Companhia de Engenharia de Tráfego

Nota Técnica 288

Edmilson Henrique Valle

Luiz Alonso Lopes Romero

DESENVOLVIMENTO DE COMUNICAÇÃO SEM FIO PARA CONTROLADORES SEMAFÓRICOS

Janeiro/2025

Sumário

Lista de Figuras

1. OBJETIVO

O presente trabalho descreve o desenvolvimento de uma solução para acesso remoto aos controladores semafóricos da cidade de São Paulo, que tiveram os gabinetes alteados (instalados em altura acima do padrão convencional) para coibir ações de vandalismo e furto. Essa solução consistiu no emprego de um roteador WiFi, que permitiu o estabelecimento da comunicação sem fio entre a interface de comunicação (software instalado em um Notebook) e os controladores semafóricos alteados.

2. INTRODUÇÃO

Devido ao aumento das ocorrências de vandalismos e furtos de controladores semafóricos fez-se necessário adotar medidas para mitigação do problema. Uma das medidas adotadas foi o alteamento dos gabinetes dos controladores, ou seja, a sua instalação em uma posição mais alta, que dificulta o acesso e eventual manuseio do equipamento por pessoa não autorizada. Contudo, essa solução acabou dificultando também o acesso das equipes próprias e credenciadas pela CET que realizam os serviços de manutenção e de operação nos equipamentos. O acesso aos controladores pelas equipes técnicas é necessário e costuma ocorrer com regularidade, nas ações de conferência, alterações da programação e monitoramento dos equipamentos realizadas. Para o atendimento desta demanda, o laboratório do Departamento de Equipamentos e Redes – DER, da Gerência de Infraestrutura e Gestão - GIG foi acionado e desenvolveu uma solução, que viabilizou o acesso remoto à CPU dos controladores a partir de um notebook de posse dos técnicos autorizados.

3. HISTÓRICO

Ocorrências de furto e vandalismo em controladores semafóricos não são uma novidade. Como parte integrante do mobiliário urbano, controladores semafóricos e demais sinalizações de trânsito estão instalados no espaço público, mais especificamente em seu viário. A forma usual de instalação destes equipamentos que, por um lado, permitia o acesso dos técnicos autorizados durante os serviços de manutenção, acabou, por outro lado, por facilitar o acesso de pessoas mal-intencionadas, dando margem aos furtos e ações de vandalismo e dificultando sua proteção.

Cabe ressaltar que, sendo um problema recorrente para as políticas públicas, o furto e o vandalismo do patrimônio público são tratados como crimes, tendo sua previsão no código penal. Em seu artigo 163, parágrafo único, inciso III, sobre danos à coisa alheia, tem-se que o dano é qualificado se cometido "contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos". Já no artigo 180, parágrafo sexto, que trata da receptação, tem-se que "Tratando-se de bens do patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos, aplica-se em dobro a pena prevista no caput deste artigo" [1].

Um levantamento feito pela Companhia de Engenharia de Tráfego (CET) sobre as ocorrências de furtos e vandalismo, ocorrido no sistema semafórico da cidade de São Paulo mostrou que: de janeiro a dezembro de 2022, foram registradas 6.035 ocorrências deste tipo de crime. Esse número representa, em média, 17 semáforos danificados por dia. O que representou um aumento de 20% em relação ao ano de 2021, quando haviam sido contabilizadas 5.237 ocorrências.

Este levantamento também apurou o seguinte:

a) Durante o ano de 2020, a CET registrou 4.554 ocorrências similares [2].

b) No ano de 2019 o registro de 1.969 ocorrências de furto e vandalismo de componentes semafóricos na cidade, distribuídas entre equipamentos eletrônicos e 176 quilômetros de cabos elétricos.

c) Em 2018, foram 1.911 ocorrências de furto e vandalismo, incluindo 90 quilômetros de cabos elétricos e componentes eletrônicos [3].

d) E, em 2017, registrou-se 761 ocorrências, sendo 577 referentes a cabos [4].

Estes dados explicitam a evolução do número de delitos na cidade de São Paulo e podem ser vistos na Tabela 1, a seguir, e no respectivo Gráfico 1, adiante.

[1] Fonte: Presidência da República Casa Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (acessado em 07/02/2024).

[2] Fonte: Companhia de Engenharia de Tráfego - CETSP. Disponível em: http://www.cetsp.com.br/noticias/2023/01/11/sao-paulo-soma-mais-de-6-mil-casos-de-furto-e-vandalismo-a-semaforos-em-2022.aspx (acessado em 07/02/2024).

[3] Fonte: Prefeitura de São Paulo. Disponível em: https://www.capital.sp.gov.br/noticia/entre-janeiro-e-novembro-cidade-registrou-4-243-ocorrencias-de-furto-e-vandalismo-de-semaforos (acessado em 07/02/24).

[4] Fonte: Jornal Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/07/casos-de-vandalismo-em-semaforos-de-sao-paulo-este-ano-ja-supera-2017.shtml (acessado em 07/02/2024).

Tabela 1: Evolução das ocorrências de furtos de equipamentos semafóricos na cidade.

Ano	Número de ocorrências
2017	761
2018	1.911
2019	1.969
2020	4.554
2021	5.237
2022	6.035

Gráfico 1: Evolução das ocorrências de furtos de equipamentos semafóricos na cidade

Esse crescimento acentuado e constante nos furtos de equipamento de sinalização semafórica, de 761 em 2017 para mais de 6 mil em 2022 (em apenas 5 anos), vai ao encontro do relato da concessionária de energia elétrica da Região Metropolitana de São Paulo que afirmou em audiência à CPI do Furto de Fios e Cabos na Câmara de Vereadores de São Paulo que a Grande São Paulo "teve um aumento exponencial superior a 1000% no número de ocorrências entre o período de 2018 e 2022" [5].

[5] Fonte: Câmara Municipal de São Paulo. Disponível em: https://www.saopaulo.sp.leg.br/blog/furto-de-fios-na-grande-sp-foi-superior-a-1000-nos-ultimos-5-anos-diz-enel-em-cpi/ (acessado em 07/02/2024).

4. DESCRIÇÃO DA PESQUISA E DESENVOLVIMENTO

Logo de início, quando foi exposto o problema, optou-se por utilizar a tecnologia de comunicação sem fio "WiFi". A disponibilidade de adaptadores de rede WiFi pré-instalados nos Notebooks em uso pela área operacional da CET, pesou favoravelmente na escolha desta tecnologia de comunicação sem fio, em detrimento de outras tecnologias possíveis. Adicionalmente, considerou-se que a tecnologia WiFi facilitaria a transmissão entre a interface de comunicação (computador/programador) e a CPU do controlador, uma vez que os controladores da marca GW, selecionados para etapa 1 dos testes, possuem originalmente uma comunicação Ethernet entre o controlador e o software de programação, via endereçamento IP.

Na escolha desta tecnologia considerou-se ainda o fato de o roteador WiFi/Ethernet ser um produto de mercado e de baixo custo. Em decorrência destes fatores, decidiu-se que, para as etapas seguintes, com controladores dos demais fabricantes, seria mantida a tecnologia WiFi, desenvolvendo-se desta forma uma solução única para a comunicação sem fio com todos os modelos de controladores de fabricantes em uso pela CET.

Dois fatores foram determinantes para o início do desenvolvimento de uma solução individualizada para cada marca de controlador. Primeiro, a interface de programação, um software proprietário instalado no Notebook, que é diferente, a depender do fabricante. Segundo, os tipos de conexão controlador/computador são diferentes, variando também conforme o fabricante. Como exemplos de conexões existentes temos: Ethernet com conector RJ-45 (utilizado pela GreenWave no controlador GWBR), porta Serial RS-232 com conector DB-9 (no controlador DP40A da Dataprom) e porta USB 2.0 tipo B (no CD-300 da fabricante Digicon).

Um dos itens mais importantes considerados nessa pesquisa foi a utilização de um produto de mercado com alta confiabilidade e segurança que pudesse, acima de tudo, ser integrado à nossa aplicação específica.

As soluções foram desenvolvidas no laboratório da GIG/DER em três etapas:

a) Primeira etapa: utilização de um roteador WiFi/Ethernet TP-Link modelo TL-MR-3020 para os controladores GW.

b) Segunda etapa: utilização de um conversor WiFi/RS-232 fabricado pela Hi-Flying Technology modelo HF2211 para os controladores DP40A.

c) Terceira etapa: desenvolvimento da solução de acesso remoto para os controladores CD300, utilizando-se o mesmo equipamento utilizado na segunda etapa. Foi necessário, porém, realizar uma adaptação técnica, pois o controlador CD300 possui conexões USB 2.0 tipo B na CPU e também no Painel de Facilidades. Como o roteador HF2211 utiliza conexão RS-232, foi necessário desligar o Flat Cable do Painel de Facilidades, conectar os pinos referentes à comunicação RS-232 a um conector DB-9 e então ligá-lo ao roteador WiFi/RS-232.

Importante notar que o equipamento modelo HF2211, incorporado na segunda e terceira etapas do estudo, possibilitou também a comunicação com os controladores GW (usados na primeira etapa), uma vez que além ser um conversor WiFi/RS-232, ele possui ainda a função de roteador WiFi/Ethernet.

O total de tempo utilizado no processo de Pesquisa e Desenvolvimento foi de 2 anos e 9 meses, dividido em três etapas. O período de Pesquisa e Desenvolvimento foi de 06 de Junho de 2020 (início da Pesquisa) até 26 de Fevereiro de 2021 para o roteador MR-3020, sendo que nesta data foi feita a configuração dos primeiros 19 Módulos dos 30 que foram instalados em Campo, sendo esta a Etapa 1. Em 19 de Fevereiro de 2021 iniciamos a pesquisa da solução HF2211 para o controlador DP40A, onde foi feito o primeiro contato com a empresa FlexMedia. Conseguimos finalizar o desenvolvimento desta etapa 2 em 20 de Dezembro de 2022 para os controladores GW e DP40A. Começamos a desenvolver a solução para o controlador CD300 em Janeiro de 2023 e concluímos todo o processo de Desenvolvimento em 03 de Março de 2023, finalizando a Etapa 3.

4.1. EQUIPAMENTOS UTILIZADOS NA ETAPA 1

A seguir são listados os equipamentos utilizados nos procedimentos dos testes de comunicação da primeira etapa, os quais podem ser vistos adiante:

a) Roteador WiFi/Ethernet do fabricante TP-Link modelo TL-MR-3020 (Figura 1);

b) Controlador GreenWave GWBR Tempo Real de 24 grupos semafóricos (Figura 2);

c) Controlador GreenWave GWBRH Tempo Fixo de 16 grupos semafóricos (Figura 3); e

d) Controlador GreenWave GW3 Tempo Fixo de 8 grupos semafóricos (Figura 4)

Figura 1 – Roteador TP-Link TL-MR-3020

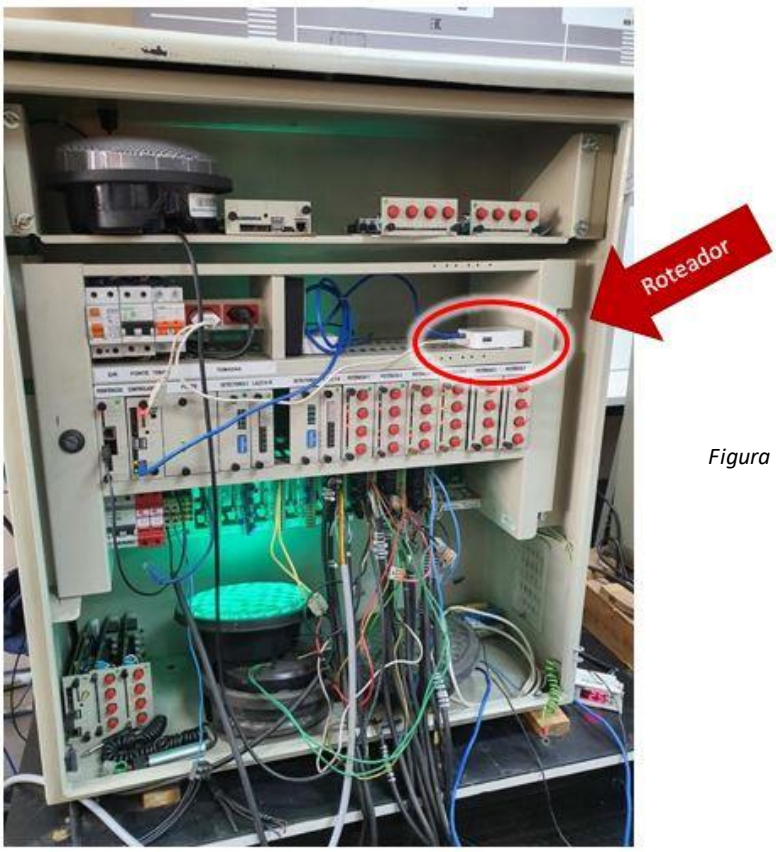

Figura 2 – Controlador GreenWave GWBR

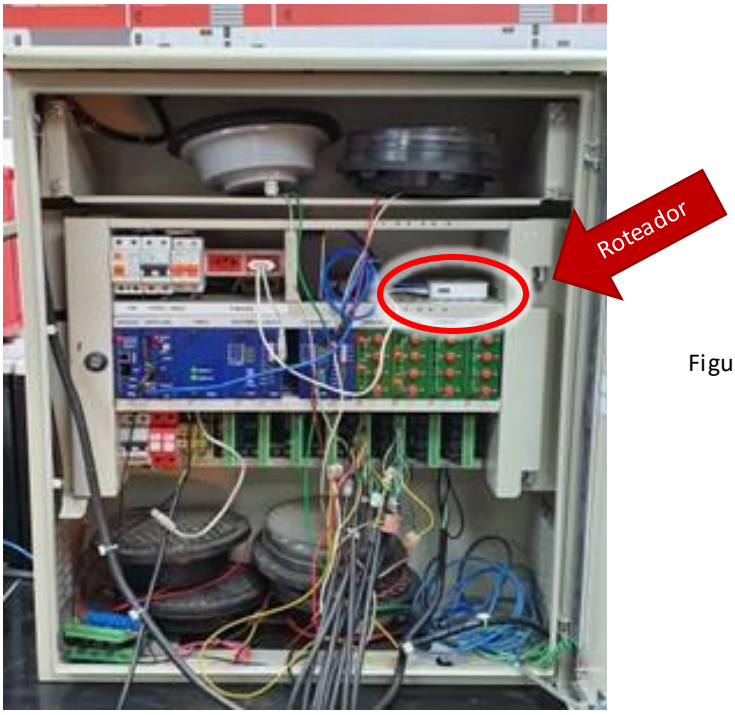

Figura 3 – Controlador GreenWave GWBRH

Figura 4 – Controlador GreenWave GW3

4.2 EQUIPAMENTOS UTILIZADOS NA ETAPA 2

Os equipamentos utilizados nos procedimentos dos testes de comunicação da 2ª etapa foram:

a) Controlador Dataprom DP40A de 16 grupos semafóricos (Figuras 5 e 6, abaixo); e

b) Roteador WiFi/RS-232/Ethernet do fabricante Hi-Flying Technology modelo HF2211 (Figuras 6 e 7, abaixo).

Figura 5 – Controlador Dataprom - DP40A

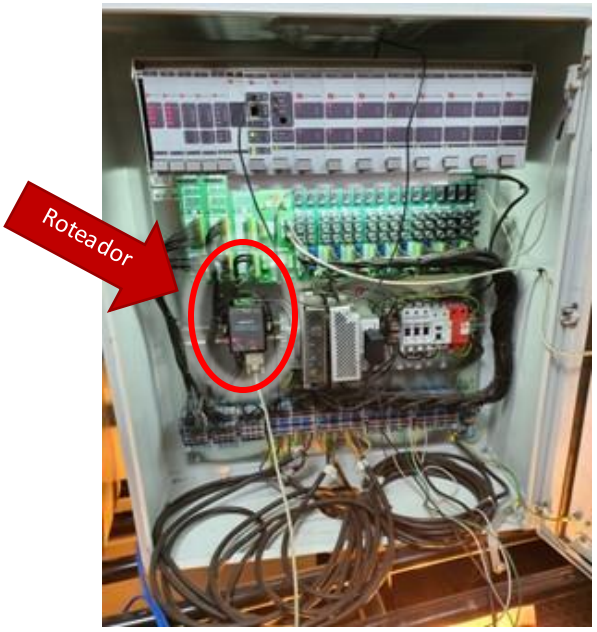

Figura 6 – DP40A com Roteador WiFi/RS-232 - HF2211

Figura 7 – Detalhe Roteador WiFi/RS-232 - HF2211

4.3 EQUIPAMENTOS UTILIZADOS NA ETAPA 3

Para os procedimentos dos testes de comunicação da 3ª etapa foram utilizados:

a) Controlador Digicon CD300 de 16 grupos semafóricos (Figura 8 abaixo); e

b) Roteador WiFi/RS-232/Ethernet do fabricante Hi-Flying Technology modelo HF2211 (Figura 9, abaixo).

Figura 8 – Controlador Digicon - CD300

Figura 9 – Roteador WiFi/RS-232 - HF2211

4.4 TESTES REALIZADOS

4.4.1 TESTES DE LABORATÓRIO

Neste item são descritos os testes de comunicação sem fio, entre a interface de comunicação (no Notebook) e a CPU do controlador, realizados no laboratório da GIG/DER. Ressalta-se que todos os testes propostos foram executados sem intercorrências e de forma satisfatória, conforme segue:

a) Recebimento do arquivo de programação dos controladores para inserção no notebook;

b) Alteração de plano arquivado no notebook e envio da nova programação para a CPU do controlador;

c) Alteração de horário arquivado no notebook e envio da nova programação para a CPU do controlador;

d) Forçamento de Planos e Modos de Operação, a partir da interface de programação, para execução na CPU do controlador;

e) Monitoramento do Plano e Modo corrente no controlador;

f) Verificação de Relógio;

g) Verificação de Log de falhas;

h) Limpeza de falhas e Reset remoto de um ou mais anéis em falha.

4.4.2 TESTES DE CAMPO

A implementação dos roteadores foi iniciada em fevereiro de 2021, mas foi interrompida em 2022 devido a alterações administrativas no responsável pela manutenção dos semáforos da cidade. Nos testes de campo, o roteador TP-Link MR3020 foi instalado em apenas 30 controladores dos tipos: GWBR Tempo Real; GWBRH Tempo Fixo; e GW3.

Durante os testes de campo, a área operacional relatou dificuldades na configuração remota dos equipamentos. Outro relato menciona ainda a dificuldade de conexão da interface com o controlador, estando o operador dentro da viatura, especialmente em dias de chuva. Também foi relatada a necessidade de se estar muito próximo ao controlador para se conseguir uma conexão estável.

Parte dessas interferências na comunicação já eram esperadas. No primeiro caso elas podem ocorrer quando há uma barreira física ou há algum outro equipamento que utiliza a mesma frequência do Wi-Fi, ou até mesmo uma frequência próxima do padrão do dispositivo. Barreiras físicas (como a porta do controlador ou a massa metálica da viatura) tendem a atenuar o sinal do WiFi, bem como a água da chuva, que pode absorver e refletir as ondas de rádio, causando atenuação e dispersando o sinal do Wi-Fi.

A proximidade do controlador para conseguir uma boa conexão é importante, afinal tem-se que considerar que, em ambiente externo, existem dezenas de equipamentos emitindo e recebendo sinais simultaneamente. Nesse ambiente, o WiFi do notebook procura o roteador correto para se comunicar e, para tanto, irá verificar um a um os dispositivos mais próximos até encontrar o roteador que procura.

Portanto, pode-se concluir que, quanto maior a distância entre a interface de programação e o controlador, mais tempo o WiFi do notebook levará para encontrar o roteador procurado, instalado no controlador.

5. CONFIGURAÇÕES DOS ROTEADORES

Visando a segurança de acesso à rede WiFi dos roteadores dos dois fabricantes (na etapa 1 e nas etapas 2 e 3), foi empregada uma configuração de rede oculta e foi incluída uma senha de acesso WPA2-PSK (contendo letras maiúsculas, letras minúsculas, números e caracteres especiais).

Para acessar o roteador é necessário configurar um IP fixo padrão IPv4 na placa de rede WiFi do notebook sendo que o roteador e o controlador devem estar na mesma família de sub-rede (classe de endereço IP e máscara de rede).

Os controladores DP40A do fabricante Dataprom possuem configurações seriais diferentes para os modelos de Tempo Real e de Tempo Fixo. Assim, deve-se verificar em qual dos modelos será instalado o roteador para então realizar a configuração do equipamento HF2211 conforme descrito abaixo:

a) Para o DP40A TR (Tempo Real): 9600-8-O-1;

b) Para o DP40A TF (Tempo Fixo): 1200-8-O-1.

Já o controlador CD300 do fabricante Digicon possui uma única configuração serial, tanto para o modelo Tempo Real quanto para o Tempo Fixo, devendo ser feita a seguinte configuração no roteador HF2211:

a) Para o CD300 TR/TF (Tempo Real ou Tempo Fixo): 115200-8-N-1

Deve-se utilizar também um software emulador de porta serial através da placa WiFi do notebook, pois os softwares de programação dos controladores semafóricos DP40A e CD300 somente permitem o acesso por meio deste tipo de conexão. Para isso foi utilizado o software True Port Management Tool – da empresa Perle.

6. CONSIDERAÇÕES FINAIS

A solução desenvolvida nas etapas 2 e 3, utilizando o roteador WiFi/RS-232/Ethernet do fabricante Hi-Flying Technology, modelo HF2211, atendeu plenamente a todos os requisitos necessários para acessar remotamente os controladores:

- GreenWave: GWBR Tempo Real, GWBRH Tempo Fixo e GW3.
- Dataprom: DP40A Tempo Real e Tempo Fixo.
- Digicon: CD-300 Tempo Real e Tempo Fixo.

Essa solução mostrou ser possível monitorar, receber e enviar programações, alterar relógio, forçar planos e verificar o Log de falhas dos controladores de forma remota.

Recomenda-se por fim que, para a aplicação em campo, seja realizado o treinamento das equipes operacionais para que conheçam as vantagens e limitações da tecnologia, e para que possam adequar a comunicação sem fio, por meio do roteador WiFi, às suas necessidades. A solução pode ser implantada em qualquer intersecção semaforizada que tenha controladores semafóricos CD300, DP40A ou GW (GW3, GWBR ou GWBRH).

EQUIPE TÉCNICA

Superintendência de Engenharia de Sinalização e Infraestrutura
Eder Carlos de Souza

Gerência de Infraestrutura e Gestão
Gustavo Magela Martineli

Departamento de Equipamentos e Redes
Douglas Wellington Brandão
Euphly Eduardo Piccaro
Edmilson Henrique Valle
Luiz Alonso Lopes Romero
Heliton da Silva
Thiago Lourenço Marani

Superintendência de Tecnologia
Pedro de Angelo

Gerência de Planejamento e Projetos Tecnológicos
Wladimir Sanches Caruso

Departamento de Desenvolvimento de Tecnologia
Wilson Vargas Toledo

Revisão e apoio
Alexandre Francisco Santos
Denise Lima Lopes
Paulo Seiti Ueta
Nilvio Andre Tarricone

Apoio administrativo
Radhemar Amatuzzi

Apoio Técnico

Gerência de Engenharia de Sinalização
Manoel Messia Gaspar de Almeida

Departamento de Engenharia de Campo da Sinalização 1
Marcelo Antonio Fernandes