TSMA: Uma Arquitetura para Gerenciar a Sinalização de Trânsito

Everton Rocha Lira

Universidade Federal de Uberlândia
Faculdade de Computação
Programa de Pós-Graduação em Ciência da Computação

Uberlândia
2016

Everton Rocha Lira

TSMA: Uma Arquitetura para Gerenciar a Sinalização de Trânsito

Dissertação de mestrado apresentada ao Programa de Pós-graduação da Faculdade de Computação da Universidade Federal de Uberlândia como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Ciência da Computação

Orientador: Rafael Pasquini
Coorientador: Rodolfo da Silva Villaça

Uberlândia
2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

L768t
2016

Lira, Everton Rocha, 1989-
TSMA: uma arquitetura para gerenciar a sinalização de trânsito / Everton Rocha Lira. - 2016.
88 f. : il.

Orientador: Rafael Pasquini.
Coorientador: Rodolfo da Silva Villaça.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Ciência da Computação.
Inclui bibliografia.

1. Computação - Teses. 2. Trânsito - Sinais e sinalização - Teses. 3. Redes locais sem fio - Teses. 4. Trânsito - Medidas de segurança - Teses. I. Pasquini, Rafael. II. Villaça, Rodolfo da Silva. III. Universidade Federal de Uberlândia, Programa de Pós-Graduação em Ciência da Computação. IV. Título.

CDU: 681.3

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Os abaixo assinados, por meio deste, certificam que leram e recomendam para a Faculdade de Computação a aceitação da dissertação intitulada "**TSMA: Uma Arquitetura para Gerenciar a Sinalização de Trânsito**" por Everton Rocha Lira como parte dos requisitos exigidos para a obtenção do título de **Mestre em Ciência da Computação**.

Uberlândia, 16 de Fevereiro de 2016

Orientador:

Prof. Dr. Rafael Pasquini
Universidade Federal de Uberlândia

Coorientador:

Prof. Dr. Rodolfo da Silva Villaça
Universidade Federal do Espírito Santo

Banca Examinadora:

Prof. Dr. Anilton Salles Garcia
Universidade Federal do Espírito Santo

Prof. Dr. Marcelo Zanchetta do Nascimento
Universidade Federal de Uberlândia

Este trabalho é dedicado a todos os grandes questionadores,
àqueles que mudaram o mundo após rejeitar "porque sim" como resposta.

Agradecimentos

Agradeço a meus pais pelo incentivo e apoio.
Agradeço aos professores pela orientação e tratamento.
Agradeço aos colegas pelo companheirismo e amizade.
Agradeço também à FAPEMIG pelo fomento à pesquisa.

"Tenho por filosofia de vida que as dificuldades somem ao serem confrontadas de frente."
(Isaac Asimov)

Resumo

Este trabalho consiste da proposição e avaliação do TSMA (*Traffic Sign Management Architecture*), uma arquitetura voltada a solucionar limitações na infraestrutura atual de sinalizações de trânsito. Uma implementação em larga escala do TSMA permitiria, por exemplo, efetuar remotamente mudanças na sinalização de trânsito para desviar o fluxo de veículos em caso de acidentes ou mesmo aumentar a velocidade de uma via em horários de tráfego intenso. Veículos adaptados para o TSMA são equipados com um receptor que exibe as placas de trânsito ao motorista em uma tela no painel, fator este que dá o destaque devido à sinalização e que tem o potencial para reduzir o risco de acidentes causados pela desatenção dos condutores. A proposta segue uma tendência mundial de "cidades inteligentes" pela qual os sistemas envolvidos na rotina das pessoas estão interconectados e se adaptam às necessidades delas para prover mais conforto e segurança. Foram realizadas simulações dos cenários de uso da arquitetura e um protótipo de comunicação foi desenvolvido como parte deste trabalho. Resultados obtidos de experimentos utilizando o protótipo e os cenários simulados confirmaram as expectativas de viabilidade e eficiência do TSMA.

Palavras-chave: Cidades Inteligentes. *Beacon-Stuffing*. Sinalização de Trânsito. IEEE 802.11.

Abstract

This academic work consists of specifying and evaluating TSMA (*Traffic Sign Management Architecture*), an architecture that is being proposed to address limitations of the current traffic sign infrastructure. A large-scale implementation of TSMA would allow, for instance, that remote updates sent to traffic signs be used to divert the traffic flow in case of accidents or even change the limit speed of certain roads during the rush hours. TSMA-compliant vehicles have a receiver unit that displays traffic signs to the driver in the navigation system display; this feature brings into evidence the traffic signs and could potentially reduce the risk of accidents being caused by driver inattention. This work follows a global "intelligent cities" trend by which systems involved in peoples' routines are interconnected and adapt to their needs to better provide comfort and safety. Simulations were run to test the architecture's usage scenarios and a communication prototype was developed as part of this effort. Results obtained from experiments using this prototype and the simulated scenarios confirmed the positive expectations regarding TSMA's viability and efficiency.

Keywords: Intelligent Cities. *Beacon-Stuffing*. Traffic Signs. IEEE 802.11.

Lista de ilustrações

Lista de tabelas

Lista de siglas

AU *Application Unit*

AP *Access Point*

ARP *Address Resolution Protocol*

CA *Certification Authority*

CTB Código de Trânsito Brasileiro

CSMA *Carrier Sense Multiple Access*

CSMA/CD *Carrier Sense Multiple Access with Collision Detection*

DSRC *Dedicated Short-Range Communications*

GPS *Global Positioning System*

GPRS *General Packet Radio Services*

IP *Internet Protocol*

ITS *Intelligent Transportation Systems*

MANET *Mobile Ad hoc NETwork*

MAN *Metropolitan Area Network*

NTP *Network Time Protocol*

`Ns-3 Network Simulator` 3

OBU *vehicular On-Board Unit*

PKI *Public Key Infrastructure*

PKR *Public Key Repository*

QoE *Quality of Experience*

RFID *Radio-Frequency IDentification*

RSU *RoadSide Unit*

TCMC *Traffic Control Management Center*

TCP *Transmission Control Protocol*

TSMA *Traffic Sign Management Architecture*

TST *Traffic Sign Transmitter*

WAVE *Wireless Access in Vehicular Environments*

V2I *Vehicle-to-Infrastructure*

VANET *Vehicular Ad hoc NETwork*

VMS *Variable Message Sign*

VUR *Vehicular Unit Receiver*

Sumário

Capítulo 1

Introdução

O sistema atual de transportes terrestres é regido por normas estabelecidas para manter a ordem e garantir a segurança dos condutores. Cada país no mundo tem suas regras próprias e, na verdade, até pequenos territórios a nível de cidade têm uma certa liberdade para criar normas, desde que não conflitem com o que foi estabelecido por instâncias superiores. Neste cenário, onde cada região pode impor regras ao trânsito de veículos, é relevante apontar um fator que geralmente é similar até entre regiões de países diferentes: A forma convencional de apresentação da sinalização de trânsito.

A forma convencional de apresentação da sinalização de trânsito aos condutores é por meio de placas fixas de metal adesivadas com uma sinalização de trânsito, conforme pode ser visualizado na Figura 1, que apresenta uma montagem de fotos, em diversos países, de placas metálicas exibindo a sinalização de trânsito “Pare”, em suas formas equivalentes para cada uma das localidades da montagem. Esse paradigma de apresentação da sinalização, embora relativamente funcional e prático, é problemático por vários motivos que são detalhados na Seção 1.1, um deles é referente à imutabilidade da sinalização exibida na placa; não é possível alterar a sinalização exibida em uma placa metálica de trânsito sem ter o esforço manual de substituir a placa presencialmente.

O século XXI está sendo marcado pela evolução constante das formas de comunicação e pela alta responsividade dos objetos com os quais interagimos, o que evidencia ainda mais o quão obsoleto é esse sistema de sinalização de trânsito, que não permite uma adaptação rápida às condições altamente flutuantes do tráfego de veículos. O TSMA (*Traffic Sign Management Architecture*) é uma proposta de arquitetura para gestão da sinalização de trânsito que quebra esse paradigma atual das placas de trânsito, que não dão suporte a uma adaptação dinâmica da sinalização exibida nelas ao contexto do tráfego ou às necessidades dos próprios motoristas. Isso é feito por meio de um *design* que fornece aos profissionais responsáveis pela gestão do tráfego a possibilidade de atualizar remotamente os dispositivos que cumprem a função de uma “placa de trânsito” no TSMA.

Figura 1 – Placas equivalentes à sinalização de "Pare" em diversos países.

Adaptado de: "*Various stop signs found around the world.*". Disponibilizado em: <http://images.roadtrafficsigns.com/img/art/stopsigns-L.jpg>, Acesso em jan. 2016.

O funcionamento do TSMA se baseia na interação de entidades com tipos distintos:

- `TCMC`: O TCMC (*Traffic Control Management Center*) é uma central de controle do tráfego cujos funcionários têm autonomia para gerenciar a sinalização de trânsito presente em um escopo regional predefinido. Os profissionais que atuam no TCMC são responsáveis pela atribuição, via software, da sinalização de trânsito para cada uma das placas de trânsito que, no modelo do TSMA, são representadas pelos dispositivos TST;

- `TST`: Os dispositivos TST (*Traffic Sign Transmitter*) equivalem, dentro do TSMA, às placas de trânsito do modelo convencional de sinalização de trânsito. Cada dispositivo TST tem o potencial para disseminar via *Wi-Fi* a sinalização de trânsito vigente no momento e exibi-la, em uma tela acoplada, a motoristas nas imediações;

- `VUR`: Cada veículo em conformidade com o TSMA estará equipado com um dispositivo VUR (*Vehicular Unit Receiver*) que é responsável por recuperar do meio *Wi-Fi*, e exibir ao motorista, a sinalização de trânsito especificada em cada uma das mensagens emitidas por dispositivos TST nas proximidades.

Uma das metas na especificação do TSMA é fazer uso, sempre que possível, de dispositivos e tecnologias de domínio público ou de baixo custo. O Capítulo 3 contém um detalhamento de cada uma das três entidades descritas, bem como dos mecanismos aplicados na arquitetura.

A garantia da confiabilidade da solução, especialmente sob o aspecto de segurança e integridade da sinalização de trânsito, é considerada uma das maiores prioridades na atividade de especificar o TSMA. Uma arquitetura vulnerável poderia causar o fornecimento de um serviço instável e, potencialmente, levar à perda de vidas. Por isso é importante garantir a confiabilidade do TSMA, e as avaliações realizadas apontam nessa direção de forma positiva. As avaliações contaram com o uso de ferramentas de simulação tais como `Ns-3`[1], `SUMO`[2], `OMNet++`[3] e, principalmente, contaram com experimentos utilizando um protótipo, desenvolvido no escopo desta dissertação, implementado com minicomputadores de baixo custo (Raspberry Pi[4]).

Nas seções seguintes são detalhadas as motivações para a concepção do TSMA (Seção 1.1), os objetivos da pesquisa e os desafios envolvidos (Seção 1.2), as hipóteses sobre as quais a pesquisa foi desenvolvida (Seção 1.3), as contribuições obtidas com o desenvolvimento do trabalho (Seção 1.4) e, por fim, a organização dos próximos capítulos da dissertação (Seção 1.5).

1.1 Motivação

Uma das causas de mortalidade em alta evidência no Brasil é referente a acidentes envolvendo veículos automotivos, causa esta que, segundo (SIVAK, 2014), é responsável em escala global por 2,1% do total de mortes contabilizadas anualmente. De fato, os dados da Figura 2 apontam que em 2010 o Brasil obteve a quarta posição na listagem de países com maior quantidade de mortes no trânsito. Há estudos recentes que apontam uma alta correlação entre investir na atualização e melhoria da infraestrutura do tráfego veicular e reduzir a taxa de mortalidade, um país que exemplifica esta relação é o Japão, que entre os anos 2000 e 2008 diminuiu essa taxa em 42% (ZHANG; DELGROSSI, 2012).

Existem diversas causas para a não-conformidade do motorista em relação a um dado sinal de trânsito, um dos motivos apontados está relacionado ao aumento da longevidade da população. (GRACA, 1986) aponta que um dos três principais motivos de acidentes iniciados por pessoas de idade avançada é a dificuldade na interação com a sinalização de trânsito, fato evidenciado pela pesquisa de (MALFETTI, 1985) com essa faixa da população, na qual 25% dos entrevistados não responderam bem à sinalização convencional de trânsito apontando problemas como o posicionamento, tamanho, estado de manutenção e difícil interpretação das placas.

[1] www.nsnam.org
[2] www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883
[3] www.omnetpp.org
[4] www.raspberrypi.org

Países com maiores números absolutos de morte no trânsito - 2010

Ranking	País	Posição no IDH	População estimada[1]	Nº de mortes[2]	Taxa de Mortes por 100 mil hab.	Número de veículos registrados	Taxa de mortes por 1 mil veículos
1º	China	101º	1.348.932.032	275.983	20,5	207.061.286	1,33
2º	Índia	136º	1.224.614.272	231.027	18,9	114.952.000	2,01
3º	Nigéria	153º	158.423.184	53.339	33,7	12.545.177	4,25
4º	Brasil[3]	85º	194.946.488	42.844	22	64.817.974	0,66
5º	Indonésia	121º	239.870.944	42.734	17,8	72.692.951	0,59
6º	Estados Unidos	3º	310.383.968	35.490	11,4	258.957.503	0,14
7º	Paquistão	146º	173.593.384	30.131	17,4	7.853.022	3,84
8º	Rússia	55º	142.958.156	26.567	18,6	43.325.312	0,61
9º	Tailândia	103º	69.122.232	26.312	38,1	28.484.829	0,92
10º	Irã	76º	73.973.628	25.224	34,1	20.657.627	1,22

Instituto Avante Brasil, PNUD, OMS, Datasus

[1] Os dados populacionais foram extraídos do banco de dados da Divisão de População das Nações Unidas

[2] As taxas de mortalidade no trânsito foram extraídas dos registros de morte reportados pelos Estados à Organização Mundial da Saúde, dos registros oficiais divulgados por cada país e através de um modelo regressivo para estimar se o número de mortes no trânsito do modificado na publicação Global Status Report on Road Safety 2013.

[3] Número de mortes no trânsito no Brasil de acordo com os dados oficiais do Datasus, em 2010.

Figura 2 – Países com maiores números absolutos de morte no trânsito.

Adaptado de: "*Mortes no trânsito: Brasil é o 4o do mundo*.". Disponibilizado em: <http://uploads.jusbr.com/publications/artigos/113704460/images/1393352195.jpg>, Acesso em fev. 2016.

Outro problema evidente envolvendo o modelo atual de sinalização de trânsito é o aumento na dificuldade de enxergar as placas durante o período noturno, fator que, apesar de ser mais presente em pessoas com problemas de visão e, dentre essas, as de idade avançada, afeta toda a população em menor ou maior grau (PETERMAN, 2013). De fato, é estimado que a taxa de acidentes automotivos no período noturno aproxima-se do triplo da taxa no período diurno (OPIELA; ANDERSEN, 2007).

Mas a causa principal ou, no mínimo, um dos maiores motivadores de acidentes automobilísticos é a desatenção do condutor (HENDRICKS; FELL; FREEDMAN, 2001). Em 2006 foi divulgado um estudo sobre o papel da desatenção como causa de acidentes, nele constavam os resultados de um experimento envolvendo motoristas de ambos os gêneros e diversas faixas de idade. Constatou-se que o fator desatenção, em suas diversas formas, fez parte das causas em 78% dos acidentes automobilísticos (KLAUER et al., 2006).

A infraestrutura atual de trânsito, em sua maioria, baseia-se em placas de sinalização que não podem ser alteradas remotamente, não se adaptam às necessidades visuais dos condutores, não têm mecanismos de detecção de vandalismo, e não são sensíveis ao contexto do veículo que trafega na via. É importante frisar que, apesar das diversas limitações do modelo atual de sinalização de trânsito, ele sofreu poucas alterações desde a sua padronização em 1908 (BEKIARIS; WIETHOFF; GAITANIDOU, 2011).

1.2 Objetivos e Desafios da Pesquisa

O objetivo principal deste trabalho é a proposição do TSMA, uma arquitetura que tem o potencial de contribuir para a melhoria do sistema atual de sinalização de trânsito ao apresentar mecanismos que superam várias das limitações do modelo atual, conforme detalhado na Seção 1.1.

Uma consideração feita nesta dissertação é a de que este objetivo principal do trabalho pode ser decomposto em objetivos menores e que o cumprimento de todos esses objetivos menores implica na realização satisfatória do objetivo principal. Sendo assim, o objetivo principal foi decomposto nas seguintes tarefas:

- ❏ Realizar a especificação da arquitetura, com o detalhamento de seus componentes (TCMC, TST e VUR) e de como ocorre a interação entre tais componentes;
- ❏ Descrever os mecanismos de segurança que são utilizados no TSMA para garantir a integridade (dados inalterados de ponta a ponta) e autenticidade (dados provém da origem especificada) da sinalização de trânsito;
- ❏ Utilizar experimentos simulados e testes em protótipos para comprovar a viabilidade e desempenho satisfatório do TSMA, especialmente em suas etapas mais críticas.

Dessa forma, o cumprimento dos objetivos listados é demonstrado nos próximos capítulos da dissertação, conforme a organização descrita na Seção 1.5.

1.3 Hipótese

A especificação do TSMA foi desenvolvida considerando os problemas descritos na Seção 1.1 como limitações que, na medida do possível, deveriam ser inexistentes neste novo modelo proposto. Parte dessas limitações do sistema atual se refere à impossibilidade de atualizar remotamente, e de maneira eficaz, a sinalização de placas de trânsito em resposta às condições da pista; outra parte das limitações é devido ao fato de as placas de trânsito serem apresentadas de forma igual a todos os motoristas, desconsiderando quaisquer necessidades especiais que esses possam ter.

No TSMA é previsto que operadores humanos, que estejam em um dado TCMC, gerenciem remotamente a sinalização que é disseminada em cada unidade TST (equivalente à placa de trânsito convencional) da área de atuação do referido TCMC. Essa funcionalidade permite uma adaptação rápida da sinalização ao fluxo de veículos e às condições da pista, algo inviável no sistema atual de sinalização de trânsito. Outra característica do TSMA que soluciona limitações do sistema atual é criar a possibilidade de que a sinalização de trânsito disseminada por unidades TST seja recebida por dispositivos VUR

presentes em cada veículo, e que esse dispositivo dispare um alerta audiovisual ao motorista. É previsto que o tamanho da tela para exibição de alertas e o volume de reprodução dos mesmos sejam adaptáveis às necessidades especiais do motorista, reduzindo assim o risco de a sinalização ser ignorada.

A principal hipótese implícita na proposição dessas funcionalidades do TSMA é de que ambas, a comunicação entre o TCMC e os dispositivos TST, e a transmissão de dados entre dispositivos TST e dispositivos VUR, são viáveis e eficazes em larga escala. O êxito em ambas essas etapas de transmissão da sinalização de trânsito é o que garante o sucesso do TSMA como solução válida. É relevante citar que uma das prioridades na especificação da arquitetura foi a minimização de custos na escolha dos dispositivos e tecnologias envolvidos. No Capítulo 4 são apresentados os resultados dos testes de desempenho e viabilidade das técnicas que são aplicadas nestas etapas do TSMA;

1.4 Contribuições

Ao final do desenvolvimento deste trabalho as contribuições resultantes são:

- A especificação formal do TSMA, com o detalhamento de seus componentes e da interação entre os mesmos, contemplando aspectos de segurança da solução;
- As análises de viabilidade e desempenho do TSMA, embasadas nos resultados de experimentos utilizando protótipos e simulações;
- O código-fonte desenvolvido para executar nos dispositivos Raspberry Pi as funcionalidades básicas de dispositivos emissor e receptor, bem como realizar os testes de protótipo.

1.5 Organização da Dissertação

Segue a organização dos capítulos seguintes da dissertação: O Capítulo 2 descreve a terminologia envolvida na pesquisa, bem como é apresentado o estado da arte para esses termos e, quando aplicável, são feitas comparações com o TSMA. O Capítulo 3 apresenta a especificação formal da arquitetura, detalhando cada um dos seus componentes, bem como descrevendo aspectos de segurança da solução. No Capítulo 4 são descritos os experimentos que foram realizados para analisar a viabilidade e desempenho da arquitetura, bem como são apresentados os resultados dos mesmos. Por último, no Capítulo 5, as contribuições do trabalho são detalhadas, bem como são apresentadas algumas sugestões de trabalhos futuros.

Capítulo 2

Fundamentação e Trabalhos Relacionados

Neste capítulo são apresentados os termos mais relevantes à temática desta dissertação (Seção 2.1), são discutidos trabalhos com temática similar à do TSMA para analisar a contribuição do mesmo frente ao estado da arte da literatura (Seção 2.2) e, por fim, é feita uma análise comparativa do TSMA e os trabalhos correlatos mais próximos (2.3).

2.1 Conceitos Básicos

As seções seguintes contém as definições de conceitos, modelos e técnicas citados diretamente na especificação do TSMA ou em trabalhos correlatos a este. A Seção 2.1.1 descreve aplicações ITS, detalha o modelo de comunicação entre veículos e infraestrutura (V2I), e explica a relação de ambos com o TSMA. A tecnologia RFID é apresentada na Subseção 2.1.2 para auxiliar a compreensão dos trabalhos relacionados. Na Seção 2.1.3 são discutidos três tópicos relacionados à temática, no caso os padrões: IEEE 802.11, WAVE e DSRC. A Seção 2.1.4 é dedicada à técnica *beacon-stuffing* que é usada para implementar a comunicação V2I do TSMA.

2.1.1 ITS | V2I

O termo ITS (*Intelligent Transportation Systems* - Sistemas Inteligentes de Transporte) foi definido, em julho de 2010, pelo conselho diretivo da União Europeia como sendo o conjunto de meios adotados para prover serviços inovadores ao setor de transporte rodoviário, incluindo melhorias com foco na infraestrutura, nos veículos, na interface com os usuários, na gestão do tráfego, de mobilidade, ou na interface com outros meios de transporte (DIRECTIVE, 2010).

O TSMA é uma proposta de arquitetura com foco na melhoria da infraestrutura atual de sinalização de trânsito (ao especificar uma nova forma de apresentação da sinalização

aos condutores) e na melhoria dos meios de gestão do tráfego (ao descrever mecanismos de atualização remota das placas); dessa forma, o TSMA está claramente aplicando os conceitos de ITS.

Ainda com relação ao termo ITS, é importante ressaltar que a grande maioria dos trabalhos propondo mudanças na sinalização de trânsito é direcionada a melhorar o controle e apresentação de um tipo específico de sinalização, no caso os semáforos, sendo bem menor o número de pesquisas encontradas que se dedicam à melhoria das placas convencionais de sinalização, que é o caso do TSMA.

Grande parte das propostas no contexto de ITS, que tem por foco a melhoria do tráfego urbano, envolve alguma forma de interação V2I (*Vehicle-to-Infrastructure*) para troca de informações relevantes à atuação do motorista ou do sistema proposto em si. Há dois elementos nesse modelo de interação, o OBU (*vehicular On-Board Unit*) que é um módulo comunicador instalado nos veículos envolvidos, e o RSU (*RoadSide Unit*) que é um dispositivo comunicador implantado ao lado das vias de tráfego. Um exemplo clássico de interação do veículo com uma infraestrutura auxiliar (V2I) está nos sistemas automatizados de cobrança de pedágio, no Brasil a marca "Sem Parar"[1] oferece o serviço mais conhecido dessa modalidade.

Na maioria das vezes é prevista a existência de um canal seguro de comunicação entre o OBU e o RSU, para evitar que haja acesso indevido a informações privadas. A tecnologia de comunicação usada entre os dispositivos depende das necessidades do projeto em questão, mas algumas das mais convencionais são:

- *Radio-Frequency IDentification* (RFID);
- IEEE 802.11 b/g/n;
- *Wireless Access in Vehicular Environments* (WAVE);
- *Dedicated Short-Range Communications* (DSRC).

Essas tecnologias, bem como exemplos da aplicação delas neste contexto, são descritos nas seções que seguem.

2.1.2 RFID

O RFID (*Radio-Frequency IDentification*) é uma tecnologia que descreve o uso de sinais de radiofrequência para recuperar informações por meio da operação de leitura de etiquetas (*tags*) RFID. Em um sistema RFID há quatro elementos bem definidos que podem ser visualizados na Figura 3.

[1] <www.semparar.com.br>

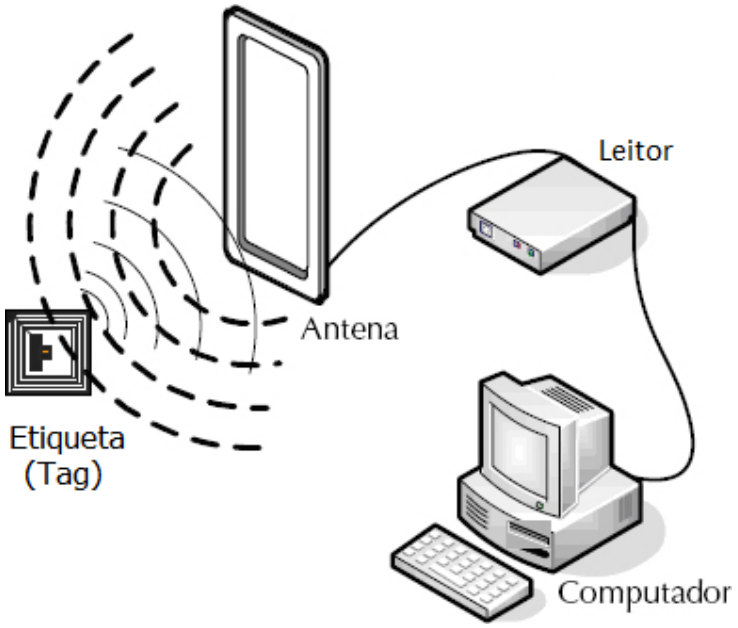

Figura 3 – Interação entre elementos de um sistema RFID genérico.

Adaptado de: "*What is RFID?*". Disponibilizado em: <http://www.epc-rfid.info/wp-content/themes/gintinfo/images/how%20rfid%20works.png>, Acesso em jan. 2016.

Os elementos apresentados na Figura 3 seguem:

- **Etiqueta (*Tag*)**: A etiqueta RFID é um invólucro para dois componentes, um microchip cuja memória contém os dados identificadores que podem ser recuperados por terceiros e uma antena capaz de aceitar requisições de dados e também de transmitir esses dados;

- **Antena (Leitora)**: Emite o sinal de radiofrequência que aciona etiquetas RFID que estiverem em seu alcance. A antena também é responsável pela recepção da resposta emitida pelas etiquetas acionadas, os dados provindos da referida resposta são encaminhados ao leitor;

- **Leitor**: Efetua o processamento dos dados identificadores recuperados pela antena; dados estes que, após o procedimento, são transmitidos ao computador;

- **Computador (Base de Dados)**: Efetua o reconhecimento e tratamento dos dados identificadores que tiverem sido recuperados das etiquetas.

As etiquetas RFID podem ser ativas (usa bateria interna como fonte de energia) ou passivas (usa a energia do sinal recebido como fonte de energia para a ativação e emissão da resposta). Etiquetas passivas têm um alcance baixo (inferior a 10 metros), mas seu preço é baixo e sua durabilidade é muito alta; já etiquetas ativas têm um alcance maior

(pode ser superior a 100 metros), porém seu preço é alto e sua vida útil é de no máximo 10 anos (WEIS, 2007).

São vários os usos dessa tecnologia. Dentre eles há aplicações dos seguintes tipos:

- ❏ Rastreamento e identificação de pacotes ou animais;
- ❏ Pagamento de tarifas ou pedágios e acesso seguro a finanças pessoais;
- ❏ Concessão de acesso a lugares e eventos;
- ❏ Medidas contra furto ou fraude.

Além das aplicações descritas, é relevante citar o uso da tecnologia RFID, no contexto de ITS, para transmitir informações relevantes e sinalizações de trânsito; aplicação esta que é descrita na Seção 2.2.3.

2.1.3 IEEE 802.11 | WAVE | DSRC

O padrão IEEE 802.11 tem alto reconhecimento por ser o mais adotado na comunicação sem fio para redes locais de dispositivos, especialmente em ambientes domésticos. Esse padrão tem muitas variantes que servem a propósitos específicos e nem sempre letras sequenciais representam melhorias da variante anterior; um exemplo de melhoria (na segurança da comunicação e alcance do sinal) entre variantes de mesmo tipo é a relação entre os protocolos IEEE 802.11b, IEEE 802.11g e IEEE 802.11n. É importante citar a existência da variante IEEE 802.11p, também conhecida como tecnologia WAVE (*Wireless Access in Vehicular Environments* - Acesso Sem Fio em Ambientes Veiculares), que foi especificada tendo em mente as condições peculiares da comunicação entre veículos e dispositivos RSU, entre elas a alta velocidade dos veículos em condições normais.

Outro diferencial do protocolo WAVE quando comparado às variantes b/g/n é com relação à faixa de frequência usada na transmissão, as variantes b/g/n usam a frequência 2,4 GHz, enquanto o WAVE transmite a uma frequência de 5,9 GHz. Entre outros benefícios, o uso da frequência 5,9 GHz resulta em uma menor possibilidade de sofrer interferência de outros dispositivos, visto que a frequência 2,4 GHz é usada por muitas modalidades de dispositivos eletrônicos e tem menos canais de transmissão disponíveis se comparado à variante de 5,9 GHz.

O termo DSRC (*Dedicated Short-Range Communications*) se refere a um conjunto de canais de transmissão sem fio que foi designado para comunicação unidirecional ou bidirecional com alcance mediano (até 1 km). O DSRC começou a ser pesquisado em 1993 por um grupo corporativo da JSK no Japão e, nos anos seguintes, passou também a ser objeto de estudos na Europa e Estados Unidos (BEYLOT; LABIOD, 2013). Nos Estados Unidos o DSRC foi liberado para uso em faixas de frequência próximas a 5,9 GHz, já na Europa e Japão o DSRC opera em faixas de frequência próximas a 5,8 GHz.

O uso do DSRC para coletar eletronicamente taxas de estacionamento e pedágio constitui o uso mais comum dessa tecnologia.

A semelhança nas propostas do DSRC e WAVE é bem evidente, especialmente quando se compara as faixas de frequência adotadas; isto, na verdade, não é uma coincidência. O WAVE é um modelo de comunicação voltado a redes veiculares que, definiu-se, atua exatamente na faixa de frequências que recebeu o nome de DSRC (5,8–5,9 GHz). Não é incomum que outras tecnologias, como o já citado RFID, também operem na faixa de frequências DSRC. A Figura 4 indica o foco principal de atuação dos padrões DSRC e WAVE; basicamente, a definição do padrão WAVE foi fundamentada na do DSRC, de forma que o WAVE engloba o DSRC. O padrão WAVE oferece nativamente recursos que eliminam alguns dos problemas contornados na especificação do TSMA, como, por exemplo: segurança com autenticação na troca de mensagens, rapidez na identificação e troca de mensagens, confiabilidade na transmissão de dados a veículos com velocidade de até 200 km/h.

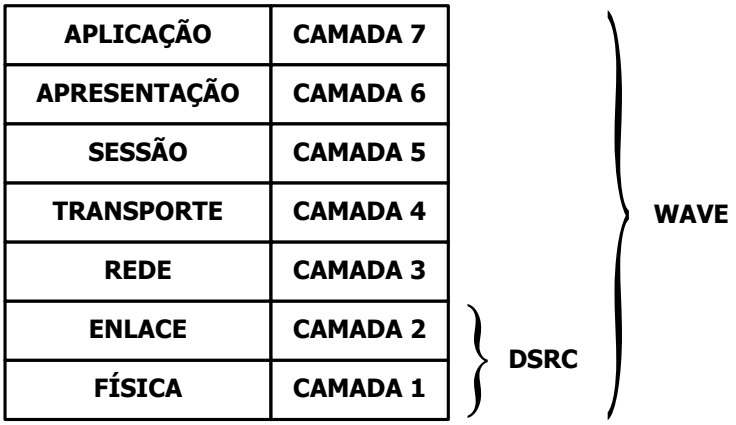

Figura 4 – Focos de atuação do DSRC e WAVE no modelo OSI.

Adaptada de: "*Protocol Stack*." (WEIGLE, 2008).

O TSMA, conforme mencionado no Capítulo 1, provê a funcionalidade de exibição da sinalização de trânsito no painel do veículo conforme as necessidades do condutor e para segurança do mesmo. Entretanto, essa funcionalidade depende da transmissão de dados, por meio sem fio, entre o módulo TST e o dispositivo VUR. Apesar das aparentes vantagens do padrão WAVE, e de ele estar se tornando o padrão oficial para redes veiculares, no TSMA essa transmissão V2I é atualmente implementada usando o protocolo IEEE 802.11n. Alguns dos motivos que justificam tal escolha são:

- Baixo custo e alta disponibilidade de equipamentos no padrão IEEE 802.11n, algo condizente com a proposta de especificar o TSMA de forma a possibilitar uma implementação de custo reduzido. Isso contrasta totalmente com a dificuldade para encontrar equipamentos no padrão WAVE à venda para pessoas físicas;

- Embora o uso do protocolo IEEE 802.11n represente uma possibilidade maior de sofrer interferência no envio de dados, é necessário considerar que o tamanho das mensagem de sinalização emitida pelos dispositivos TST é muito baixo (conforme é detalhado na Seção 3.4).

2.1.4 *Beacon-stuffing*

O processo tradicional de comunicação *Wi-Fi*, sob os protocolos IEEE 802.11 b/g/n, ocorre pela associação de entidades-cliente a *Access Points* disponíveis. A partir do momento em que a associação *Wi-Fi* é realizada, estará estabelecido um canal para transmissão bilateral de dados entre o cliente associado e o *Access Point* ao qual este cliente se associou.

Uma etapa do ciclo de funcionamento do TSMA é a transmissão unilateral de dados, via *Wi-Fi*, entre o módulo TST e os dispositivos VUR que estejam nas imediações. É relevante apontar que os dispositivos VUR estão instalados em veículos que podem estar, potencialmente, em alta velocidade. Dessa forma, a transmissão de dados precisa ser feita rapidamente e, visto que o demorado processo de associação *Wi-Fi* é praticamente inviável neste contexto, uma possibilidade que ganhou destaque foi a de usar a técnica *beacon-stuffing*.

A proposta do *beacon-stuffing* é ser uma forma de transmissão unilateral de dados a partir de dispositivos *Wi-Fi* que estejam atuando como *Access Points*. O diferencial da técnica está em realizar o envio de dados sem que tenha havido uma associação do dispositivo receptor ao emissor. A especificação que descreve o padrão IEEE 802.11 prevê que um equipamento *Access Point* deve anunciar a disponibilidade de sua rede *Wi-Fi* por meio da emissão contínua de *beacon frames*, estruturas que contém informações da rede que está sendo disponibilizada. A Figura 5 detalha os campos de um *beacon frame* genérico.

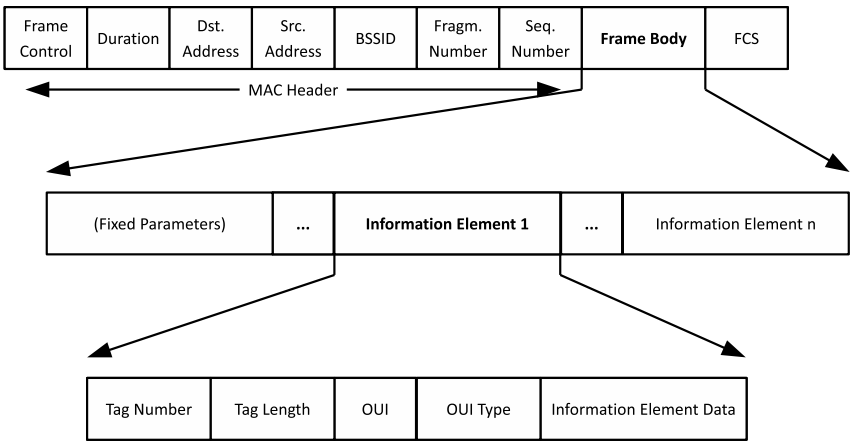

Figura 5 – Estrutura de um *beacon frame* padrão.

O foco do detalhamento na Figura 5 é a presença de um campo de tamanho variável chamado *Information Element*, transportado no *Frame Body*. Quando esse campo é marcado com o identificador 221 ele é conhecido como "*Vendor Specific*" e costuma ser usado para armazenar informações do fabricante do dispositivo de rede em questão. Esse tipo de campo pode armazenar até 255 bytes arbitrários por instância e, conforme previsto no padrão IEEE 802.11, pode haver várias instâncias desse campo em um único *beacon frame*. A alta versatilidade desse campo opcional faz com que ele seja ideal para a manipulação e inserção de informações, podendo essas serem recuperadas durante um procedimento de busca por redes *Wi-Fi* realizado pelo dispositivo receptor.

Essa é uma técnica de aplicação limitada, visto que a taxa de envio de dados é relativamente baixa. Além disso, essa técnica não possibilita fazer uma comunicação bidirecional simultânea sem que cada um dos dispositivos tenha dois componentes *Wi-Fi* distintos, o que encareceria a solução. Apesar desses fatores considerados negativos, essa técnica é ideal para as necessidades de comunicação sem fio no TSMA, visto que:

- ❏ A frequência da alteração de placas de trânsito é naturalmente baixa e o tamanho da mensagem contendo uma sinalização de trânsito é relativamente pequeno (inferior a 252 bytes);

- ❏ Não há necessidade de haver comunicação bidirecional para o funcionamento da transmissão ou para validação dos dados transmitidos, basta a comunicação unidirecional a partir do módulo TST para o(s) dispositivo(s) VUR;

- ❏ O fato de não haver associação *Wi-Fi* reduz qualquer risco de saturação do dispositivo TST nas situações em que houver uma alta quantidade de veículos, e consequentemente de dispositivos VUR, nas imediações.

O *beacon-stuffing* é uma técnica recente na literatura, da qual a referência mais antiga encontrada é o artigo (CHANDRA et al., 2007), no qual são descritos os referenciais teóricos da técnica e são propostas três formas de utilização da mesma para divulgar anúncios comerciais. Sugestões de melhorias e extensões da técnica foram feitas nos anos seguintes, sendo uma delas (GUPTA; ROHIL, 2012) onde foram listados e detalhados os campos do *beacon* que podem ser utilizados para a inserção de dados.

A partir da descrição inicial da técnica surgiram também outras propostas de uso do *beacon-stuffing*, algo que é apresentado nesta dissertação a título de curiosidade. Uma dessas propostas é o uso para melhorar a precisão com que um certo usuário é localizado geograficamente para melhorar a interação social entre amigos (BANERJEE et al., 2010). Outras utilizações recentes da técnica são (KÖNINGS; SCHAUB; WEBER, 2013), que propõe o uso de *beacons* para propagar informações relevantes à manutenção da privacidade do usuário no contexto de computação ubíqua, e (GIRÓN et al., 2012), onde o

beacon-stuffing é usado para melhorar a QoE (*Quality of Experience*) do usuário no cenário de redes sem fio cooperativas.

Acredita-se que o TSMA é uma proposta inovadora no uso do *beacon-stuffing* no contexto de ITS e, mais especificamente, na implementação de um modelo V2I. Em toda a fase de estudos preliminares, e também durante o período de redação do texto, não foram encontradas referências ao uso da técnica *beacon-stuffing* para melhorar a forma de gestão e exibição das placas de trânsito.

2.2 Trabalhos Correlatos

Segundo (DOWNS, 2004), há uma forte tendência de que o número de congestionamentos, dentre outras consequências do aumento na densidade do tráfego urbano, continue a crescer. Os termos "cidades inteligentes" e "sistemas de transporte inteligentes" ganham destaque em meio às tentativas de minimizar essas consequências e prover segurança e praticidade nas atividades relacionadas ao trânsito. Cada uma das seções a seguir contém a descrição de um trabalho correlato envolvendo um, ou mais, tópicos que estão relacionados ao tema central desta dissertação.

2.2.1 *Variable Message Sign*s (VMS)

As placas de trânsito eletrônicas começaram a ganhar destaque entre as décadas de 80 e 90, e, desde então, têm sido utilizadas em vários contextos substituindo as placas tradicionais. Várias tecnologias foram testadas para a manufatura das VMS, mas tecnologia atualmente dominante é a LED (Light Emitting Diode - Diodo Emissor de Luz). Um exemplo de VMS utilizando a tecnologia LED é exibido na Figura 6.

Os benefícios desse tipo de sinalização sobre as placas tradicionais são próximos do que o TSMA oferece, no caso, o fator dinamicidade que permite a adaptação da sinalização exibida ao contexto do trânsito. Um exemplo disso é a própria sinalização da Figura 6, que avisa aos motoristas de um congestionamento na rodovia 260 envolvendo todas as pistas. Também é importante citar que, embora as primeiras gerações de VMSs só pudessem ser atualizadas presencialmente, alguns dos modelos mais novos já podem até ser atualizadas remotamente, por exemplo utilizando uma conexão GPRS (*General Packet Radio Services*).

É relevante citar que VMSs de LED colorido já estão sendo implantadas e possibilitariam uma gradual substituição da sinalização de trânsito convencional. Neste cenário, é necessário comparar o estado da arte do padrão VMS com o que o TSMA tem a oferecer. As escolhas de tecnologia para a confecção dos painéis é diferente, enquanto as VMSs mais recentes usam a tecnologia LED, o TSMA adotou a tecnologia *E-ink*, que tem um menor consumo energético. Ambos os padrões possibilitam a atualização remota da sinalização,

Figura 6 – Placa de trânsito eletrônica utilizando tecnologia LED.

Retirado de: "*Sign over Interstate 94 in Saint Paul, Minnesota, advising of a road blockage during a winter storm.*".
Disponibilizado em: <*https* : *//commons.wikimedia.org/wiki/File* : *MN_Changeable_Message_Sign.jpg*>, por: Wheresmysocks.
Acesso em jan. 2016.

então nenhuma fica em desvantagem nesse critério. A maior diferença é que a solução do TSMA prevê a interação com veículos e a exibição da sinalização no painel dos mesmos, uma escolha mais compatível com as tendências crescentes de cidades inteligentes e veículos autônomos.

2.2.2 (BARBA et al., 2012)

A proposta contida em (BARBA et al., 2012) é descrita como um método para manter os motoristas atualizados com relação à situação do tráfego nas vias que estão adiante do veículo. No cenário descrito é previsto que houve troca dos semáforos por dispositivos chamados ITLs (*Intelligent Traffic Lights*), que expandem o funcionamento de semáforos tradicionais. Neste cenário também considera-se que cada veículo contém:

- ❏ Módulo veicular adaptado para comunicação *Wi-Fi* no padrão Ad hoc;
- ❏ Dados de posicionamento atual via módulo GPS;
- ❏ Mapa da cidade atual onde constam as posições de cada um dos ITLs (semáforos).

Nesse modelo, cada dispositivo ITL comunica-se via *Wi-Fi*, no padrão Ad hoc, com os veículos que estão em seu alcance, com o objetivo de coletar informações sobre suas posições e enviar-lhes avisos referentes ao nível de congestionamento das vias (cálculo este que é feito dinamicamente, de forma cooperativa entre os ITLs, utilizando o conjunto das

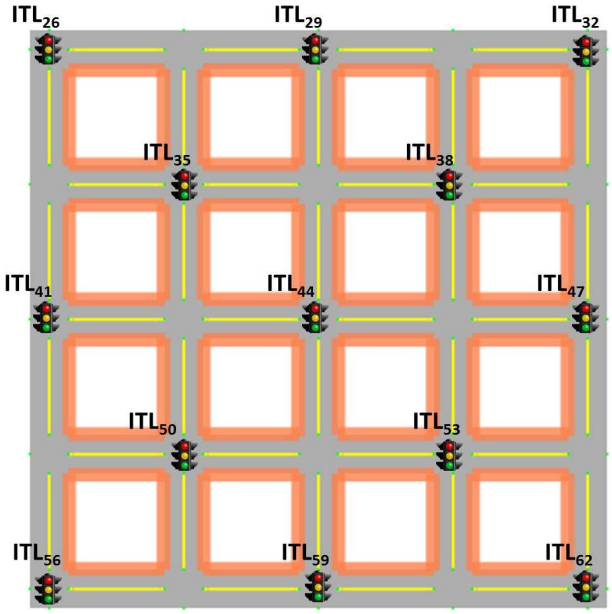

Figura 7 – Distribuição dos Semáforos Inteligentes (ITL)

Retirada de: "*Intelligent Traffic Lights distribution.*" (BARBA et al., 2012).

informações coletadas dos veículos). São usadas antenas *Wi-Fi* omnidirecionais para garantir o alcance do sinal, em todas as direções, pela distância equivalente a um quarteirão. A distribuição dos ITLs que garante cobertura plena é demonstrada na Figura 7.

A proposta contida em (BARBA et al., 2012) não é comparável ao TSMA com relação à sua eficácia, visto que as motivações e objetivos de ambos são diferentes. O diferencial dessa proposta é o uso da tecnologia *Wi-Fi* convencional para comunicação V2I, algo que é implementado, com objetivos e meios diferentes, no TSMA.

2.2.3 (SATO; MAKANAE, 2006)

Em (SATO; MAKANAE, 2006) é apresentado o detalhamento de um sistema eletrônico de sinalização de trânsito que complementa o sistema convencional preexistente. Basicamente, ao invés de depender unicamente das placas de trânsito, o motorista receberia os alertas de sinalização em um dispositivo veicular com tela, conforme apresentado na Figura 8.

A motivação da proposta é reduzir o número de acidentes de trânsito que podem ser evitados ao utilizar uma forma mais chamativa de apresentação da sinalização de trânsito aos motoristas. É previsto que a implantação do sistema é feita enterrando etiquetas (*tags*) RFID passivas contendo os dados da sinalização de trânsito adequada em pontos específicos da pista. Foi escolhido um modelo de etiqueta com 40 cm de alcance, logo, para que um motorista tenha acesso a esses dados, é necessária a instalação de uma antena de leitura RFID embaixo de seu veículo.

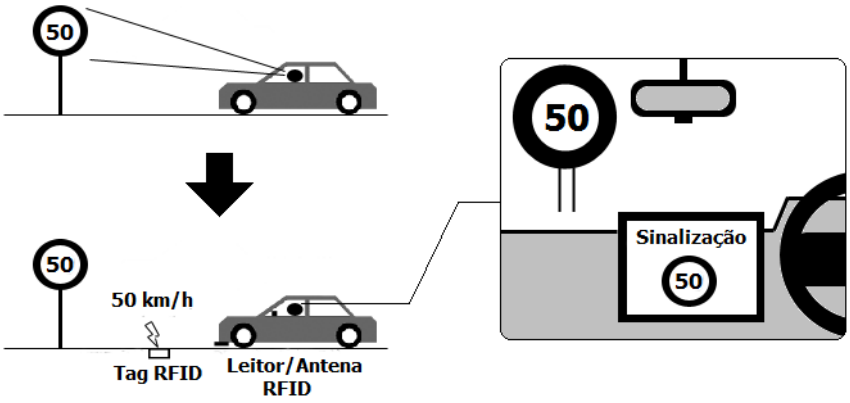

Figura 8 – Sinalização de Trânsito recebida no Veículo.

Adaptada de: "*The in-vehicle signing system utilizing RFID.*" (SATO; MAKANAE, 2006).

A proposta descrita em (SATO; MAKANAE, 2006) é comparável ao TSMA, por exemplo, nos seguintes aspectos:

- Enquanto em (SATO; MAKANAE, 2006) a tecnologia usada para a transmissão da sinalização é o RFID (usando etiquetas passivas), no TSMA a tecnologia adotada é o *Wi-Fi* (usando a técnica *beacon-stuffing*);

- A forma de apresentação da sinalização de trânsito ao motorista é equivalente; no caso, a sinalização é exibida por meio de uma tela no painel veicular;

- A proposta de (SATO; MAKANAE, 2006) não contempla atualizações remotas da sinalização ou mesmo aspectos de segurança como, por exemplo, formas de impedir que alguém mal-intencionado compre uma etiqueta RFID e falsifique uma sinalização. O TSMA permite atualizações remotas (de forma segura e por autoridades competentes) e contém mecanismos de validação das mensagem de sinalização.

2.2.4 (BALDESSARI et al., 2007)

O documento (BALDESSARI et al., 2007) resume e descreve os componentes principais do projeto nomeado "*CAR 2 X Communication System*"; esse modelo prevê a comunicação entre veículos, de veículos com a infraestrutura, e vice-versa. O consorcio que está desenvolvendo este projeto conta com a parceria de grandes montadoras de veículos, entre as quais: Audi, Ford, Honda, Hyundai, Volvo e BMW.

Segundo a proposta, a comunicação entre os elementos do sistema ocorre principalmente por meio do protocolo WAVE, que é descrito na Seção 2.1.3. A Figura 9 exibe um cenário de interação dos elementos envolvidos. Os componentes OBU, RSU e AU são detalhados logo a seguir.

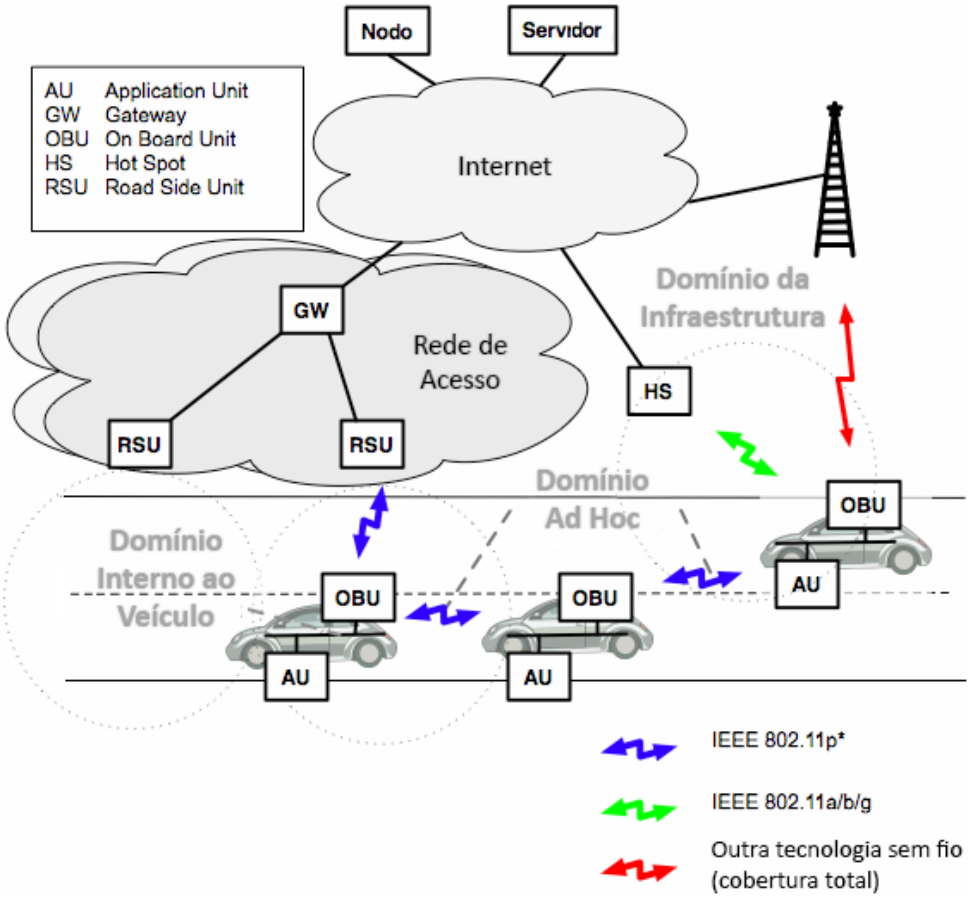

Figura 9 – Sinalização de Trânsito recebida no Veículo.

Adaptada de: "*Draft reference architecture.*" (BALDESSARI et al., 2007).

Na Figura 9 são exibidos três domínios que precisam ser descritos para entendimento pleno do sistema:

- **Domínio Interno ao Veículo**: É uma rede formada pelo módulo OBU (*vehicular On-Board Unit*) e por um número variável de AUs (*Application Unit*s). O AU é um dispositivo que executa um, ou mais, aplicativo(s) que faz(em) uso dos recursos de comunicação disponibilizados pelo OBU. Um AU pode ser tanto um dispositivo fisicamente integrado ao OBU quanto um notebook ou celular, pertencente a um dos ocupantes do veículo, que esteja temporariamente associado ao OBU;

- **Domínio Ad Hoc**: Essa rede, também conhecida como VANET (*Vehicular Ad hoc NETwork*), é composta de veículos equipados com OBUs e módulos fixos que são implantados na lateral das vias, os RSUs (*RoadSide Unit*s). Cada OBU tem, no mínimo, uma interface de rede sem fio que é dedicada à troca de informações utilizadas para garantir a segurança no trânsito. Os OBUs se comunicam por meio de MANETs (*Mobile Ad hoc NETwork*s) que permitem a comunicação direta entre os nós, de forma distribuída, desde que haja conectividade sem fio entre eles. Proto-

colos de roteamento serão aplicados caso a rota de conectividade entre dois nós não seja direta, e o encaminhamento é feito até que o nó de destino seja encontrado. A função principal de cada módulo RSU é atuar como intermediário na expansão do alcance da rede ad hoc, e, dessa forma, ao possibilitar a análise de mais dados das condições de tráfego, aumentar a segurança nas vias;

- **Domínio da Infraestrutura:** Esse domínio provê acesso à Internet para qualquer OBU ou RSU que se associe a ele. O referido domínio está vinculado a uma PKI (*Public Key Infrastructure* - Infraestrutura de Chaves Públicas) que garante a segurança da solução, sendo que uma CA (*Certification Authority* - Autoridade Certificadora) atribui certificados digitais para os dispositivos OBU e os módulos RSU. Esses certificados digitais são usados nas comunicações entre nós da rede para garantir a autenticação dos envolvidos. Os dispositivos OBU tem acesso à Internet enquanto estiverem na área de cobertura de, no mínimo, um módulo RSU, e essa Internet, de igual forma, é compartilhada pelo dispositivo OBU entre os AUs que solicitarem.

A proposta de sistema contida em (BALDESSARI et al., 2007) não pode ser comparada ao TSMA, visto que as motivações são diferentes. O sistema descrito em (BALDESSARI et al., 2007) é um modelo completo e seguro de interação entre veículos e infraestrutura; a implementação desse modelo permitiria, por exemplo, que todos os veículos (em área de cobertura) tivessem acesso à Internet, à situação dos veículos próximos, e às condições do tráfego nas vias adiante. Resumindo, o sistema não tem foco específico na otimização da sinalização de trânsito, mas sua infraestrutura é uma base estável sobre a qual podem ser desenvolvidas aplicações diversas. Um exemplo disso é a proposta descrita na Seção 2.2.5, que aproveita o modelo de (BALDESSARI et al., 2007) e faz uma aplicação com foco na melhoria da sinalização de trânsito.

2.2.5 (FERNANDES, 2009)

Em (FERNANDES, 2009), o autor desenvolve uma linha de argumentação da motivação bem próxima ao que é apresentado nesta dissertação. Basicamente, o autor explica que seu projeto é uma expansão da arquitetura de tráfego explicada na Seção 2.2.4, ou seja, considera-se um ambiente no qual o padrão WAVE é utilizado para estabelecer, de forma natural e cooperativa, comunicação entre os veículos e dos veículos com a infraestrutura que provê Internet. Neste cenário é feito um questionamento com relação à baixa ou inexistente adaptação das placas de trânsito e semáforos a situações rotineiras do trânsito, como acidentes que bloqueiam pistas por um dado período de tempo.

De fato, o autor considera válidas algumas suposições para construir sua proposta:

- ❏ Todos os veículos, sem exceções, estão adaptados ao modelo descrito em 2.2.4, assim sendo, todos dispõem de acesso constante à Internet, um mapa digital, e um equipamento GPS;
- ❏ São garantidas a segurança, baixa latência e confiabilidade da rede de comunicações descrita em 2.2.4 à qual os carros têm acesso;
- ❏ O GPS não apresentará falhas de posicionamento que situem o veículo fora de sua faixa atual.

Nesse contexto, cada veículo mantém uma tabela cujos registros são representações digitais de sinalizações de trânsito contendo, dessa forma, informações como: Identificador da sinalização, localidade de atuação, horário, duração, tipo da sinalização e dados específicos do tipo (complemento). A Tabela 1 exemplifica como seria uma tabela com essa finalidade.

Tabela 1 – Exemplo de Tabela de Sinalizações de Trânsito

Adaptada de: "*Traffic Signs Table (TST).*" (FERNANDES, 2009).

Identificador	**Localidade**	**Horário**	**Duração**	**Tipo**	**Complemento**
203	X_1 Y_1 Z_1	1095370199.25	10s	Semáforo	...
103	X_2 Y_2 Z_2	1095370199.00	1h	Aviso	...
157	X_3 Y_3 Z_3	1095370199.26	30s	Pare	...
...	...	...	...	...	...

É previsto que as verdadeiras tabelas do modelo, que são representadas aqui pela Tabela 1, sejam atualizadas (usando a Internet disponível) com uma alta frequência, especialmente porque os semáforos também são descritos como entidades virtuais nesse trabalho.

De posse da tabela de sinalizações, a exibição delas no painel do veículo é controlada por um algoritmo que exibe a sinalização ao motorista se duas condições forem satisfeitas:

1. A posição atual do veículo está numa proximidade aceitável de **Localidade**;
2. A hora atual está no intervalo entre **Horário** e **Horário** + **Duração**.

O trabalho descrito em (FERNANDES, 2009) é um dos mais similares ao TSMA, visto que essa abordagem se propõe a resolver tanto o problema da impossibilidade de atualizar remotamente a sinalização de trânsito, quanto o problema da sinalização de trânsito exibida de forma insatisfatória.

Apesar das semelhanças de objetivos, é importante notar que a proposta em (FERNANDES, 2009) tenta solucionar os problemas de forma muito diferente, por exemplo nas decisões seguintes:

- **Correlato**:
  Elimina todos os dispositivos físicos de sinalização de trânsito.
  TSMA:
  Atualiza os dispositivos, contemplando substituição pelos equivalentes.

- **Correlato**:
  Total dependência de alta precisão do GPS e disponibilidade da Internet (Embora seja presumida, não é listada nenhuma margem de segurança quanto ao posicionamento GPS recuperado, o que tende a causar erros ou não-funcionamento); sem Internet a tabela de sinalizações não é atualizada e podem surgir situações de inconsistência.
  TSMA:
  Confiança relativa na precisão do GPS, estabelece uma margem de segurança dentro da qual a sinalização é apresentada ao motorista; a Internet só é necessária caso o motorista nunca tenha visitado o lugar atual ou sequer feito o *download* prévio das chaves necessárias para decodificar a sinalização do referido local.

Um resumo da comparação entre as propostas VMS, (SATO; MAKANAE, 2006), (FERNANDES, 2009) e o TSMA está representado na tabela da Seção 2.3.

2.3 Comparativo

É visível que cada uma das três soluções listadas neste capítulo que propõe a adequação da sinalização de trânsito à era digital tem seus pontos positivos e negativos. A Tabela 2 apresenta uma comparação visual de alguns dos fatores que devem ser considerados na avaliação delas. Na Tabela 2, "VMS" refere-se ao modelo descrito na Seção 2.2.1, "Sato" refere-se à proposta contida em (SATO; MAKANAE, 2006) e descrita na Seção 2.2.3, "Jorge" refere-se à solução adotada em (FERNANDES, 2009) e descrita na Seção 2.2.5, enquanto "TSMA" refere-se à proposta que está sendo apresentada por meio desta dissertação.

Entre os atributos comparados na Tabela 2 é importante destacar os seguintes:

- **"Prevê Atualização Remota da Sinalização"**:
  Fator que indica se a solução permite a alteração da sinalização de trânsito por meios digitais de forma não-presencial.

Tabela 2 – Comparativo das Soluções Apresentadas

	VMS	**Sato**	**Jorge**	**TSMA**
Protocolo de Transmissão da Sinalização	-	RFID	802.11p	802.11n
Prevê Atualização Remota da Sinalização?	Sim	Não	Sim	Sim
Dependência de Sinal GPS preciso	Nula	Nula	Alta	Mediana
Dependência de Internet funcional	Esporádica	Nula	Alta	Esporádica
Mantém Placa de Trânsito externa?	Sim	Sim	Não	Sim
Aspectos de Segurança foram Definidos?	Sim	Não	Sim	Sim
Recebimento da Sinalização no Veículo?	Não	Sim	Sim	Sim

- **"Mantém Placa de Trânsito externa"**:
  Fator que indica se na solução é prevista a existência de uma placa de trânsito física que exiba a sinalização aos motoristas. A manutenção dessa placa física é importante como uma redundância positiva em caso de falha do mecanismo principal de sinalização, caso este ocorra pelo recebimento da sinalização no veículo.

- **"Recebimento da Sinalização no Veículo"**:
  Fator que indica se os veículos adaptados para esta solução têm mecanismos de recebimento da sinalização de trânsito e exibição dessa sinalização ao motorista. Esse fator tem o potencial de reduzir o número de acidentes causados pela desatenção dos condutores.

Esses fatores destacados estão relacionados à segurança, confiabilidade e versatilidade dos modelos. Sendo assim, é importante reiterar que o TSMA é a única arquitetura, entre os sistemas comparados, que atende simultaneamente os três fatores destacados.

O Capítulo 3, que segue, apresenta um detalhamento minucioso dos componentes do TSMA, de suas regras de funcionamento e dos mecanismos de segurança que ele implementa.

Capítulo 3

TSMA

O TSMA (*Traffic Sign Management Architecture*) é uma arquitetura de gestão da sinalização de trânsito que permite uma real adaptação das placas ao contexto do trânsito. A proposição desta arquitetura visa abrir novas perspectivas no cenário de ITS, evidenciando a defasagem do modelo atual de gestão da sinalização de trânsito e os riscos inerentes desta condição. Na Figura 10 pode-se observar uma visão geral da proposta.

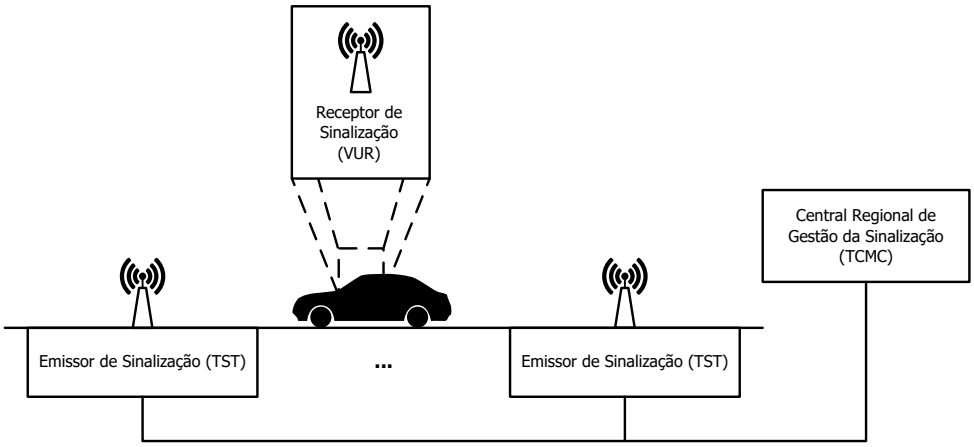

Figura 10 – Comunicação da Sinalização de Trânsito no TSMA.

O cenário exibido na Figura 10 apresenta a interação entre elementos da arquitetura que são detalhados neste capítulo para que haja compreensão do cenário geral. Basicamente, a **Central Regional de Gestão da Sinalização (TCMC - *Traffic Control Management Center*)** é a entidade responsável pela geração e atribuição das placas de trânsito, atribuição esta que é feita pelo envio de dados para entidades do tipo **Emissor de Sinalização (TST - *Traffic Sign Transmitter*)**; que emitem a sinalização recebida para que veículos próximos possam recuperá-la por meio de dispositivos do tipo **Receptor de Sinalização (VUR - *Vehicular Unit Receiver*)**, que são responsáveis por informar o motorista da sinalização vigente. Todos os elementos e interações contemplados no TSMA são detalhados a seguir.

3.1 Central Regional de Gestão da Sinalização (TCMC)

O TCMC é uma entidade local que é responsável pela gestão de todos os TSTs, dispositivos equivalentes às atuais placas de trânsito sob a ótica do TSMA, em sua área de atuação predefinida. Os TCMCs são previstos como sendo extensões do órgão nacional de trânsito. Assim como os funcionários dos órgãos municipais de trânsito realizam a instalação e manutenção das placas de trânsito em suas cidades, de forma equivalente os profissionais de cada TCMC realizam a implantação e manutenção dos dispositivos TST no escopo de atuação do seu respectivo TCMC.

A área de atuação de um TCMC não é fixada por fronteiras municipais, o parâmetro usado para determiná-la é a conveniência dos envolvidos; deve-se considerar a quantidade potencial de placas de trânsito a serem controladas na referida área, o esforço e quantidade de funcionários necessários para isso, entre outros fatores. Uma cidade com 100.000 habitantes pode, por exemplo, manter um único TCMC gerenciando toda a sinalização de trânsito do município, enquanto outra cidade, de porte similar ou maior, pode dividir essa responsabilidade entre dois ou mais TCMCs; a única recomendação feita é de que não haja sobreposição entre as áreas de atuação deles. A Figura 11 apresenta os principais módulos funcionais de um TCMC.

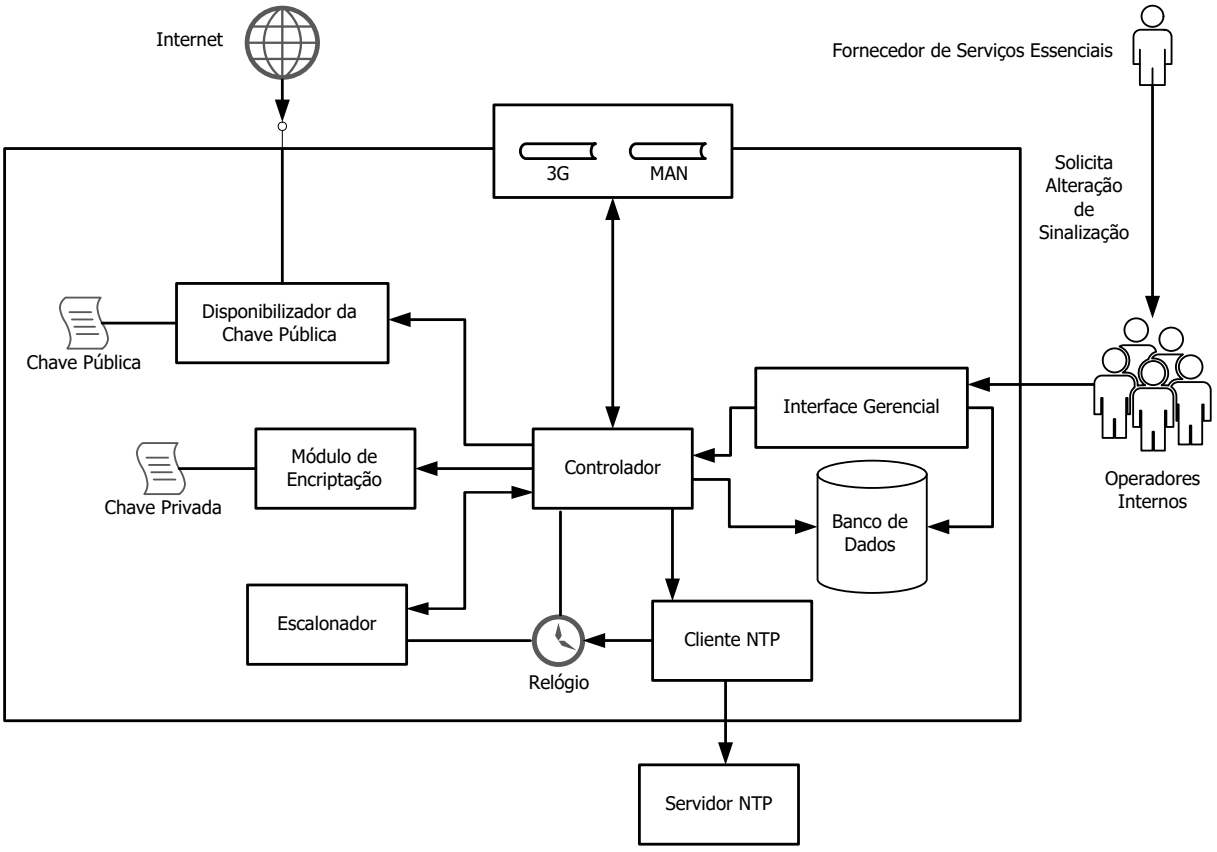

Figura 11 – Detalhamento dos Módulos e Entidades do TCMC.

As interações entre os módulos, elementos, e entidades do TCMC exibidos na Figura 11 ocorrem pela seguinte sequência de passos:

1. Devido a alguma requisição de um **Fornecedor de Serviços Essenciais**, ou motivado por alguma demanda interna, um **Operador Interno** faz uso da **Interface Gerencial** para atribuir uma dada sinalização de trânsito a algum dos TSTs sob sua responsabilidade. O operador tem à sua disposição, por meio da **Interface Gerencial**, um mapa virtual que exibe a posição de cada um dos dispositivos TST; isto facilita a escolha do TST que esteja na localização mais adequada para apresentar a sinalização aos motoristas nas proximidades;

2. A atribuição feita na etapa anterior foi cadastrada com propriedades bem definidas, sendo uma delas a janela de tempo (validade) da sinalização especificada. O módulo **Controlador** é informado dessa atribuição e realiza dois procedimentos, o primeiro é gravar todos os dados e propriedades dessa atribuição como registros do **Banco de Dados** relacional; o segundo é gerar um lembrete no **Escalonador** para que a continuidade do processo de atribuição de sinalização ocorra mais próximo ao horário previsto pela janela de tempo;

3. O **Controlador** é acionado pelo **Escalonador** no horário predefinido e o processo de criação da mensagem de sinalização de trânsito é iniciado. Este processo consiste da recuperação dos dados da atribuição, que foram armazenados no **Banco de Dados**, da organização dos referidos dados conforme a estrutura descrita na Seção 3.4, e da encriptação da referida estrutura, ação executada no **Módulo de Encriptação** usando a **Chave Privada**, para garantir a confiabilidade dos dados conforme descrito na Seção 3.5;

4. Após a geração da mensagem encriptada, seu envio é feito para o dispositivo TST indicado pelo **Operador Interno**. Isso é possível devido à manutenção de uma listagem atualizada dos endereços IP de cada dispositivo TST no **Banco de Dados**. É previsto que esse envio ocorra por meio de uma rede de área metropolitana (MAN - aclman) ou por transmissão via 3G; outras abordagens podem ser consideradas futuramente, visto que não é necessário haver um canal privado de transmissão.

O módulo **Cliente NTP** é usado para manter o **Relógio** interno do sistema atualizado por meio de consulta a servidores NTP externos. A entidade **Fornecedor de Serviços Essenciais** representa policiais e bombeiros que teriam autoridade para solicitar o bloqueio de uma via em caso de acidente, por exemplo. Detalhes sobre o módulo **Disponibilizador da Chave Pública** e os mecanismos de segurança são apresentados na Seção 3.5.

O módulo **Banco de Dados** executa sob o modelo relacional e algumas das entidades mais relevantes para os procedimentos gerenciais são:

- `Placa`: Representa um dispositivo TST que foi implantado na cidade, contém sua posição geográfica, o endereço MAC da interface de rede cabeada, o endereço IP atual do dispositivo e seu identificador único (UID);
- `Sinalização`: Os registros deste tipo correspondem aos tipos de placas de trânsito que podem ser exibidos aos motoristas, por exemplo, as sinalizações de "Pare" ou "Limite de Velocidade". Seus dados são o identificador de tipo da sinalização e a descrição do tipo;
- `Atribuição`: Cada atribuição é a associação de uma determinada `Sinalização` a uma `Placa` por um intervalo de tempo. Os dados mais relevantes da `Atribuição` são o identificador da `Sinalização`, o da `Placa`, e o período de atribuição que é definido por meio dos valores de duas propriedades que serão detalhadas na Seção 3.5: *TIMESTAMP* e *TTL*.

É relevante apontar que, apesar de o TCMC ser a central regional de gestão da sinalização, caso alguma falha técnica impeça temporariamente a gestão dos dispositivos TST, cada dispositivo continuaria funcionando, de forma autônoma, segundo os comandos recebidos previamente. Neste caso de funcionamento autônomo, a sinalização atual é exibida até o fim de seu prazo de validade (instante definido por "TIMESTAMP + TTL"), momento em que volta ser exibida a sinalização anterior, caso ainda seja válida, ou, em caso contrário, o dispositivo deixa de exibir sinalizações até receber novos comandos. Essa autonomia aumenta a confiabilidade percebida do TSMA.

3.2 Emissor de Sinalização (TST)

Os dispositivos TST são correspondentes às atuais placas de trânsito no TSMA. As funções principais de cada unidade TST são:

- Disseminar as mensagens válidas de sinalização recebidas aos veículos que estejam nas proximidades;
- Controlar a exibição, em tela acoplada, da sinalização de trânsito aos motoristas.

Ao contrário das placas de trânsito convencionais, cuja sinalização de trânsito não pode ser alterada, os dispositivos TST dispõem de mecanismos para troca da sinalização exibida e disseminada (propagada). As adaptações necessárias para prover este recurso tornam o dispositivo mais complexo e custoso do que uma placa de trânsito convencional, entretanto é necessário considerar fatores humanos, como a potencial redução do número de acidentes, e a economia obtida ao, por exemplo, evitar o deslocamento de agentes de

trânsito para fechar vias interditadas; procedimento este que, em alguns cenários, poderia ser feito por meio da atualização remota de dispositivos TST em posições estratégicas. A Figura 12 apresenta os módulos de um dispositivo TST.

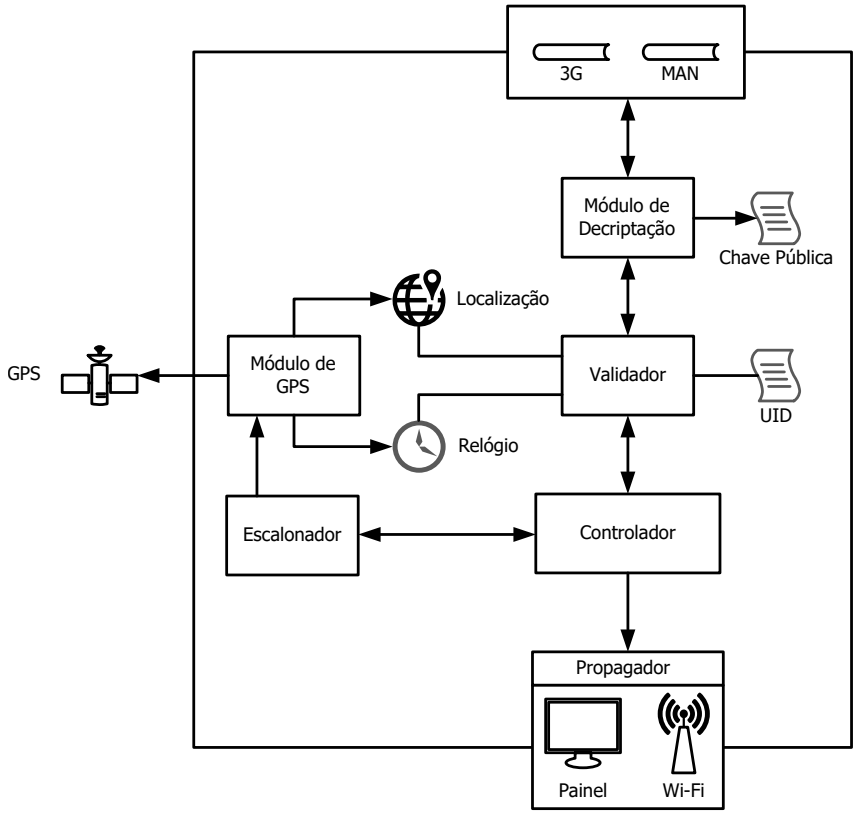

Figura 12 – Detalhamento dos Módulos do TST.

Os módulos e elementos do dispositivo TST que são apresentados na Figura 12 interagem segundo um fluxo de execução bem definido cujas etapas seguem:

1. Uma mensagem é recebida por transmissão via 3G ou por meio de uma rede de área metropolitana (MAN) e a suposição inicial do dispositivo é de que essa mensagem (`EMsg`) está parcialmente encriptada e segue os padrões do TSMA; esses padrões são descritos na Seção 3.4. As próximas etapas do fluxo de execução têm a finalidade de testar se esta suposição inicial é verdadeira e, em caso negativo, descartar a mensagem `EMsg`;

2. O **Módulo de Decriptação** faz uma tentativa de decifrar a parte encriptada da mensagem `EMsg` usando a **Chave Pública**. Em caso de fracasso deste procedimento a mensagem é descartada; já em caso de sucesso, tanto a mensagem resultante dele, `Msg`, quanto a mensagem original, `EMsg`, avançam para a etapa seguinte do teste;

3. O **Validador** é um módulo cuja função é verificar se os dados da mensagem `Msg` são válidos e se correspondem aos valores esperados de uma mensagem destinada

àquele dispositivo específico no horário atual. Este procedimento de validação é melhor descrito na Seção 3.5, onde também são explicados os motivos pelos quais ele é necessário. Em caso de validação negativa a mensagem é descartada; Em caso positivo, ambas as versões da mensagem, `Msg` e `EMsg`, avançam à próxima etapa;

4. O **Controlador** envia uma solicitação ao **Escalonador** para que este último o acione no horário de início da validade da mensagem, conforme definido pelo atributo *TIMESTAMP* de `Msg`. O **Controlador** é acionado no horário preestabelecido e inicia o processo de emissão da nova sinalização;

5. A emissão, ou propagação, da sinalização de trânsito ocorre por meio da interface *Wi-Fi* usando a técnica de *beacon-stuffing*, descrita na Seção 2.1.4. O objeto desta emissão é a mensagem `EMsg`, a mesma que foi recebida inicialmente do TCMC. Além da emissão via *Wi-Fi*, o dispositivo TST exibe a sinalização de trânsito equivalente à mensagem `Msg` em um painel acoplado ao próprio dispositivo.

A principal motivação para a existência do painel digital que exibe a sinalização de trânsito é dar suporte a motoristas cujo veículo ainda não foi equipado com uma unidade VUR. A sinalização é exibida no próprio veículo caso este já tenha sido adaptado ao padrão TSMA, ou seja, neste caso a sinalização externa torna-se redundante. A tecnologia atual considerada mais adequada para a fabricação deste painel é o *E-ink*, visto que telas *E-ink* têm um consumo de energia extremamente baixo quando são comparadas a outros padrões como *LED* ou *OLED* e também oferecem uma melhor visibilidade, tanto em período diurno quanto noturno. Um fator que reforça os benefícios das telas *E-ink* neste cenário é que já houve adoção desta tecnologia para produzir placas de trânsito digitais que estão sendo implantadas em Sidney, Austrália[1]; outro exemplo do uso de telas *E-ink* para sinalização é a adoção, em Londres, dessa tecnologia para implementar painéis com os horários de paradas dos ônibus[2].

O **Módulo de GPS** presente no dispositivo TST faz uso da funcionalidade GPS para manter atualizados a localização e relógio interno do dispositivo. É revelante citar que o TSMA, ao contrário de outras arquiteturas similares como (FERNANDES, 2009), não depende de uma precisão tão alta na localização provida pelo GPS para seu correto funcionamento. O GPS, no caso do TSMA, é usado mais em um contexto secundário de validação e, por isso, é razoável aceitar uma margem de erro.

O **UID** é um identificador único do dispositivo TST que é usado para diferenciá-lo no recebimento de mensagens, esse valor é definido no momento de preparação do dispositivo TST para implantação. O **UID** só pode ser alterado presencialmente e por um funcionário do TCMC com as permissões devidas.

[1] Fonte: <www.visionect.com/blog/worlds-first-epaper-traffic-signs>, Acesso: 23/12/2015
[2] Fonte: <www.bbc.com/news/technology-35162689>, Acesso: 23/12/2015

Visto que a transmissão da mensagem de sinalização entre o dispositivo TST e o módulo VUR acontece por meio da propagação *Wi-Fi* conforme o *beacon-stuffing*, é necessário agir preventivamente para que a sinalização seja recebida apenas por veículos que estejam em situações nas quais a sinalização é relevante. Um exemplo de situação a ser trabalhada, por exemplo, é de uma via com duas pistas de direções opostas onde somente em uma delas deve ser exibida uma sinalização indicando que é permitido seguir em frente ou virar à direita. Sendo assim, é necessário limitar a propagação apenas a veículos na pista adequada; isto pode ser feito substituindo no TST a convencional antena omnidirecional por uma de tipo setorial. Uma comparação visual entre os tipos de antena, com relação ao modelo de emissão de sinais, é exibida na Figura 13.

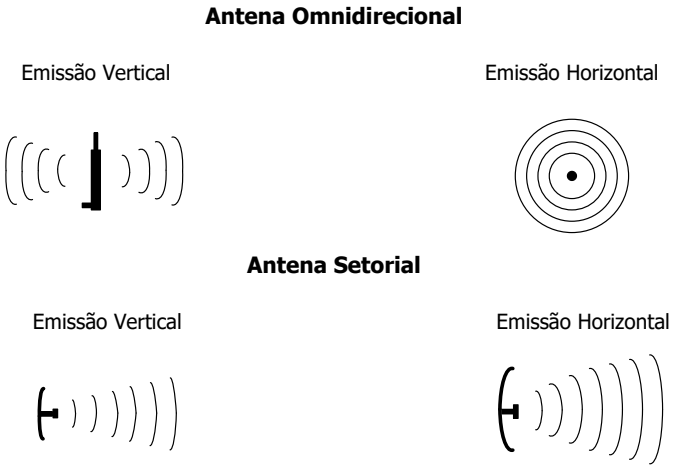

Figura 13 – Comparação entre antenas Omnidirecional e Setorial.

Conforme a Figura 13, é possível definir um foco para onde os sinais emitidos pela antena setorial são direcionados, algo que não é possível realizar, de forma prática e satisfatória, apenas com uma antena omnidirecional. Cada um desses tipos tem seu uso, e a escolha de qual antena será instalada depende da direção das pistas e do tipo de sinalização que será propagado com mais frequência a partir do local de implantação do TST.

É relevante apontar que, entre as soluções revisadas na literatura correlata (Seção 2), o TSMA é o único modelo que prevê, simultaneamente:

- ❏ Exibição da sinalização em tela externa ao veículo;
- ❏ Exibição da sinalização no painel do veículo;
- ❏ Possibilidade de atualização remota da sinalização.

3.3 Receptor de Sinalização (VUR)

Cada veículo que está em conformidade com os padrões da arquitetura TSMA dispõe de um dispositivo VUR. A principal ação do VUR é recuperar mensagens contendo sinalizações de trânsito que tenham sido emitidas por dispositivos TST via *Wi-Fi* e apresentá-las ao condutor do veículo em questão.

Uma das motivações para a proposição do TSMA é a constatação da alta taxa de mortalidade devido a acidentes de trânsito. Ao levar a sinalização de trânsito para dentro de cada veículo, e apresentá-la de forma adequada ao motorista, há uma expectativa grande de redução na quantidade de acidentes causados por desatenção.

Outra possibilidade aberta pelo recebimento da sinalização de trânsito nos veículos é o uso desses dados para melhorar a atuação de veículos autônomos. Várias tecnologias distintas que possibilitam a direção autônoma, por parte de veículos, estão sendo desenvolvidas e aprimoradas por empresas de grande porte, como Google[3] e BMW[4], o que indica um grande interesse por essa área de pesquisa. O TSMA foi especificado para, entre outras funcionalidades, transmitir a sinalização de trânsito aos veículos; após receber esses dados, sistemas de direção autônoma poderiam utilizá-los para garantir obediência à sinalização e aumentar sua própria eficácia. A Figura 14 exibe os módulos de um dispositivo VUR.

O funcionamento do dispositivo VUR é regido por uma sequência de etapas muito similar à do dispositivo TST. Basicamente, os módulos e elementos da Figura 14 interagem conforme os seguintes passos:

1. O módulo *Wi-Fi* estará fazendo buscas constantes no espectro a procura de anúncios de redes *Wi-Fi* disponíveis que contenham dados no padrão de mensagens do TSMA, procedimento este que é típico de um receptor sob a técnica *beacon-stuffing*. O procedimento de busca é executado constantemente, mas após encontrar alguma rede cujo anúncio contem dados no padrão do TSMA, tais dados são selecionados como uma mensagem (`EMsg`) que segue para análise;

2. A mensagem `EMsg`, que pode ou não conter informações de uma sinalização de trânsito válida, passa por uma tentativa de decifragem por parte do **Módulo de Decriptação**; procedimento este que será melhor explicado na Seção 3.5. É realizado o descarte de `EMsg` caso a decifragem falhe e, em caso contrário, tanto a mensagem decifrada, `Msg`, quanto a mensagem original, `EMsg`, seguem para a etapa de Validação;

[3] Fonte: <www.google.com/selfdrivingcar>, Acesso: 20/01/2016

[4] <Fonte:www.autoguide.com/auto-news/2013/02/bmw-targets-2020-for-self-driving-cars.html>, Acesso: 20/01/2016

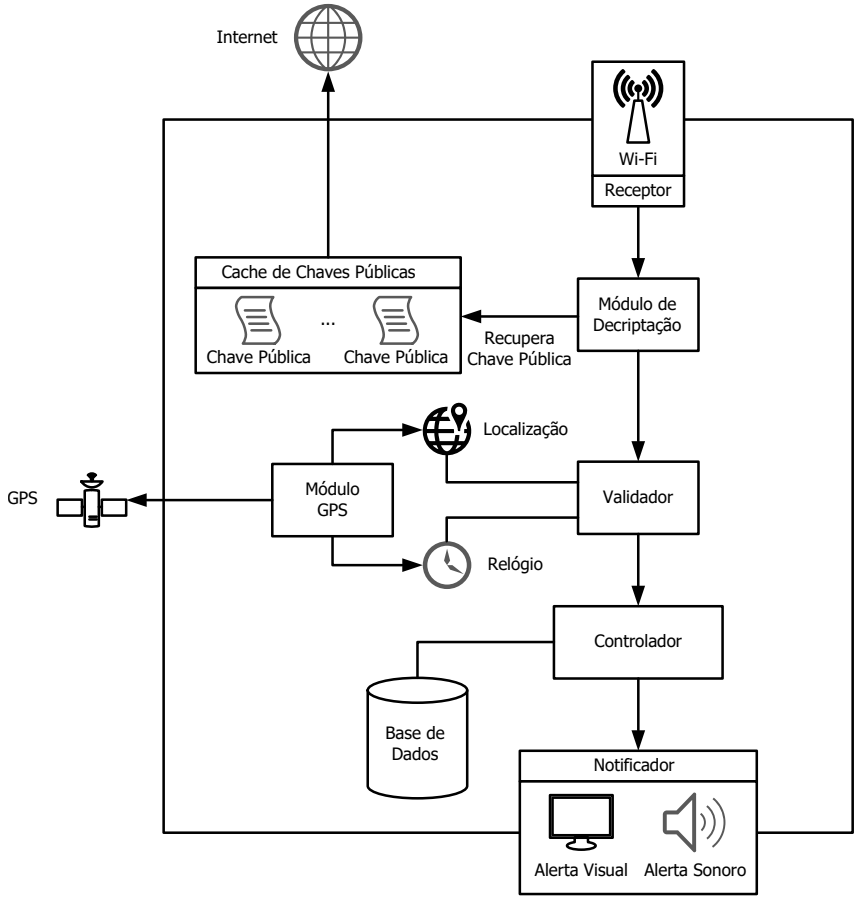

Figura 14 – Detalhamento dos Módulos do VUR.

3. O procedimento realizado pelo **Validador** ocorre pela comparação das propriedades contidas em `Msg` com o horário e localização geográfica atuais. Esta comparação é detalhada na Seção 3.5 e, em caso de sucesso da mesma, `Msg` e `EMsg` são delegadas ao **Controlador**. Em caso contrário ocorre o descarte de ambas;

4. O módulo **Controlador** armazena `EMsg` na `Base de Dados` que tem a função correspondente a uma caixa preta e provê a possibilidade de auditoria das sinalizações recebidas. Logo em seguida ocorre a notificação do motorista com a sinalização de trânsito equivalente por meio de imagem e som.

O **Módulo de Decriptação** solicita a chave necessária para decifrar a mensagem corrente ao **Cache de Chaves Públicas** e, caso ele contenha a chave requisitada, esta é oferecida em tempo mínimo. É necessário fazer uma consulta a repositórios da Internet caso a chave pública solicitada não esteja no cache e, por isso, é recomendado o uso de uma recuperação proativa baseada na localização do veículo ou no trajeto inserido no dispositivo GPS do veículo. O único motivo para recomendar uma recuperação proativa é evitar que seja feita uma consulta na Internet em tempo real, procedimento que estaria sujeito a possíveis instabilidades da rede que fogem ao controle do TSMA; entretanto,

em situações normais, essa consulta seria bem sucedida e a sinalização seria decifrada rapidamente e de forma transparente ao condutor. É importante destacar que, mesmo que ocorra um atraso na recuperação em tempo real da chave pública, a sinalização estará visível ao condutor por meio de um painel *E-ink* anexo ao dispositivo TST.

Um diferencial do TSMA, e mais especificamente do VUR, é a intensidade variável de notificação da sinalização de acordo com o contexto do veículo e as necessidades do condutor. Usando o GPS acoplado é possível identificar o contexto do veículo e adaptar o tipo de aviso à urgência do mesmo; um veículo trafegando a 80 km/h que está próximo a uma sinalização que indica 60 km/h como sendo o limite de velocidade exibirá um aviso muito mais intenso do que se o veículo estivesse trafegando a 55 km/h, por exemplo. Um exemplo de ajuste à necessidade do condutor é, por exemplo, um motorista com problemas de visão poder usar um VUR com uma tela maior acoplada e, de forma equivalente, um motorista poderia aumentar o volume de notificação do seu VUR de acordo com sua necessidade. Essas possibilidades contrastam totalmente com a forma atual de interação com as placas de trânsito estáticas que fazem parte do modelo atual de sinalização.

3.4 Mensagem de Sinalização de Trânsito no TSMA

A transmissão de uma sinalização de trânsito, a partir do TCMC até os dispositivos VUR, é feita por meio do envio de mensagens de sinalização do TSMA, que são instâncias de estruturas de dados cujo formato e propriedades seguem um padrão específico. Esse modelo estrutural garante a integridade das mensagens e limita o tamanho delas para tornar mais fluída a troca de dados entre as entidades da arquitetura. A Figura 15 apresenta tal estrutura, com todas as suas propriedades e o espaço, em bits, que ocupam.

As propriedades exibidas na Figura 15 têm as seguintes funções e tamanhos:

- **VERSION (1 Byte - 8 Bits)**:
  Identificador da versão do protocolo de comunicação do TSMA que está sendo aplicado na interação (entre versões diferentes pode haver mudanças na estrutura da mensagem, porém esta propriedade sempre ocupa a primeira posição e a mesma quantidade de espaço);

- **BEACON_TYPE (2 Bytes - 16 Bits)**:
  Identificador padrão de uma mensagem de sinalização do TSMA. Caso o valor da propriedade seja `0x56AF`, está identificada uma mensagem que deve ser tratada como participante da interação entre entidades do TSMA. Este valor foi definido de forma puramente arbitrária;

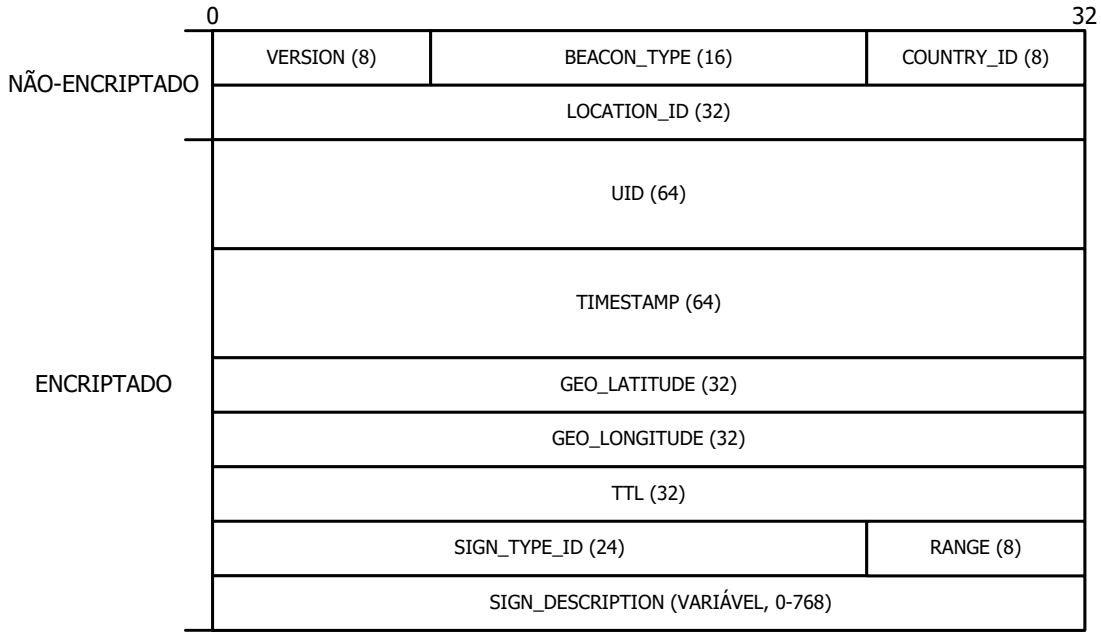

Figura 15 – Estrutura de uma Sinalização de Trânsito no TSMA.

- **COUNTRY_ID (1 Byte - 8 Bits)**:
  Identificador do país no qual o dispositivo TST está localizado. O valor desta propriedade é usado, juntamente com o valor da propriedade `LOCATION_ID`, para identificar e recuperar a chave pública que deve ser usada para decifrar a parte encriptada da mensagem;

- **LOCATION_ID (4 Bytes - 32 Bits)**:
  Identificador da região na qual o dispositivo TST está localizado. O valor desta propriedade é usado, juntamente com o valor da propriedade `COUNTRY_ID`, para identificar e recuperar a chave pública que deve ser usada para decifrar a parte encriptada da mensagem. Cada `LOCATION_ID` é único em seu país e um deles é atribuído, de forma única, a cada TCMC do país;

- **UID (8 Bytes - 64 Bits)**:
  Identificador único do dispositivo TST, no escopo de um TCMC, ao qual a sinalização foi atribuída e que realizará a disseminação da mesma;

- **TIMESTAMP (8 Bytes - 64 Bits)**:
  Horário em que a sinalização de trânsito definida por esta mensagem se tornará efetiva. Esta propriedade tem segundos como sua unidade padrão e usa a mesma data-base do *timestamp* `UNIX` , no caso, o primeiro instante do ano 1970;

- **GEO_LATITUDE (4 Bytes - 32 Bits)**:
  Latitude geográfica do dispositivo TST em representação numérica;

- **GEO_LONGITUDE (4 Bytes - 32 Bits)**:
  Longitude geográfica do dispositivo TST em representação numérica;

- **TTL (4 Bytes - 32 Bits)**:
  Quantidade de segundos que expressa a duração de validade da sinalização a partir do momento definido pelo `TIMESTAMP`;

- **SIGN_TYPE_ID (3 Bytes - 24 Bits)**:
  Identificador numérico da sinalização de trânsito que deve ser exibida aos motoristas;

- **RANGE (1 Byte - 8 Bits)**:
  Raio de cobertura da sinalização, em metros, a partir da localização geográfica do dispositivo TST. É usado, na validação de mensagens recebidas pelo VUR, para testar se o veículo em questão está dentro da área na qual a sinalização deve ser efetiva;

- **SIGN_DESCRIPTION (0 a 96 Bytes (variável) - 0 a 768 Bits**:
  Campo genérico de descrição que pode ser usado na transmissão de informações adicionais. Seu tamanho é variável, porém foi limitado em até 96 bytes nesta primeira versão da arquitetura. Essa limitação foi fixada de forma arbitrária, deixando uma margem de tamanho para futuras expansões de alguma das propriedades definidas ou mesmo para a criação de novas propriedades conforme julgar-se necessário.

Na Seção 4.4 são listados valores que cada uma das propriedades poderia assumir, bem como é demonstrada a viabilidade da transmissão dessa estrutura por meio da técnica *beacon-stuffing*.

Na técnica *beacon-stuffing*, conforme descrito na Seção 2.1.4, os dados que precisam ser transferidos são inseridos em campos opcionais do *beacon frame*, que é um bloco de informações emitido continuamente para anunciar a presença de *Access Points* (APs). Mais especificamente, o campo do *beacon frame* escolhido para uso pelo TSMA é do tipo *Information Element*. Este campo pode ser preenchido com até 255 bytes de dados e, para evitar a divisão da mensagem de sinalização entre várias instâncias do mesmo campo, foi determinado que 255 bytes é o limite teórico de tamanho que uma mensagem do TSMA poderia assumir em versões futuras da arquitetura.

Embora o limite teórico de tamanho que a mensagem de sinalização pode assumir seja de 255 bytes, nesta versão inicial da arquitetura os limites de tamanhos disponíveis para as propriedades da mensagem foram definidos de forma a resultar em um tamanho de 200 bytes, após a encriptação, conforme descrito na Seção 3.5.

3.5 Segurança no Âmbito do TSMA

Os principais mecanismos de segurança do TSMA se baseiam na criptografia assimétrica, usando uma implementação pública do clássico algoritmo RSA (RIVEST; SHAMIR; ADLEMAN, 1978). A parte da mensagem de sinalização que deve ser encriptada ocupa, no caso máximo, 128 bytes de tamanho; entretanto, o tamanho do resultado do processo de encriptação da referida parte, usando uma chave criptográfica de 1536 bits, é 192 bytes. A diferença de tamanho pós-encriptação é consequência do processo de enchimento (*padding*), que é usado para eliminar vulnerabilidades da criptografia.

O tamanho da chave criptográfica foi escolhido tendo em mente a limitação referente ao tamanho de mensagens do TSMA, que é 255 bytes. O resultado do processo de encriptação tem o mesmo tamanho que a chave utilizada devido ao enchimento. Logo, a encriptação utilizando uma chave de 2048 bits produz um resultado com tamanho de 256 bytes (maior que o limite definido para o tamanho de mensagens), enquanto uma chave de 1536 bits produz um resultado com 192 bytes de tamanho. Uma das literaturas que deu embasamento à escolha deste tamanho foi (LENSTRA, 2004), onde estimou-se que uma chave de 1536 bits utilizada no algoritmo RSA seria segura pelo menos até o ano 2025.

Como a parte não-criptografada da mensagem ocupa 8 bytes, e a parte criptografada ocupa 192 bytes, obtém-se uma mensagem resultante com 200 bytes de tamanho. A Figura 16 mostra a aplicação da criptografia assimétrica no TSMA, onde a chave privada é usada no TCMC para encriptar a mensagem de sinalização e a chave pública é usada nos dispositivos TST e VUR para decriptá-la.

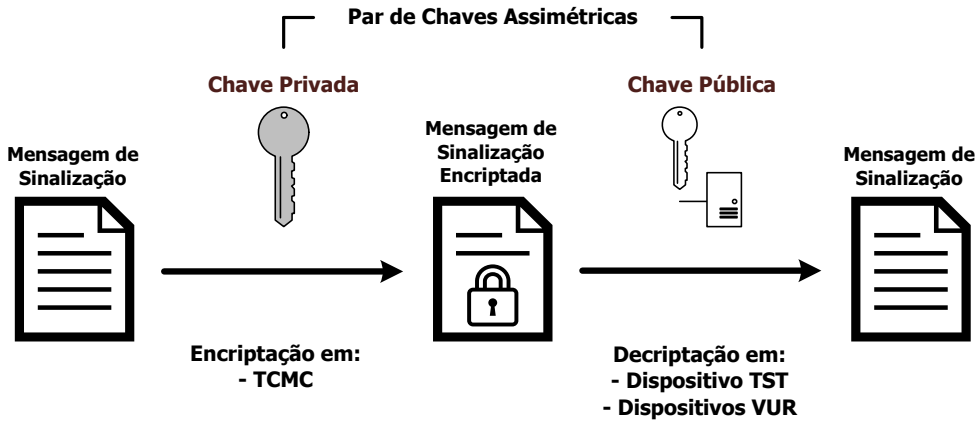

Figura 16 – Visão Geral do Uso da Criptografia Assimétrica no TSMA.

As chaves públicas, que são divulgadas abertamente pelo **Disponibilizador da Chave Pública**, podem ser agrupadas em repositórios de chaves públicas (PKR - *Public Key Repository*), de onde essas chaves serão recuperadas posteriormente por dispositivos VUR. Já as chaves privadas são mantidas em sigilo sob a responsabilidade dos gestores do TCMC. Dessa forma, o TCMC é a única entidade capaz de encriptar mensagens TSMA válidas para a região de sua competência. A mensagem de trânsito é enviada ao dispositivo TST específico logo após sua geração e encriptação usando a chave privada. Dispositivos TST e VUR serão capazes de decifrar as mensagens usando a respectiva chave pública.

Cada dispositivo TST é implantado com uma cópia da chave pública vigente em sua localidade-destino. Caso o par de chaves usado pelo TCMC precise ser trocado, por motivos de segurança, é vislumbrado que essa substituição deva ser feita por intervenção manual a cada TST, visto que a chave que poderia ser usada para a transmissão de tal atualização foi comprometida. Uma possibilidade alternativa que será pesquisada para as próximas versões da arquitetura é ter um segundo par de chaves secreto que seja utilizado apenas na atualização remota de chaves públicas.

Enquanto os dispositivos TST são implantados já com a única chave pública que precisarão utilizar, os dispositivos VUR, se não fizerem uso de uma abordagem proativa, terão de recuperar, em tempo de execução, as chaves públicas à medida que precisem delas, por meio do supracitado PKR. É relevante citar que a chave pública tem um tamanho de apenas 192 bytes, logo é razoável considerar que, em condições normais de acesso à Internet, o módulo VUR é capaz de recuperar essa informação em tempo ínfimo.

Uma infraestrutura de chaves públicas (PKI - *Public Key Infrastructure*) poderia ser utilizada como o principal mecanismo de segurança do TSMA, entretanto isso causaria um aumento na complexidade da solução, inclusive traria a necessidade de cada veículo ter um par único de chaves assimétricas. A solução formada pela combinação de simples repositórios de chaves públicas (PKR) e métodos de autenticação baseados em criptografia assimétrica gera um mecanismo de segurança muito eficiente para este cenário.

A encriptação parcial das mensagens do TSMA, associada ao sigilo da chave privada, gera uma situação na qual uma entidade mal-intencionada, que não dispõe da chave privada, não é capaz de gerar uma nova mensagem de sinalização, ou modificar uma mensagem capturada, e fazer com que tal mensagem seja aceita como válida por dispositivos da arquitetura. Outras tentativas de fraude envolvem capturar mensagens de sinalização válidas e tentar reproduzi-las em horários ou localidades indevidos, a proteção contra esses ataques é implementada por meio do módulo **Validador** dos dispositivos.

O processo de validação das mensagens é resumido na Figura 17, sendo todas as três etapas aplicáveis no recebimento de mensagens pelo dispositivo TST e somente as etapas “Validação do Horário” e “Validação da Localidade” aplicáveis no recebimento de mensagens por dispositivos VUR. Segue o detalhamento dos procedimentos realizados em cada etapa:

- **Validação do UID:**
  Evita que mensagens de sinalização criadas para serem disseminadas em um certo dispositivo TST sejam aceitas, e consequentemente disseminadas, por outro dispositivo TST. É implementada pela comparação do valor recebido na propriedade "UID" da mensagem com o valor do elemento **UID** do dispositivo, que é seu identificador único. A validação tem resultado positivo quando a comparação resulta em igualdade, ou seja, a mensagem foi recebida pelo dispositivo TST que era seu verdadeiro destinatário;

- **Validação do Horário:**
  Evita que dispositivos TST e VUR aceitem quaisquer mensagens cuja janela de validade tenha se encerrado. A janela de validade de uma mensagem é definida como o intervalo entre os resultados das expressões "TIMESTAMP" e "TIMESTAMP + TTL", que são calculados pelos valores contidos nas propriedades de mesmo nome da referida mensagem. É relevante apontar que, no caso dos dispositivos TST e VUR, o horário é mantido atualizado através da tecnologia GPS, enquanto no TCMC faz-se uso do serviço NTP para isso. Assim sendo, todas as entidades do TSMA mantém seus relógios sincronizados e evitam conflitos de horário entre si. A validação tem resultado positivo caso a janela de validade esteja vigente ou se inicie em horário futuro;

- **Validação da Localidade:**
  Evita que dispositivos TST e VUR aceitem mensagens recebidas quando estavam fora da área onde a mensagem é válida e pertinente. A validação da localidade ocorre ao comparar a localização atual do dispositivo à área de atuação definida pelos valores das propriedades "GEO_LATITUDE", "GEO_LONGITUDE" e "RANGE" da mensagem recebida, as duas primeiras no caso definem as coordenadas centrais da área de atuação e a última define um raio de atuação. O resultado da validação será positivo apenas se o dispositivo estiver atualmente na área de atuação da sinalização.

Todas as mensagens de sinalização recebidas que tiverem resultado negativo em alguma das validações são sumariamente descartadas. Embora os equipamentos GPS também forneçam um valor referente à altitude calculada, esse valor não é usado pelo TSMA, visto que a precisão desse valor é muito baixa[5] e que ele não é necessário para o funcionamento da arquitetura.

Além das medidas adotadas para garantir a confiabilidade da arquitetura, também há propostas para garantir uma resposta ágil em caso de desastre, falha ou vandalismo dos dispositivos TST. Basicamente, o **Escalonador** do dispositivo envia, sob um certo intervalo de tempo, 10 minutos, por exemplo, notificações de situação ao TCMC. Se

[5] Fonte: <http://gpsinformation.net/main/altitude.htm>, Acesso: 20/01/2016

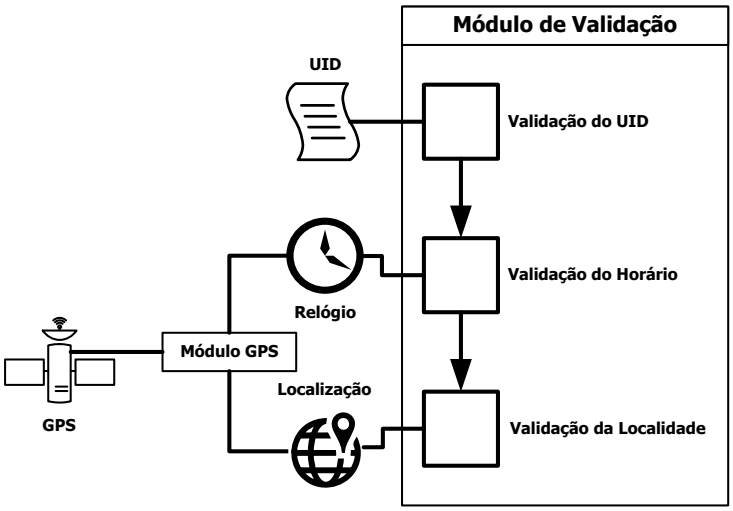

Figura 17 – Detalhamento do Mecanismo de Validação de Mensagens.

a recepção dessas mensagens cessar, é um forte indício de falha e da necessidade de verificação das condições do aparelho.

Uma pessoa mal-intencionada poderia tentar sabotar o TSMA de várias formas. Algumas dessas tentativas previstas são listadas a seguir, bem como a forma de proteção do TSMA contra o referido método de ataque:

❑ Repetição não-autorizada de mensagem do TSMA.

Ataque:
O atacante captura a transmissão de uma mensagem autêntica do TSMA e reproduz seu conteúdo em outro lugar no qual a sinalização capturada não deve ser distribuída.

Defesa:
A parte criptografada da mensagem capturada não pode ser alterada sem que a mensagem perca sua validade, visto que o atacante não possui a chave privada. Sendo assim, a mensagem só teria a chance de ser considerada válida por algum módulo VUR se fosse disseminada na própria localização do dispositivo TST cuja mensagem foi capturada e durante o tempo de validade dela, que é definido pelas propriedades “TIMESTAMP” e “TTL”. A disseminação da mensagem original, sob essas condições, pode ser problemática se o TST receber uma nova mensagem para disseminar enquanto a mensagem capturada ainda for válida. Essa situação poderia confundir motoristas caso sejam apresentados a ambas as mensagens, atualizada e desatualizada, de forma intermitente. A gravidade dessa situação é atenuada, visto que o painel anexo ao TST estaria exibindo a sinalização atualizada, para tirar quaisquer dúvidas dos condutores. Além disso, em momentos nos quais o dispositivo VUR recupere ambas as si-

nalizações, sua escolha pela mensagem mais recente elimina o problema. Outra forma de atenuar esta situação é utilizando mensagens válidas por uma duração menor que são renovadas constantemente. De fato, este tipo de ataque não apresenta uma vulnerabilidade considerável do TSMA, visto que a criptografia é usada para manter a integridade das mensagens.

- ❑ Movimentação indevida do TST

  Ataque:
  Um dispositivo TST é levado, de forma não-autorizada, para outra localidade.

  Defesa:
  Todas as mensagens contendo sinalizações de trânsito que são atribuídas a dispositivos TST contém as coordenadas geográficas do TST em questão, de forma que as mensagens só serão disseminadas pelo TST caso ele esteja em uma localidade dentro de uma pequena margem de erro das referidas coordenadas que vieram na mensagem. Logo, o TSMA não é vulnerável a este tipo de ataque, dado que as validações de localização impedem o funcionamento do TST fora de sua área original de atuação.

- ❑ Geração de mensagens falsas de sinalização do TSMA

  Ataque:
  Um atacante tenta gerar uma mensagem válida do TSMA.

  Defesa:
  As informações críticas das mensagens de sinalização do TSMA passam por um processo de encriptação, usando uma chave privada, para garantir sua integridade. Caso o atacante não disponha da chave privada (que é mantida em sigilo no TCMC), ele não é capaz de gerar mensagens que sejam consideradas válidas.

- ❑ Ataque *Man-in-the-middle*

  Ataque:
  Um atacante tenta modificar uma mensagem válida do TSMA que está sendo transmitida do TCMC a um TST.

  Defesa:
  Conforme exibido na Figura 15, os dados mais importantes de uma mensagem do TSMA são mantidos encriptados e, dessa forma, mantendo o sigilo da chave privada é possível garantir a integridade das mensagens entre o TCMC e os dispositivos TST e VUR. Logo, qualquer tentativa de modificação sem ter a chave privada invalida a mensagem.

A Figura 18 é um diagrama de sequência que apresenta, de forma resumida, a interação entre os elementos citados neste capítulo em um fluxo típico de execução do TSMA, contemplando os passos de validação da mensagem de sinalização.

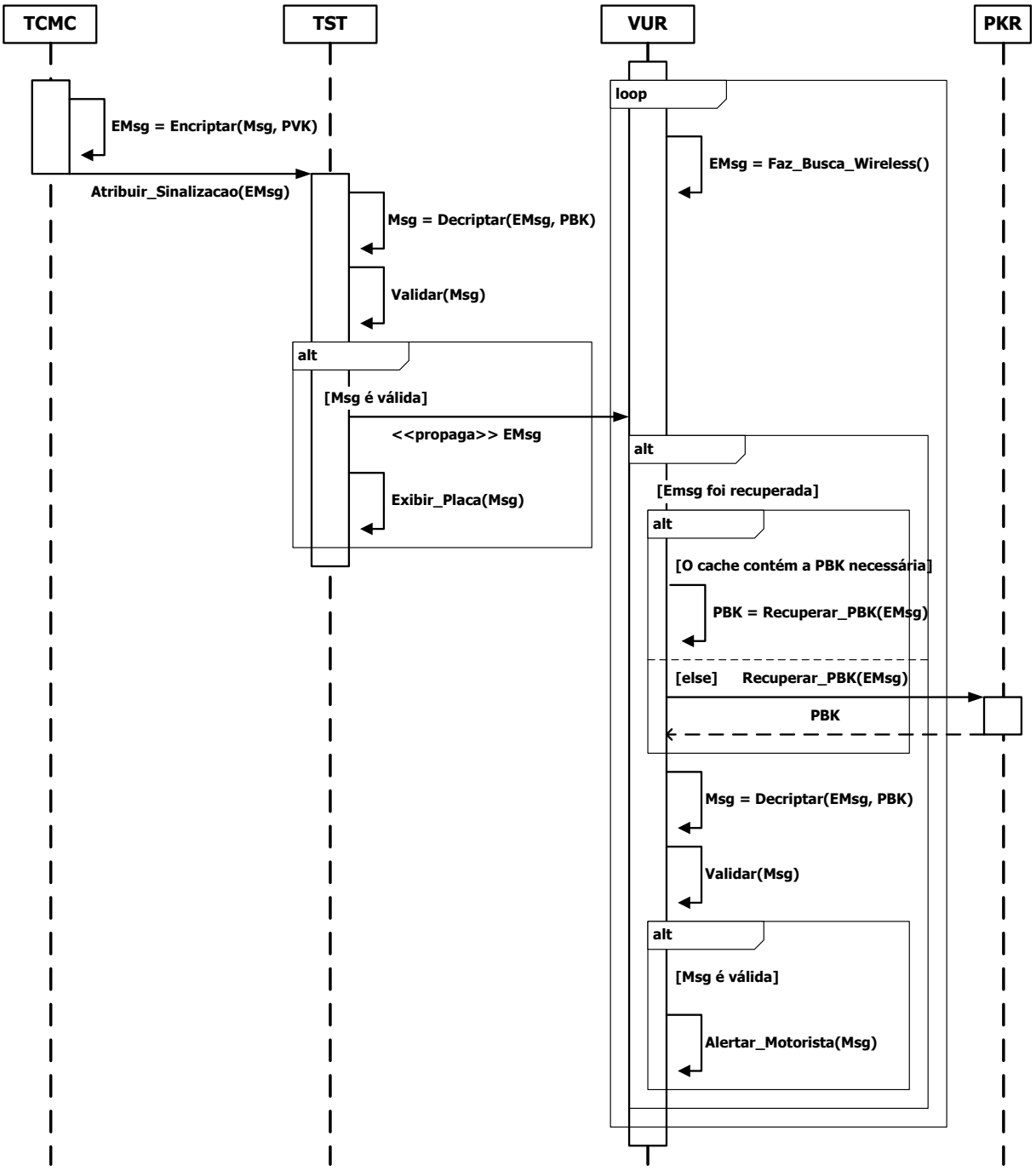

Figura 18 – Diagrama de sequência do fluxo principal de execução do TSMA.

O Capítulo 4, que segue, detalha experimentos que foram realizados para validar as hipóteses apresentadas na Seção 1.3, e, dessa forma, demonstrar o valor da proposta do TSMA nos cenários apresentados.

Capítulo 4

Experimentos e Análise dos Resultados

Conforme detalhado no capítulo anterior, o funcionamento do TSMA se dá pela comunicação entre as entidades TCMC, TST e VUR. Este capítulo é dedicado à descrição dos experimentos realizados para comprovar a viabilidade e eficiência em larga escala das formas de transmissão de dados escolhidas para comunicação entre as entidades do TSMA. Uma hipótese secundária, também testada por meio dos experimentos, foi verificar a possibilidade de implementar o TSMA utilizando componentes e tecnologias de baixo custo.

Os experimentos aqui descritos são classificados entre os dois tipos definidos a seguir:

- `Prático:` Denota um experimento que foi realizado utilizando hardware;
- `Simulado:` Denota um experimento que foi realizado em um ambiente emulado utilizando ferramentas de simulação.

Na Seção 4.1 são descritos os materiais e softwares envolvidos nos experimentos; na Seção 4.2 são detalhados o preparo e os resultados de um experimento que testa a viabilidade do método de encriptação escolhido em uma grande quantidade de mensagens; a Seção 4.3 é dedicada às informações e resultados de um experimento simulado que avalia a capacidade de envio de mensagens, a partir do TCMC, para dispositivos TST; na Seção 4.4 é apresentado um experimento que foi feito para testar a viabilidade do uso da técnica *beacon-stuffing* na comunicação entre dispositivos TST e VUR; a Seção 4.5 contém os detalhes e resultados obtidos de um experimento simulado que testa se o tempo necessário para comunicação entre dispositivos TST e VUR inviabiliza o uso da tecnologia *Wi-Fi*; na Seção 4.6 um minicomputador de baixo custo é avaliado com relação ao desempenho na decriptação de mensagens do TSMA; e, por fim, na Seção 4.8 são avaliados os resultados dos experimentos com relação às hipóteses descritas na Seção 1.3.

4.1 Equipamentos e Preparo dos Experimentos

Cada experimento foi realizado utilizando um conjunto particular de equipamentos e softwares, nesta seção são descritas as especificações das referidas ferramentas.

4.1.1 Raspberry Pi e Adaptador *Wi-Fi*

O Raspberry Pi[1] é um minicomputador de custo reduzido (U$ 35/unidade) que, apesar do preço e tamanho, é capaz de executar sistemas operacionais com as mesmas funcionalidades que máquinas tradicionais. A Figura 19 é a fotografia de um dispositivo Raspberry Pi, em sua segunda versão, cujas dimensões são 8,5 cm x 5,6 cm x 1,7 cm (altura).

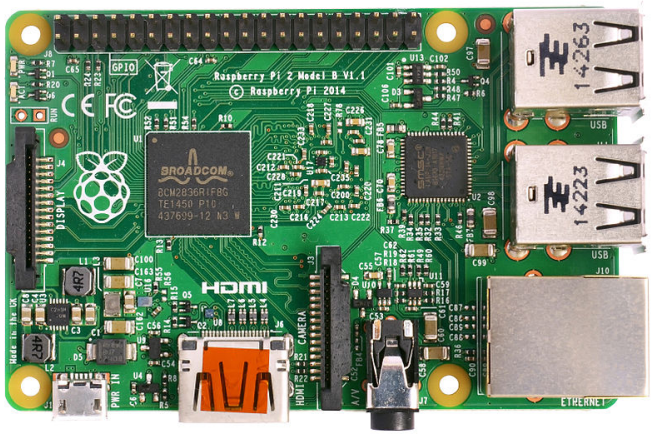

Figura 19 – Dispositivo Raspberry Pi 2.

Retirado de: "*Raspberry Pi 2 Model B v1.1*.".
Disponibilizado em: <*https* : *//commons.wikimedia.org/wiki/File* : *Raspberry_Pi_2_Model_B_v*1.1*_top_new_*(*bg_cut_out*).*jpg*>, por: Multicherry. Acesso em jan. 2016.

A versão 2 do Raspberry Pi dispõe dos seguintes recursos:

- ❏ Processador quad-core da arquitetura ARM a 900 MHz;
- ❏ 1 gigabyte de memória RAM;
- ❏ 1 interface Ethernet 10/100;
- ❏ 4 portas USB 2.0;
- ❏ Conexão HDMI.

O sistema operacional básico do Raspberry Pi é o "Raspbian", variante do Debian que foi adaptada para processadores ARM.

[1] <www.raspberrypi.org>

Para realizar testes de transmissão *Wi-Fi* com os dispositivos Raspberry Pi foi necessário adquirir separadamente adaptadores *Wi-Fi* compatíveis com os mesmos. Foi escolhido o modelo TL-WN722N, fabricado pela TP-LINK, para esta função. Este adaptador vem equipado com uma antena de 4dBi de potência e tem boa compatibilidade com o Raspbian.

Devido à vantajosa relação custo x benefício desses dispositivos, foram utilizadas unidades Raspberry Pi 2 para a prototipação do sistema e também para os seguintes experimentos:

- ❏ Seção 4.2 - Desempenho na encriptação de mensagens;
- ❏ Seção 4.4 - Transmissão de dados do TSMA utilizando o método *beacon-stuffing*;
- ❏ Seção 4.6 - Desempenho na decriptação de mensagens.

4.1.2 Ns-3 (Network Simulator 3)

O `Ns-3`[2] é uma ferramenta de simulação discreta que permite a descrição de cenários para simulação utilizando a linguagem C++. O `Ns-3` fornece módulos desenvolvidos em C++ que representam elementos típicos de redes de computadores, e tais módulos devem ser aplicados na referida descrição dos cenários.

A versão do `Ns-3` referenciada no contexto desta dissertação é a 3.23; ela foi utilizada para simular a transmissão de mensagens, a partir do TCMC, para cada um dos dispositivos TST atualizados. O seguinte experimento foi realizado por meio do `Ns-3`:

- ❏ Seção 4.3 - Desempenho no envio de mensagens de sinalização.

4.1.3 OMNet++ e SUMO

O `OMNet++`[3] é uma ferramenta para simulação que permite a descrição de cenários prevendo conexões *Wi-Fi* e mobilidade básica. Uma das limitações inerentes do `OMNet++` é não oferecer funcionalidades de mobilidade avançada nas simulações, porém essa limitação pode ser superada ao utilizar o `SUMO`[4] em conjunto com ele.

Basicamente, o `OMNet++` fornece o mecanismo de simulação e vários dos elementos de rede enquanto o `SUMO` provê funcionalidades de mobilidade avançada à simulação; o resultado dessa cooperação resulta em um excelente meio para a análise de cenários envolvendo *Wi-Fi* e veículos, que é o caso do TSMA. Essas ferramentas foram usadas para simular a interação entre dispositivos TST e VUR no seguinte experimento:

- ❏ Seção 4.5 - Comparação do *beacon-stuffing* com o padrão de associação *Wi-Fi*.

[2] <www.nsnam.org>
[3] <www.omnetpp.org>
[4] <www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883>

4.2 Desempenho na Encriptação de Mensagens (TCMC)

Durante a montagem de mensagens de sinalização do TSMA, que ocorre nos TCMCs, a etapa que potencialmente envolve o maior esforço computacional é a da encriptação parcial das mensagens utilizando o algoritmo RSA, conforme descrito na Seção 3.5.

O objetivo deste experimento foi avaliar o esforço computacional necessário para realizar essa atividade, considerando um grande número de mensagens. Embora o TCMC seja descrito como uma sede regional, dispondo de um considerável aparato computacional, este experimento tem o objetivo secundário de desmistificar a noção de que apenas máquinas potentes seriam capazes de processar as tarefas desempenhadas no TCMC. Neste sentido, os testes foram realizados em um dos dispositivos Raspberry Pi descritos na Seção 4.1.1 e, além disso, utilizando apenas um dos núcleos de seu processador. Para a encriptação dos dados foi usada a implementação do RSA contida na biblioteca `Crypto++`[5], que é de código aberto.

Para este experimento, foram preenchidos dados de 1.000 sinalizações de tamanhos variados (devido à propriedade "SIGN_DESCRIPTION") e uniformemente distribuídos. Em seguida essas sinalizações foram programaticamente enfileiradas para encriptação sequencial. Os resultados deste experimento são descritos na Seção 4.2.1.

4.2.1 Resultados

Após a execução do experimento, verificou-se um gasto de tempo médio de 0,00228 segundos (2,28ms) por mensagem encriptada, com desvio padrão de 0,00018 segundos (0,18ms). Isto equivale, proporcionalmente, a ser capaz de encriptar 1.000 mensagens em menos de três segundos, o que configura um resultado satisfatório, especialmente considerando a máquina utilizada e o uso de apenas um núcleo do processador, e reforça a ideia de que a demanda computacional para implementar o TSMA é baixa.

4.3 Desempenho no Envio de Mensagens (TCMC→TST)

Conforme descrito no Capítulo 3, após a atribuição e subsequente geração das mensagens de sinalização, tais mensagens são transmitidas, cada uma para o dispositivo TST ao qual foi atribuída. A especificação do TSMA prevê que essa transmissão seja feita interface principal de transmissão segue o padrão Ethernet, e é previsto que o TCMC estará conectado em rede com cada um dos TSTs em sua área de cobertura.

Essa transferência de mensagens entre cada TCMC e vários TSTs foi um dos focos de simulação para que fossem avaliados o desempenho e, consequentemente, a viabilidade do processo considerando uma alta quantidade de dispositivos. A Figura 20 exibe a topologia descrita para implementar a simulação.

[5] <www.cryptopp.com>

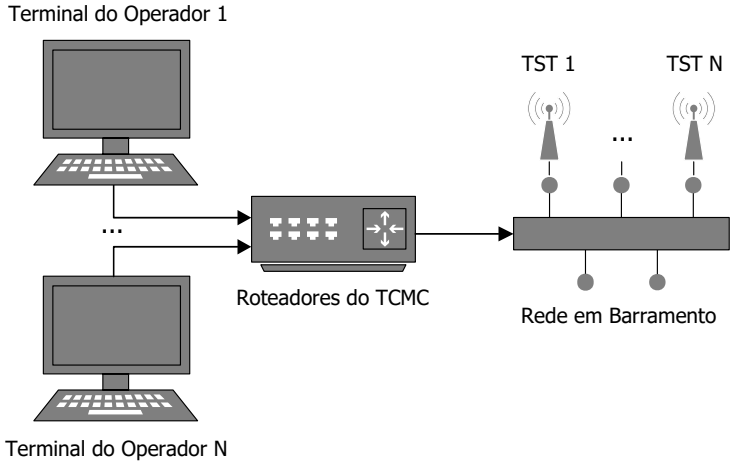

Figura 20 – Topologia de rede simulada no Ns-3.

Conforme a Figura 20, foi escolhida uma topologia de barramento para simular a forma de comunicação entre o TCMC e os dispositivos TST sob sua responsabilidade. Esta escolha é coerente com o objetivo de minimizar custos de uma possível implementação do TSMA, visto que o custo de implementar um barramento em comum é inferior ao custo de implementar ligações ponto a ponto individuais. Entretanto, nada impede que, em um cenário real de implantação, outra topologia ou forma de acesso ao canal de rede sejam utilizados de acordo com a infraestrutura preexistente e a conveniência dos responsáveis pela implantação.

O `Ns-3`, descrito na Seção 4.1.2, foi a ferramenta de simulação escolhida para este experimento. Para o cenário de execução do experimento foram definidos os seguintes parâmetros:

- **Largura do Barramento Compartilhado**: 10 Mbps;
- **Tamanho de cada Mensagem de Sinalização do TSMA**: 200 Bytes.

Foram realizadas execuções considerando que, para um TCMC teórico, haveriam:

- 1 TST;
- 10 TSTs;
- 100 TSTs;
- 1.000 TSTs;
- 10.000 TSTs.

Para cada quantidade de TSTs simulada, a frequência de envio das mensagens de sinalização também foi variada nos seguintes valores:

- 500 Hz;
- 1 kHz;
- 2 kHz.

É relevante apontar que, para simular redes com topologia de barramento, o `Ns-3` disponibiliza somente o protocolo CSMA (*Carrier Sense Multiple Access*) em sua versão original[6], em contraste com o mundo real onde o padrão Ethernet utiliza o CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). A diferença entre ambos está no fato de o CSMA/CD, ao contrário do CSMA, prover um mecanismo de detecção e tratamento de colisões entre diferentes transmissões de dados. Logo, a versão original do protocolo CSMA, utilizada neste experimento, não contempla a detecção de colisões entre pacotes, evento que pode acontecer de acordo com a frequência de envio de dados e que tem efeito negativo no desempenho da rede. O `Ns-3` é uma ferramenta de simulação discreta que, ao menos para o tipo de cenário que este experimento envolve, não lida com elementos aleatórios ou com desempenho variável dos componentes. Sendo assim, não há variabilidade nos resultados obtidos entre execuções de um mesmo cenário de simulação.

A motivação deste experimento foi testar a viabilidade do TSMA com relação a transmitir grandes quantidades de mensagens, a partir do TCMC para vários TSTs. Os resultados do experimento, e a interpretação deles, são detalhados na Seção 4.3.1.

4.3.1 Resultados

Conforme apresentado na Figura 21, o melhor desempenho obtido no envio de quantidades maiores de dados foi com a frequência de envio em 1 kHz. O péssimo desempenho obtido, em iguais condições, quando enviando mensagens de sinalização a uma frequência de 2 kHz provavelmente deve-se à colisão de dados mencionada anteriormente. Nota-se, em quantidades iguais ou superiores a 1.000 mensagens, uma proporcionalidade inversa entre o tempo de envio com taxas de 500 Hz e 1 kHz; essa proporcionalidade é explicada pelo fato de ambas as frequências de envio serem baixas o bastante para não causarem colisões. Sendo assim, para uma quantidade considerável de dados e dentro da capacidade do canal, enviar o dobro de mensagens no mesmo período de tempo (1 kHz ao invés de 500 Hz) equivale a, aproximadamente, reduzir pela metade o tempo necessário para a transferência das mensagens.

É relevante apontar que a transferência de mensagens entre o TCMC e dispositivos TST está sendo prevista e simulada como ocorrendo sob os moldes do conjunto de protocolos TCP/IP. Dessa forma, é sabido que na transmissão de qualquer mensagem, além do tamanho dela em si, ocorre também a transferência de uma certa quantidade extra de

[6] Fonte: <www.nsnam.org/docs/release/3.8/doxygen/group____csma__model.html>, Acesso: 20/01/2016

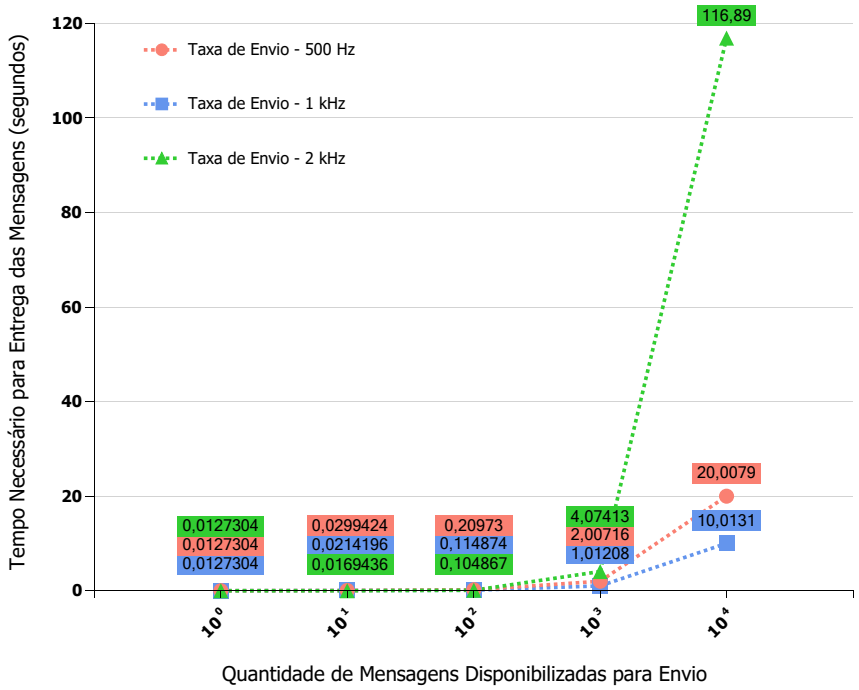

Figura 21 – Desempenho na Transmissão de Mensagens por Taxa de Envio.

dados (*overhead*) que é algo típico da comunicação TCP/IP. No caso de mensagens do TSMA, embora o tamanho de uma mensagem seja 200 bytes, no processo de sua transmissão há uma troca de 826 bytes entre o remetente e o destinatário. Essa diferença é explicada pelos seguintes fatores:

- ❏ Troca de pacotes ARP (*Address Resolution Protocol*) - 128 bytes;
- ❏ Interação SYN-ACK-FIN típica do TCP - 428 bytes;
- ❏ Cabeçalho TCP/IP que envolve a mensagem - 70 bytes.

A soma destes valores com os 200 bytes da mensagem resulta no total de 826 bytes transferidos para a transmissão de cada mensagem do TSMA. A simulação realizada no `Ns-3` contempla este fator.

De acordo com os resultados obtidos e apresentados na Figura 21, considerando a largura de banda e tamanho de mensagem especificados, seria possível o envio de 10.000 mensagens de sinalização de trânsito do TSMA em 10 segundos, o que configura um bom desempenho para a solução, especialmente vislumbrando um cenário de carga inicial de todos os dispositivos TST de uma cidade. É importante considerar que esses dados refletem a capacidade de envio de acordo com a largura do barramento, desprezando o tempo de transmissão que deve ser considerado em análises de baixo nível.

4.4 Viabilidade da Disseminação por *Beacon-stuffing* (TST→VUR)

Após o recebimento, no dispositivo TST, de uma mensagem de sinalização proveniente do TCMC, e após a validação positiva da mesma, é feita a propagação da referida mensagem para os módulos VUR de veículos que estejam nas imediações. A proposta do TSMA é de que essa propagação seja feita por meio da técnica *beacon-stuffing*, que foi detalhada na Seção 2.1.4. Foram utilizados dois minicomputadores Raspberry Pi, equipados com adaptadores *Wi-Fi*, para avaliar a viabilidade da transmissão de sinalizações de trânsito no padrão TSMA utilizando essa técnica.

Um dos Raspberry Pi foi configurado como protótipo de um dispositivo TST, ou seja, um *Access Point* (AP) emissor de *beacons* nos quais as mensagens de sinalização foram inseridas. Tendo conectado o adaptador *Wi-Fi* em uma das portas USB do protótipo, sua configuração como um AP ocorre ao executar e configurar um software livre chamado `hostapd`[7]. Para este experimento, foi emitida uma sinalização, no padrão do TSMA, que não foi encriptada. Essa propagação da mensagem sem encriptação não afetou negativamente o valor do experimento, visto que o foco dele estava em testar a viabilidade da transmissão. Caso a mensagem fosse enviada encriptada, conforme é o padrão do TSMA, seria inviável identificar visualmente os valores das propriedades da mensagem no *software* `Wireshark`[8], visto que é feita a coleta do *beacon* puro, antes que seja feita qualquer manipulação (por exemplo, a decriptação) dos dados.

Outro Raspberry Pi, também equipado com um dos adaptadores *Wi-Fi*, foi configurado como protótipo de um dispositivo VUR, cuja função é recuperar as mensagens de sinalização emitidas por dispositivos TST. Essa recuperação de mensagens, em termos práticos, ocorre ao efetuar buscas contínuas no espectro *wireless* por APs cujos *beacons* de anúncio contenham mensagens de sinalização no padrão do TSMA. Este procedimento de busca contínua se baseia no código do `iwlist`, um *software* que é parte do pacote `Wireless Tools for Linux`[9]. Esse pacote de ferramentas é de código aberto e financiado pela Hewlett-Packard (HP). O `iwlist`, basicamente, faz uma chamada de sistema ao dispositivo *Wi-Fi* indicado para recuperar a lista de *Access Point*s disponíveis (com suas informações) e faz uma formatação destes dados para exibição ao usuário. No caso deste experimento, a recuperação foi feita por meio do monitoramento das transmissões *wireless* por meio do `Wireshark` e seguem os resultados desta recuperação na Seção 4.4.1.

[7] <https://w1.fi/hostapd/>
[8] <www.wireshark.org>
[9] <www.labs.hpe.com/personal/Jean_Tourrilhes/Linux/Tools.html>

4.4.1 Resultados

A Figura 22 apresenta um *beacon frame*, estrutura típica do padrão IEEE 802.11, que foi capturado utilizando o *software* `Wireshark`, e no qual foram inseridos, por meio da técnica *beacon-stuffing*, dados de uma sinalização nos padrões do TSMA. Seguem os valores de cada uma das propriedades da mensagem de sinalização que foi inserida no *beacon*:

- ❏ VERSION (1 byte): 0x01
- ❏ BEACON_TYPE (2 bytes): 0x56AF
- ❏ COUNTRY_ID (1 byte): 0x01
- ❏ LOCATION_ID (4 bytes): 0x00305F9E
- ❏ UID (8 bytes) 0x0000000034C477C7
- ❏ TIMESTAMP (8 bytes): 0x0000000054A91D42 (1420369218 - 04/01/2015 09:00:15)
- ❏ GEO_LATITUDE (4 bytes): 0x0012A336 (40.7143528)
- ❏ GEO_LONGITUDE (4 bytes): 0x8021E093 (-74.0059731)
- ❏ TTL (4 bytes): 0x00001C20 (7200 segundos - 2 horas)
- ❏ SIGN_TYPE_ID (3 bytes): 0x005207
- ❏ RANGE (1 byte): 0x50 (80 metros)
- ❏ SIGN_DESCRIPTION (18 bytes): 0x4F76657274616B6520466F7262696464656E ("Overtake Forbidden" - Proibido Ultrapassar, caracteres em ASCII hexadecimal)

É relevante citar que embora a mensagem transmitida tenha um tamanho de 58 bytes (soma dos bytes utilizados nos campos), em caso de encriptação a mensagem passaria a ocupar 200 bytes de espaço devido ao mecanismo de enchimento descrito na Seção 3.5. Esse aumento no tamanho da mensagem não muda nenhum critério de desempenho e nem causa a segmentação da mensagem em múltiplos campos do *beacon*, visto que o campo "*Information Element*" do mesmo suporta dados de até 255 bytes, conforme detalhado na Seção 3.4.

Os valores descritos foram utilizados no experimento e representam um hipotético dispositivo TST implantado em Nova Iorque, Estados Unidos. Embora as propriedades LOCATION_ID e UID tenham sido selecionadas de forma aleatória, as coordenadas definidas por GEO_LATITUDE e GEO_LONGITUDE são coordenadas reais da referida cidade, e o valor de COUNTRY_ID é o código internacional de discagem para os Estados Unidos. O recebimento desses valores pode ser observado na Figura 22:

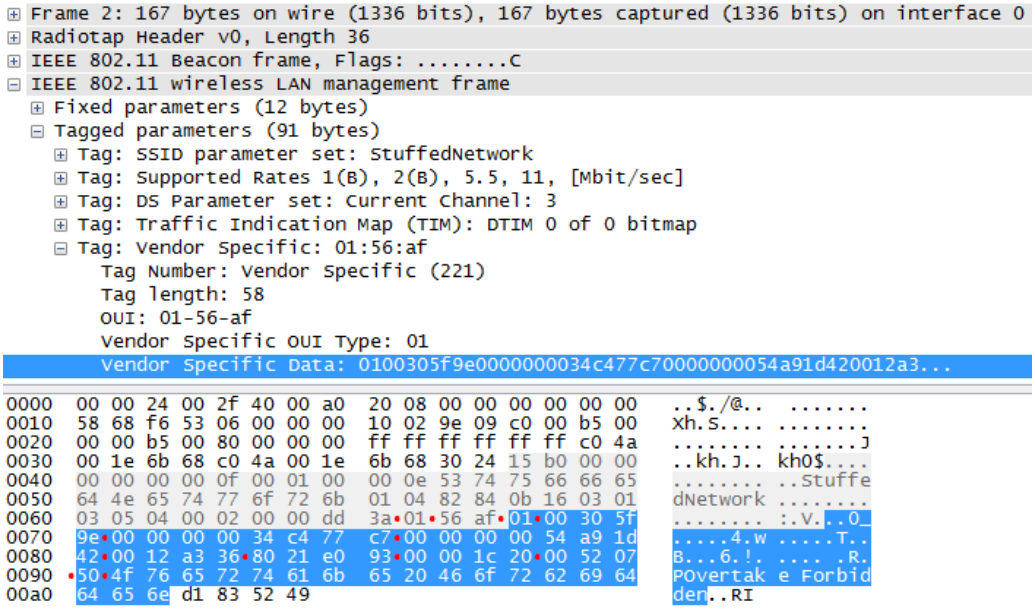

Figura 22 – *Beacon* contendo sinalização do TSMA é exibido no Wireshark.

Conforme mencionado, a Figura 22 apresenta os valores de uma mensagem de sinalização do TSMA que não passou pelo processo de encriptação. Na parte superior da imagem são exibidos os nomes das propriedades e seus valores, enquanto na parte inferior são exibidos apenas os valores em seu formato puro, sem distinção de propriedade. Fica visível na figura, especialmente na parte inferior, que a seleção de dados em azul está destacando os valores da mensagem a partir da propriedade COUNTRY_ID, e não a partir da propriedade VERSION, o que ocorre apenas por uma política de identificação do `Wireshark`. Apesar disso, os valores das propriedades VERSION (0x01) e BEACON_TYPE (0x56AF) constam, sequencialmente, logo antes da seleção em azul, bem de acordo com o posicionamento esperado. A única alteração digital feita na figura após sua coleta foi a inclusão de pontos vermelhos, marcando o início dos valores das propriedades, para facilitar a identificação dos mesmos.

Após a coleta do *beacon*, no dispositivo receptor, por meio do `Wireshark`, o experimento foi avaliado como bem-sucedido, visto que não houve qualquer corrupção dos dados. Dessa forma, considerou-se que o resultado deste experimento prova a viabilidade de utilizar a técnica *beacon-stuffing* para a propagação de mensagens a partir de dispositivos TST para dispositivos VUR no contexto do TSMA.

4.5 Deslocamento até o Recebimento (TST→VUR)

Ao instalar uma placa convencional de sinalização de trânsito é necessário garantir que ela seja visível aos condutores com uma antecedência que inclua tempo suficiente para a visualização, compreensão e reação adequada à sinalização exibida. De forma análoga este critério também tem valor no TSMA, visto que ao transmitir uma sinalização para dispositivos VUR é necessário garantir o recebimento da mesma em tempo hábil utilizando as tecnologias *Wi-Fi* disponíveis.

Conforme mencionado na Seção 2.1.4, há dois métodos de transmissão de dados que poderiam ser utilizados para realizar essa interação, o *beacon-stuffing* e o método de associação *Wi-Fi* tradicional. A ferramenta de simulação `OMNet++` foi utilizada em conjunto com o simulador de mobilidade `SUMO`, ambos descritos na Seção 4.1.3, para avaliar como seria a recepção de dados, utilizando ambos os métodos, considerando veículos em diferentes velocidades. A Figura 23 exibe a configuração do cenário de simulação para comparação das técnicas.

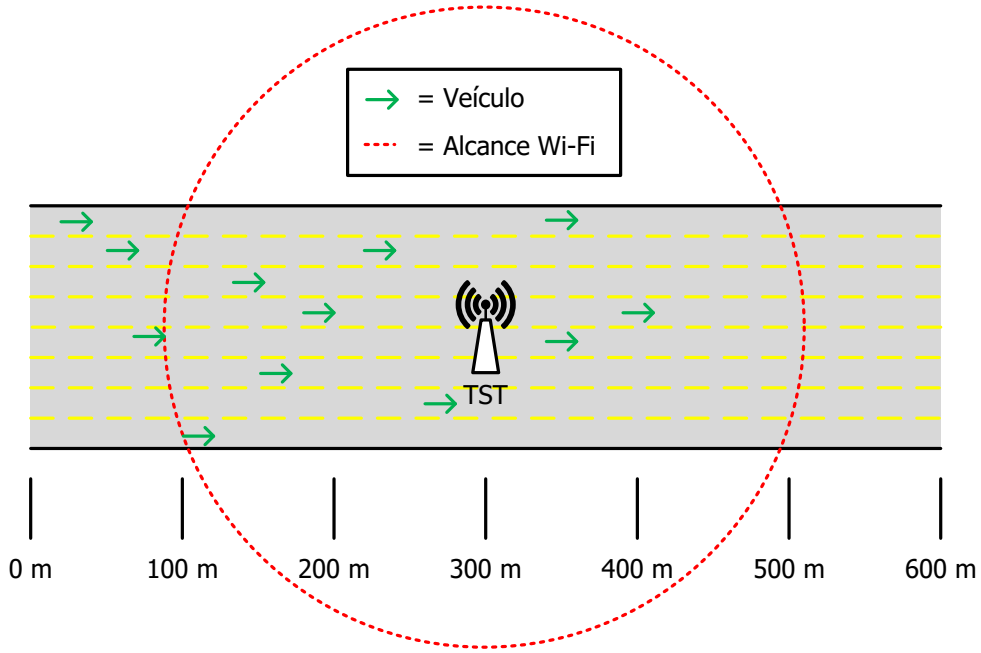

Figura 23 – Configuração para simulação do cenário de deslocamento veicular.

Conforme exibido na Figura 23, para a simulação considerou-se o cenário de uma via com 600 metros de extensão e oito pistas de mesmo sentido. No cenário considerou-se que o dispositivo TST estaria no meio da pista, uma situação irreal porém que não compromete a validade do experimento, visto que o foco do mesmo é a interação dos veículos com o TST após a entrada dos mesmos na área de alcance deste. Na verdade, o posicionamento do TST neste cenário ajuda a realizar as medições de desempenho, considerando a área de atuação de sua antena omnidirecional.

Embora a maioria da definição do cenário tenha sido feita no `OMNet++`, a emissão e movimentação dos veículos foi gerada pelo `SUMO`. Cada simulação considerou a existência e participação de 100 veículos, e cada uma delas foi executada com os veículos trafegando em velocidades de 40 km/h a 140 km/h, em incrementos de 10 km/h.

Para cada velocidade diferente, variou-se também a forma de transmissão de dados entre o dispositivo TST e os módulos VUR dentre os seguintes modos:

- ❏ ***Beacon-stuffing* - 1 Hz**: Um *beacon* emitido por segundo;
- ❏ ***Beacon-stuffing* - 3 Hz**: Três *beacons* emitidos por segundo;
- ❏ ***Beacon-stuffing* - 10 Hz**: Dez *beacons* emitidos por segundo;
- ❏ **Associação *Wi-Fi***: Modo tradicional de comunicação *Wi-Fi*.

A apresentação e análise dos resultados deste experimento constam na Seção 4.5.1.

4.5.1 Resultados

A Figura 24 apresenta os resultados do experimento, onde cada medição apresenta o valor médio e desvio padrão dos valores coletados.

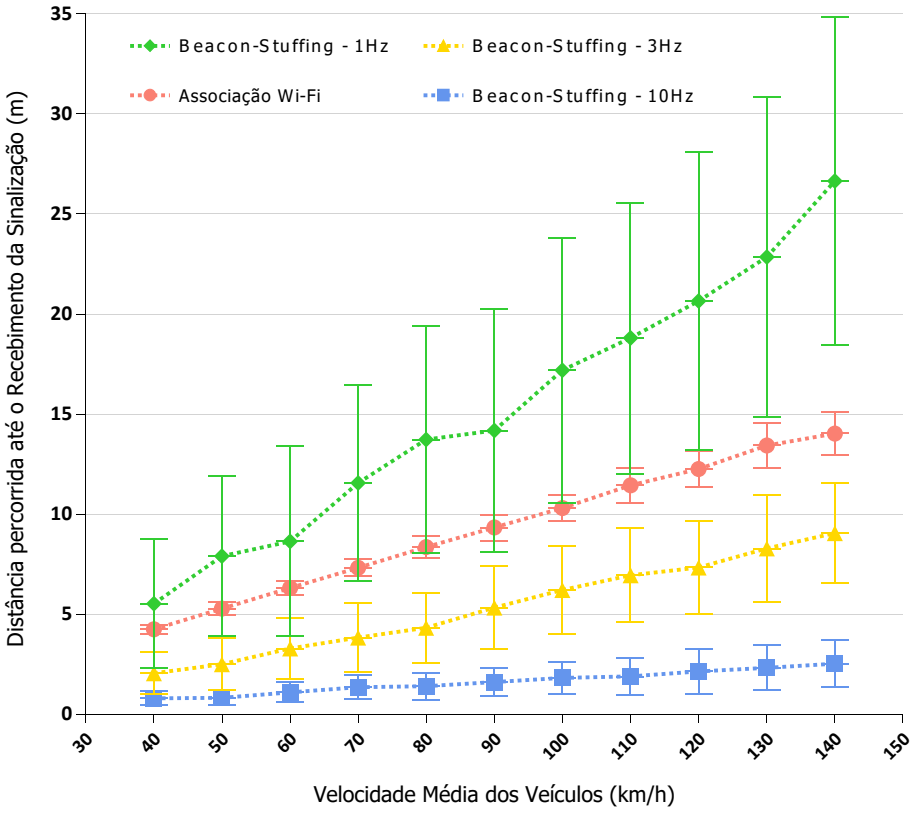

Figura 24 – Distâncias médias percorridas até o recebimento da sinalização do TSMA por veículos em velocidades diversas.

Conforme indica a Figura 24, quando utilizando o método *beacon-stuffing*, quanto maior a frequência de envio dos *beacons*, mais rapidamente ocorrerá a recepção dos dados por parte dos dispositivos VUR. É necessário considerar que, tratando-se de uma ferramenta de simulação, não são modelados aspectos complexos da comunicação *Wi-Fi* como, por exemplo, as interferência de outros dispositivos.

Para realizar uma análise de viabilidade, é importante considerar um contexto realista; logo, pensando em um cenário urbano, o foco deve ser o intervalo de velocidade até 80 km/h que contém todas as velocidades permitidas pelo artigo 61 do CTB (Código de Trânsito Brasileiro). Em todas as séries no gráfico da Figura 24 nota-se uma correlação positiva entre o valor do eixo horizontal (velocidade máxima) e o valor do eixo vertical (distância percorrida até o recebimento), ou seja, quanto maior a velocidade do veículo, maior será também a distância que ele terá percorrido, a partir da posição em que adentrou a área de cobertura de um dispositivo TST, até que seu módulo VUR recupere a mensagem de sinalização.

Entre todas as séries no gráfico da Figura 24 o maior valor de distância percorrida obtido para a velocidade de 80 km/h foi cerca de 14 metros. Este não é um valor significativo, considerando que equivale ao comprimento de pouco mais que três carros estacionados em fila e que a área de cobertura de uma antena *Wi-Fi* básica é mais que cinco vezes superior a isso (conforme a Tabela 3, apresentada na Seção 4.7). Ou seja, puramente de acordo com essa simulação, em perímetro urbano, um motorista que respeite os limites de velocidade teria tempo de reagir adequadamente à sinalização recebida em qualquer um dos quatro cenários apresentados pelo gráfico da Figura 24.

Em cenários de rodovia a velocidade máxima é de 110 km/h e, em raciocínio análogo ao apresentado para o cenário urbano, esta é a velocidade mais relevante à análise. A maior distância média percorrida pela a velocidade de 110 km/h é de aproximadamente 18 metros e, especialmente para um cenário com poucos objetos e construções que obstruem a transmissão *Wi-Fi*, este valor também é muito baixo se comparado à área de cobertura de um dispositivo TST provido de uma antena *Wi-Fi* básica, conforme detalhamento na Tabela 3.

As velocidades selecionadas para o experimento abrangem os limites de velocidade previstos no código de trânsito brasileiro com certa margem (140 km/h, limitado em 110 km/h pela legislação). Fica evidente na Figura 24 o impacto que tem a frequência de emissão dos *beacons*, por parte dos dispositivos TST, no desempenho geral da solução. É visível, por exemplo, que a abordagem do *beacon-stuffing* tem desempenho inferior à associação *Wi-Fi* tradicional quando a frequência de emissão de *beacons* adotada pelo dispositivo TST é igual ou inferior a 1 Hz, ou seja, um *beacon* emitido por segundo.

Um fator relevante à análise que o simulador não considerou no cálculo das distâncias percorridas (expresso na Figura 24) é o tempo necessário para que um dispositivo VUR faça uma busca por APs em todo o espectro *wireless*. É importante reforçar que o simu-

lador também não emula perfeitamente o impacto negativo de fatores como a velocidade dos veículos e interferências de dispositivos externos. O processo convencional de associação *Wi-Fi* envolve mais etapas de comunicação entre os dispositivos, o que gera mais pontos possíveis de falha quando afetado por algum desses fatores externos.

O resultado exibido na Figura 24 foi mantido, ignorando esses fatores negativos, conforme as medições obtidas do `OMNet++`; entretanto, na Seção 4.7, é feita uma análise mais inclusiva com relação a estes aspectos não simulados.

Ainda na comparação entre o *beacon-stuffing* e o método tradicional de associação *Wi-Fi*, é necessário considerar que cada associação *Wi-Fi* impõe um custo de recursos computacionais no *Access Point*, em questões de memória e processamento, o que limitaria a capacidade de propagação da sinalização de trânsito realizada por dispositivos TST, enquanto o uso do *beacon-stuffing* permite a comunicação com um número virtualmente ilimitado de módulos VUR. A Figura 25 exibe essa comparação e as limitações conhecidas para alguns dos adaptadores *Wi-Fi* disponíveis no mercado.

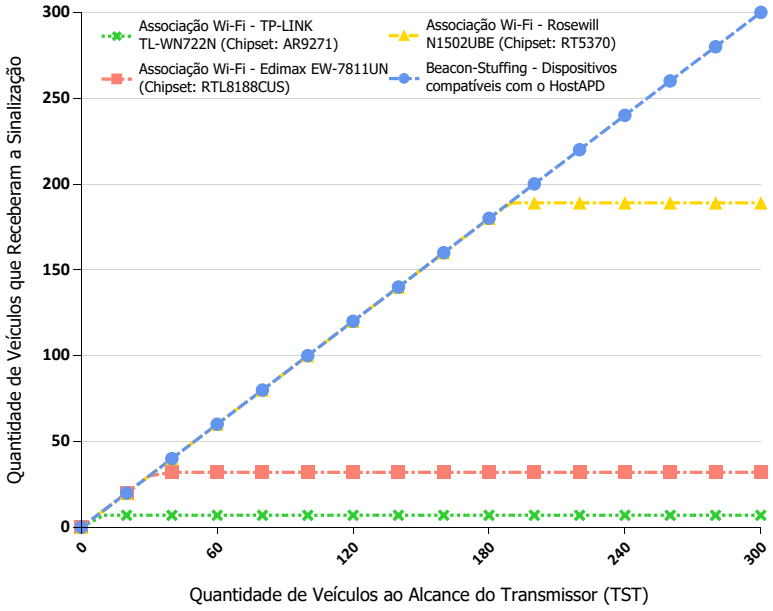

Figura 25 – Quantidade de veículos atendidos por abordagem e módulo *Wi-Fi*.

Como evidenciado na Figura 25, o método *beacon-stuffing* permite o uso de uma ampla gama de interfaces *Wi-Fi* e oferece vantagem também quando é necessário propagar a sinalização para grandes quantidades de veículos. Há melhorias que podem ser aplicadas para melhorar o desempenho da técnica *beacon-stuffing* no TSMA, entretanto é visível a superioridade da mesma, com relação ao método tradicional de associação *Wi-Fi*, para este cenário de comunicação entre dispositivos TST e VUR, especialmente com relação à quantidade de dispositivos VUR que podem ser alcançados usando hardware de baixo custo. Um comparativo mais detalhado é apresentado na Seção 4.7.

4.6 Desempenho ao Decriptar Mensagens (TST e VUR)

Cada mensagem do TSMA recebida por dispositivos TST ou VUR deve ser decriptada para a validação da mesma e recuperação das informações da sinalização de trânsito contidas nela. A motivação deste experimento foi calcular o esforço computacional necessário para decriptar uma mensagem e verificar se a natureza deste procedimento inviabiliza o uso de equipamentos de baixo custo. Assim como o experimento descrito na Seção 4.2, foram utilizados um minicomputador Raspberry Pi e a biblioteca de criptografia `Crypto++`.

Os dados preparados para a realização do experimento foram 1.000 mensagens encriptadas no padrão do TSMA, ou seja, todas com tamanho de 200 bytes. A decriptação dessas mensagens foi realizada sequencialmente, utilizando só um núcleo do processador do dispositivo, e os resultados do experimento constam na Seção 4.6.1.

4.6.1 Resultados

O tempo médio de decriptação das mensagens foi 0,0668 segundos (66,8ms) com um desvio padrão de 0,00055 segundos (0,55ms). Considerando um carro que trafega a 140 km/h, o tempo gasto na decriptação da mensagem equivale a um deslocamento de apenas 2,59 metros. De acordo com (GREEN, 2000) o tempo de reação humana, em condições ideais, para acionar a frenagem de um dado veículo, é situado entre 0,7 e 0,75 segundos. Dessa forma, é justificável considerar que um processo de decriptação realizado em menos de um décimo desse tempo é perfeitamente satisfatório. Sendo assim, tem-se mais uma evidência da viabilidade de implementar o TSMA utilizando ferramentas de baixo custo. O impacto deste fator é detalhado na Seção 4.7.

4.7 Análise Estimada da Comunicação TST→VUR

Conforme mencionado inicialmente na Seção 4.5.1, é natural que ferramentas de simulação desconsiderem algumas das variáveis envolvidas nos cenários. Na própria Seção 4.5.1, a Figura 24 apresenta um gráfico, montado a partir de dados extraídos do simulador `OMNet++`, cujos resultados desconsideram, por exemplo, o tempo necessário para realizar buscas por APs no espectro *wireless* e o tempo necessário para decriptar a mensagem de sinalização recebida. O impacto desses fatores está detalhado e estimado nesta seção.

O procedimento de busca, que não foi considerado pelo simulador, foi medido para análise nesta dissertação. Em um experimento com 1,000 repetições utilizando o hardware do protótipo (Raspberry Pi e adaptador *Wi-Fi* TL-WN722N) o tempo necessário para fazer uma busca em todo o espectro *wireless* foi, em média, 1,35 segundos com um desvio padrão de 0,00052 segundos (0,52ms).

O tempo de decriptação de mensagens do TSMA, que foi medido e detalhado na Seção 4.6, também não foi contabilizado pelo simulador. Este tempo de decriptação (avaliado em

aproximadamente 0,067 segundos) e o tempo necessário para realizar um procedimento completo de busca (avaliado em aproximadamente 1,35 segundos) foram aplicados aos resultados do experimento da Seção 4.5.1 para estimar, de forma mais realista, o deslocamento de um dado veículo desde o instante em que entra na área de cobertura da antena *Wi-Fi* de um dispositivo TST até o instante em que consegue decriptar a mensagem de sinalização recebida. O resultado dessa estimativa é expresso pela Figura 26.

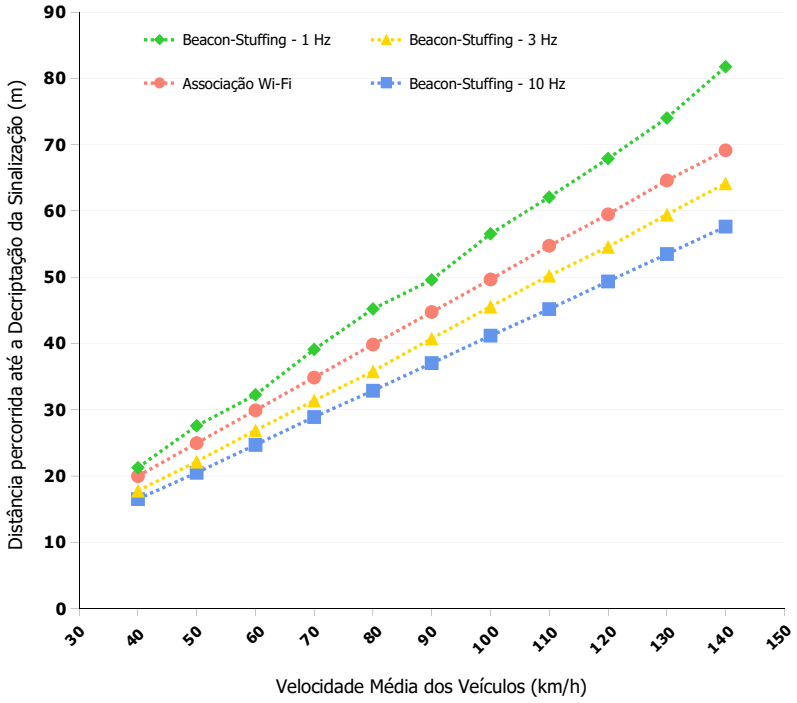

Figura 26 – Distâncias médias percorridas até a decriptação de uma sinalização do TSMA por veículos em velocidades diversas.

Cada marcação do eixo vertical (distância percorrida) no gráfico da Figura 26 foi calculada pela soma de três termos:

- Média da distância percorrida por 100 veículos simulados na velocidade definida, até o recebimento da mensagem de sinalização (conforme obtida por meio do `OMNet++` e exibida na Figura 24);
- Distância que seria percorrida por um veículo, na velocidade definida, durante o tempo de uma busca completa no espectro *wireless* (1,35 segundos);
- Distância que seria percorrida por um veículo, na velocidade definida, durante o tempo necessário para decriptar uma mensagem do TSMA, dado que a chave pública já é conhecida (0,067 segundos).

De forma equivalente à análise feita na Seção 4.5, é importante avaliar se a solução é inviabilizada pela quantidade de tempo necessária entre o instante em que o veículo

adentra a área de cobertura da antena *Wi-Fi* do dispositivo TST e o momento em que a sinalização de trânsito é exibida ao motorista pelo módulo VUR. Essa análise, baseada nos dados expressos na Figura 26, é feita considerando o método *beacon-stuffing* e 3 Hz como a frequência de emissão de *beacons* adotada pelo dispositivo TST. A Figura 27 exibe um cenário onde fica evidente o impacto deste fator.

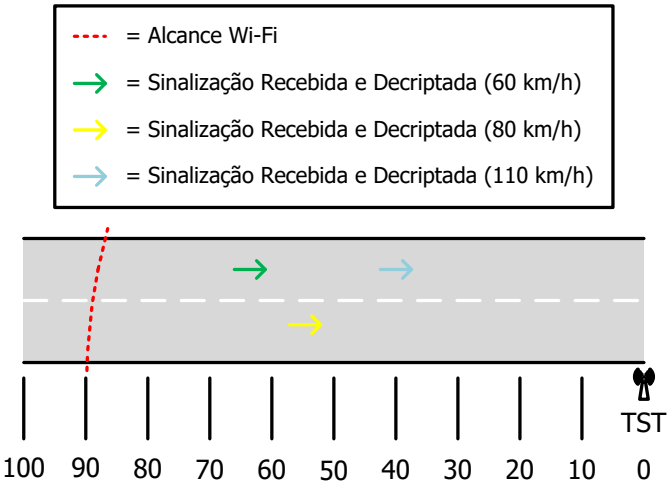

Figura 27 – Posições em que veículos exibiriam a sinalização de trânsito recuperada.

A Figura 27 apresenta um cenário no qual a antena *Wi-Fi* omnidirecional do dispositivo TST oferece cobertura a um raio de aproximadamente 90 metros. Para entender o impacto real deste atraso, é necessário ter conhecimento dos padrões de trânsito descritos no CTB. Cada uma das situações expressas pela Figura 27 serão descritas abaixo:

- **Velocidade de 60 km/h ou inferior:**
  Essas velocidades são típicas de vias urbanas nas quais há travessia de pedestres em nível e, possivelmente, semáforos. Dessa forma, é previsto que em vários momentos seja necessária a frenagem total do veículo em resposta à sinalização. Para a velocidade de 60 km/h, é calculado que a sinalização seria exibida no veículo cerca de 30 metros após adentrar a área de cobertura da antena *Wi-Fi*. Na situação descrita pela Figura 27, o motorista ainda teria 60 metros de pista para reagir à sinalização.

- **Velocidade superior a 60 km/h:**
  Nessa condição estão as vias de trânsito rápido (perímetro urbano, limite de 80 km/h) e as rodovias (via rural pavimentada, limite de 110 km/h). Em ambos os casos não há semáforos e não é recomendada a travessia de pedestres em nível. Dessa forma, seria rara, ou mesmo desnecessária, a súbita frenagem total de um veículo em tais vias. No cenário da Figura 27, para as velocidades de 80 km/h e 110 km/h, o motorista teria, respectivamente, 56 e 40 metros de pista para reagir à situação. Essas são margens de segurança pequenas, entretanto é necessário considerar que

nenhuma das sinalizações exibidas solicitaria a frenagem total do veículo e considerar também que, especialmente considerando um ambiente aberto como essas vias, é muito modesto pensar que a cobertura dos dispositivos TST seria apenas de 90 metros, argumento que é detalhado a seguir.

Embora estes 90 metros utilizados na figura tenham um bom efeito didático, a capacidade de alcance do TST, especialmente em campo aberto, promete ser bem superior, de forma que os motoristas teriam uma margem de segurança maior. A Tabela 3 apresenta resultados independentes que reforçam essa afirmação.

Tabela 3 – Alcance *Wi-Fi* de acordo com a Potência da Antena.

Adaptado de: "*Wireless Antenna Properties*". Disponibilizado em: <www.liveport.com/support-tech/wireless-antenna-properties>, Acesso em jan. 2016.

Potência da Antena	**Alcance**
0dB	200m
4dB	440m
7dB	620m
10dB	1.2km

Conforme a Tabela 3, mesmo antenas de baixa potência garantem amplas áreas de cobertura aos dispositivos TST. Além disso, é previsto que painéis *E-ink* anexos aos dispositivos TST sempre exibam a sinalização atual aos motoristas, eliminando o improvável cenário de eles serem surpreendidos por uma sinalização sem ter tempo de reação.

O procedimento de busca completa é um dos fatores que mais aumenta o tempo necessário para recebimento da sinalização de trânsito, e ele é presente tanto na abordagem do *beacon-stuffing* quanto na associação *Wi-Fi* tradicional.

4.8 Avaliação dos Resultados Frente à Hipótese

Na Seção 1.3 é detalhada a hipótese que fundamenta o TSMA e norteia sua especificação. Tal hipótese é, resumidamente, de que a comunicação entre as entidades do TSMA é viável e eficiente. E, de fato, os experimentos apresentados nas seções anteriores foram importantes para comprovar a viabilidade e bom desempenho das soluções adotadas em cada uma das etapas da transmissão de mensagens do TSMA, desde a criação delas no TCMC, até seu recebimento nos dispositivos VUR dos veículos. Em todos os experimentos foram utilizados dispositivos de baixo custo, como o referido Raspberry Pi, bem como softwares e tecnologias de uso livre sempre que aplicável. Assim sendo, considera-se que os objetivos iniciais definidos para a especificação do TSMA foram alcançados, embora ainda haja vários desafios futuros, dentre os quais alguns são citados na Seção 5.2.

Capítulo 5

Conclusão

O TSMA foi apresentado, avaliado, e comparado a trabalhos correlatos nos capítulos anteriores. Neste capítulo são detalhadas as contribuições que a proposição desta arquitetura oferece à comunidade científica e apresentadas algumas sugestões de trabalhos futuros em continuidade a esta etapa.

Um dos grandes motivadores para o desenvolvimento do TSMA foi a alta taxa de mortalidade no trânsito causada, especialmente, pela imprudência e desatenção dos condutores. De fato há uma demanda não-satisfeita por melhorias na infraestrutura de trânsito que proporcionem melhorias do tráfego e promovam uma adequação às tendências de interatividade e sistemas de transporte inteligentes (ITS). Ao estudar o sistema atual de mobilidade urbana ficou muito evidente a defasagem do modelo atual de sinalização de trânsito, modelo este que não sofreu grandes alterações desde o início do século XX.

Esta dissertação tem por foco a especificação do TSMA, uma arquitetura de gestão da sinalização de trânsito que foi proposta como uma colaboração à meta de satisfazer tal demanda. O TSMA é um modelo pelo qual as placas de sinalização podem ser alteradas remotamente por autoridades competentes e no qual a sinalização, além de ser exibida em painéis digitais externos, é apresentada aos motoristas no painel de cada veículo, como uma tentativa de reduzir o impacto da desatenção nas estatísticas de acidentes.

É relevante apontar que foram cumpridos todos os objetivos, que haviam sido listados na Seção 1.2, para o desenvolvimento deste trabalho, a saber:

- ❏ Especificação da arquitetura e seus componentes (Capítulo 3);
- ❏ Detalhamento dos mecanismos de segurança adotados no TSMA (Seção 3.5);
- ❏ Apresentação de experimentos que validaram as etapas críticas (Capítulo 4).

A Seção 5.1 é dedicada à apresentação das contribuições do trabalho.

A Seção 5.2 traz um detalhamento das limitações atuais do TSMA e possíveis soluções que podem ser investigadas futuramente, bem como melhorias pendentes.

A Seção 5.3 lista as publicações que são consequências diretas deste trabalho.

5.1 Principais Contribuições

Um dos focos deste trabalho é demonstrar o viés inovador do TSMA, que é expresso em diversos fatores como, por exemplo, o uso da técnica *beacon-stuffing* (descrita na Seção 2.1.4) em um contexto de V2I e a escolha, sempre que possível e aplicável, de tecnologias de baixo custo para aumentar a viabilidade da arquitetura.

Outros modelos e tecnologias já foram descritos, por autores diversos, com objetivos parecidos ao do TSMA, entre eles temos a tecnologia VMS (Seção 2.2.1), o modelo (SATO; MAKANAE, 2006) (Seção 2.2.3), a solução (FERNANDES, 2009) (Seção 2.2.5), entre outros. Uma comparação feita na Seção 2.3 entre o TSMA e esses padrões citados apontou que o TSMA é o único que oferece simultaneamente os seguintes recursos:

- ❏ Exibição da sinalização em tela externa ao veículo;
- ❏ Exibição da sinalização no painel do veículo;
- ❏ Possibilidade de atualização remota da sinalização.

Dessa forma, é natural considerar que a proposição do TSMA, especialmente como um modelo não-patenteado, constitui uma contribuição inovadora. Todos os componentes e entidades do TSMA foram detalhados, no caso: o TCMC (Seção 3.1), o TST (Seção 3.2) e o VUR (Seção 3.3). A descrição desses elementos, bem como do formato de mensagem que é transmitida entre eles (Seção 3.4), foi feita com referencial gráfico e detalhamento de cada um dos módulos, de suas funções e das interações entre eles.

Além dos componentes citados, é relevante mencionar que a especificação do TSMA envolve aspectos de segurança (Seção 3.5), um tópico fundamental quando se precisa garantir a integridade (dados inalterados de ponta a ponta) e autenticidade (dados provém da origem especificada) das mensagens recebidas por um dado elemento do TSMA. A importância desses tópicos de segurança deve-se à alta necessidade de confiabilidade em sistemas de trânsito no geral, visto que um ataque bem-sucedido a um sistema crítico como o TSMA, dependendo de seu tipo e escopo, teria alto potencial de causar acidentes graves.

Embora toda a especificação da arquitetura esteja permeada com conceitos de segurança, esse foco é muito evidente na descrição da mensagem de sinalização. Um mecanismo de criptografia assimétrica é usado para evitar que um atacante mal-intencionado consiga criar ou modificar mensagens que seriam aceitas como válidas pelos outros elementos da arquitetura. Neste âmbito, foi necessário rever a literatura de criptografia existente e, por fim, foi adotado o uso do algoritmo RSA, com chaves de 1536 bits.

A mensagem de sinalização é transmitida entre o TCMC e um dado dispositivo TST, e propagada, a partir do dispositivo TST, para todos os módulos VUR nas proximidades. Houve o cuidado de definir uma mensagem que fosse leve para a transmissão e cuja transmissão por meio do método *beacon-stuffing* não causasse segmentação do pacote.

Sendo assim, o resultado foi uma mensagem de sinalização relativamente leve, com 200 bytes de tamanho quando encriptada.

Há fortes indícios de que a especificação feita do TSMA cumpriu os objetivos previamente estipulados. Os resultados dos experimentos realizados (Capítulo 4) confirmam o valor, ou no mínimo o potencial, do TSMA como uma solução de relativo baixo custo e com bom desempenho em larga escala. O código-fonte dos protótipos utilizados nos experimentos foi disponibilizado e está acessível publicamente por meio do GitHub em: <https://github.com/evertonrlira/TSMA>.

5.2 Trabalhos Futuros

Apesar de todos os experimentos indicarem que o TSMA é uma arquitetura viável e com boa escalabilidade, sempre é bem-vinda a melhoria de pontos críticos. Dessa forma, alguns aspectos abertos a melhorias são expostos nesta seção.

Uma das limitações atuais do TSMA é que a recepção das sinalizações de trânsito nos veículos está sendo atrasada devido ao custoso, porém atualmente inevitável, procedimento de busca *Wi-Fi* completa. Embora seja possível definir e padronizar o canal de frequências utilizado pelos dispositivos TST, atualmente não é conhecida alguma forma de limitar o esforço de busca *wireless* dos dispositivos VUR a apenas uma faixa de frequência.

Uma das propostas para resolver essa limitação é tentar aprimorar o `iwlist`, ferramenta de código aberto mencionada na Seção 4.4, para implementar buscas *Wi-Fi* em frequências específicas, algo que potencialmente seria bem menos custoso que realizar a busca completa. Outra proposta é permitir que os dispositivos VUR aceitem mensagens de sinalização de TSTs que ainda estejam a distancias maiores que o previsto na especificação da área de atuação ("RANGE") da sinalização. Neste caso, a sinalização ficaria armazenada temporariamente e só seria exibida ao motorista quando o veículo adentrasse a área de atuação da mesma.

Embora a tecnologia IEEE 802.11n seja utilizada com relativo sucesso na transmissão de dados entre o dispositivo TST e os módulos VUR nas proximidades, a tecnologia WAVE tem um potencial muito claro para este tipo de situação e, quando os dispositivos compatíveis com a tecnologia WAVE forem mais acessíveis, seria muito positivo testar os benefícios que ela oferece.

A estrutura atual proposta para os TCMCs é que todos tenham o mesmo funcionamento e importância, sendo a área total de manutenção dividida entre áreas menores de acordo com a demanda e capacidade de gestão de cada TCMC. Uma das propostas de mudança nesse paradigma sugere a existência de uma hierarquia entre os TCMCs, de forma que um TCMC de 1^o nível seja responsável apenas pela gestão lógica da política de atualização das sinalizações e atendimento ao contato externo, enquanto TCMCs de 2^o nível seriam responsáveis por dar manutenção aos equipamentos e implementar a atu-

alização da sinalizações conforme os pedidos do TCMC de 1º nível. Este modelo poderia ser aplicado a nível de grandes cidades.

Um assunto passível de investigação é a possibilidade de haver outras formas de alteração da sinalização dos dispositivos TST além da atualização prevista por cabeamento, algumas das propostas são a atualização por meio de veículo especialmente equipado ou de equipamentos portáteis que estariam sob responsabilidade dos fornecedores de serviços essenciais. Ambas as alterações requerem mudanças no hardware dos dispositivos TST e têm grandes implicações no tópico de segurança, sendo assim, tal análise está em estágios bem preliminares.

Outro assunto que pode ser investigado é "como minimizar a chance de um TST, que perdeu temporariamente sua conexão com o TCMC, deixar de exibir sinalizações até o reestabelecimento da conexão". Pesquisar formas e impactos de transferir conjuntos de sinalizações do TCMC a cada TST, ao invés de sinalizações únicas, pode ser promissor no aspecto de confiabilidade da arquitetura.

Novamente é importante reiterar que o TSMA apresentou bons resultados nos experimentos apresentados no Capítulo 4 e não foi descoberto qualquer impedimento à viabilidade da solução em larga escala. Assim sendo, esta seção de "Trabalhos Futuros" foi dedicada apenas a propostas de melhoria que serão analisadas em momento oportuno.

5.3 Contribuições em Produção Bibliográfica

As principais contribuições bibliográficas do trabalho são:

- Everton Lira, Enrique Fynn, Paulo R. S. L. Coelho, Luis F. Faina, Lásaro J. Camargos, Rodolfo S. Villaça e Rafael Pasquini. "*An Architecture for Traffic Sign Management in Smart Cities*". Aceito para publicação no 30º *IEEE International Conference on Advanced Information Networking and Applications* (AINA 2016), 23 a 23 de Março de 2016, Crans-Montana - Suiça. QUALIS A2.

- Everton Lira, Paulo R. S. L. Coelho, Luis F. Faina, Lásaro J. Camargos, Rodolfo S. Villaça e Rafael Pasquini. "Versão Estendida de *An Architecture for Traffic Sign Management in Smart Cities*". Atualmente em elaboração, com o objetivo de ser submetido a uma das chamadas de edições especiais associadas ao AINA 2016.

Referências

BALDESSARI, R. et al. Car-2-car communication consortium manifesto: Overview of the c2c-cc system, version 1.1. **Inst. Commun. Navig., Braunschweig, Germany, Tech. Rep. C2C-CC Manifesto**, 2007.

BANERJEE, N. et al. Virtual compass: relative positioning to sense mobile social interactions. In: **Pervasive computing**. [S.l.]: Springer, 2010. p. 1–21.

BARBA, C. T. et al. Smart city for vanets using warning messages, traffic statistics and intelligent traffic lights. In: IEEE. **Intelligent Vehicles Symposium (IV), 2012 IEEE**. [S.l.], 2012. p. 902–907.

BEKIARIS, E.; WIETHOFF, M.; GAITANIDOU, E. **Infrastructure and Safety in a Collaborative World**. [S.l.]: Springer, 2011.

BEYLOT, A.-L.; LABIOD, H. **Vehicular Networks: Models and Algorithms**. [S.l.]: John Wiley & Sons, 2013. 47–48 p.

CHANDRA, R. et al. Beacon-stuffing: Wi-fi without associations. In: IEEE. **Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop on**. [S.l.], 2007. p. 53–57.

DIRECTIVE, E. Council directive 2010/40/eu of 7 july 2010 on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport text with eea relevance. **Official Journal of the European Communities**, p. 1–13, 2010.

DOWNS, A. Why traffic congestion is here to stay.... and will get worse. **ACCESS Magazine**, v. 1, n. 25, 2004.

FERNANDES, R. J. **VANET-Enabled In-Vehicle Traffic Signs**. Dissertação (Mestrado) — University of Porto, Portugal, 2009.

GIRÓN, M. A. L. et al. Gossipmule: scanning and disseminating information between stations in cooperative wlans. In: ACM. **Proceedings of the third ACM international workshop on Mobile Opportunistic Networks**. [S.l.], 2012. p. 87–88.

GRACA, J. L. Driving and aging. **Clinics in Geriatric Medicine**, v. 2, n. 3, p. 577–589, 1986.

GREEN, M. "how long does it take to stop?"methodological analysis of driver perception-brake times. **Transportation human factors**, Taylor & Francis, v. 2, n. 3, p. 195–216, 2000.

GUPTA, V.; ROHIL, M. Information embedding in ieee 802.11 beacon frame. In: **National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC**. [S.l.: s.n.], 2012.

HENDRICKS, D.; FELL, J.; FREEDMAN, M. **The relative frequency of unsafe driving acts in serious traffic crashes**. [S.l.]: National Highway Traffic Safety Administration Washington, DC, 2001.

KLAUER, S. G. et al. **The impact of driver inattention on near-crash/crash risk: An analysis using the 100-car naturalistic driving study data**. [S.l.], 2006.

KÖNINGS, B.; SCHAUB, F.; WEBER, M. Prifi beacons: piggybacking privacy implications on wifi beacons. In: ACM. **Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication**. [S.l.], 2013. p. 83–86.

LENSTRA, A. K. Key lengths. **Handbook of Information Security**, Wiley, v. 2, p. 617–635, 2004.

MALFETTI, J. L. 55+ drivers: Needs and problems of older drivers: Survey results and recommendations. proceedings of the older driver colloquium (orlando, florida, february 4-7, 1985). ERIC, 1985.

OPIELA, K. S.; ANDERSEN, C. K. **Maintaining traffic sign retroreflectivity: Impacts on state and local agencies**. [S.l.]: Turner-Fairbank Highway Research Center, 2007.

PETERMAN, D. R. **Ensuring That Traffic Signs Are Visible at Night: Federal Regulations**. [S.l.], 2013.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, ACM, v. 21, n. 2, p. 120–126, 1978.

SATO, Y.; MAKANAE, K. Development and evaluation of in-vehicle signing system utilizing rfid tags as digital traffic signs. **International Journal of ITS Research**, v. 4, n. 1, 2006.

SIVAK, M. Mortality from road crashes in 193 countries: a comparison with other leading causes of death. University of Michigan, Ann Arbor, Transportation Research Institute, 2014.

WEIGLE, M. Standards: Wave/dsrc/802.11 p. **Vehicular Networks CS**, v. 795, p. 895, 2008.

WEIS, S. A. Rfid (radio frequency identification): Principles and applications. **System**, v. 2, 2007.

ZHANG, T.; DELGROSSI, L. **Vehicle safety communications: protocols, security, and privacy**. [S.l.]: John Wiley & Sons, 2012. v. 103.