vehicular ad hoc networks (vanet). In: IEEE. *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*. [S.l.], 2010. p. 393–398. Citado 2 vezes nas páginas 15 e 28.

SANTOS, R.; EDWARDS, R.; EDWARDS, A. Cluster-based location routing algorithm for inter-vehicle communication. In: IEEE. *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*. [S.l.], 2004. v. 2, p. 914–918. Citado na página 36.

SOLINGEN, R. V. et al. Goal question metric (gqm) approach. *Encyclopedia of software engineering*, Wiley Online Library, 2002. Citado na página 52.

SOUZA RONIEL DE; SOARES, A. C. B. Estimativa e sinalização de congestionamentos de trafego através de redes veiculares v2v. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 2014. Citado na página 27.

SUMRA, I. A.; HASBULLAH, B.; MANAN, J. Comparative study of security hardware modules (edr, tpd and tpm) in vanet. In: *Third National Information Technology Symposium”, NITS 2011 Symposium*. [S.l.: s.n.], 2011. p. 6–9. Citado na página 12.

SUNG, K.; YOO, J.; KIM, D. Collision warning system on a curved road using wireless sensor networks. In: IEEE. *2007 IEEE 66th Vehicular Technology Conference*. [S.l.], 2007. p. 1942–1946. Citado na página 22.

SYSTEMATICS, C.; MEYER, M. Crashes vs. congestion-what’s the cost to society. *Prepared for the American Automobile Association*, 2011. Citado na página 12.

TANGADE, S. S.; MANVI, S. S. A survey on attacks, security and trust management solutions in vanets. In: IEEE. *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*. [S.l.], 2013. p. 1–6. Citado 3 vezes nas páginas 29, 30 e 32.

TTI, T. T. I. U. M. *Texas Transport Institute Urban Mobility Report 2014*. 2014. Disponível em: <http://d2dtl5nnlpfr0r.cloudfront.net/tti.tamu.edu/documents/ums/congestion-data/national/national-table1.pdf>. Citado na página 12.

WANGHAM, M. S. et al. Segurança em redes veiculares: Inovações e direções futuras. Citado 6 vezes nas páginas 5, 29, 30, 31, 32 e 33.

WASEF, A. et al. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, IEEE, v. 17, n. 5, p. 22–28, 2010. Citado na página 33.

WEINGÄRTNER, E.; KARGL, F. A prototype study on hybrid sensor-vehicular networks. *Proceedings of the 6th GI/ITG KuVS Fachgespräch "Wireless Sensor Networks*, 2007. Citado na página [22](#).

XU, Q. et al. Design and analysis of highway safety communication protocol in 5.9 ghz dedicated short range communication spectrum. In: IEEE. *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*. [S.l.], 2003. v. 4, p. 2451–2455. Citado na página [12](#).

YAN, G. et al. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, IEEE, v. 14, n. 1, p. 284–294, 2013. Nenhuma citação no texto.

ZHANG, J. A survey on trust management for vanets. In: IEEE. *2011 IEEE International Conference on Advanced Information Networking and Applications*. [S.l.], 2011. p. 105–112. Citado na página [33](#).

ZHU, T.; LIU, Z. Intelligent transport systems in china: Past, present and future. In: IEEE. *Measuring Technology and Mechatronics Automation (ICMTMA), 2015 Seventh International Conference on*. [S.l.], 2015. p. 581–584. Citado na página [12](#).