SafeCable - Detecção em tempo real de furto de cabos de distribuição de energia elétrica com suporte de IoT

João Pedro Brasil Lima[1], **Luis P M Uchôa**[1], **Thiago A Santos**[1], **Alex F R Trajano**[1]

[1]LITEC - Laboratório de Inovação Tecnológica e Exploração Científica
Instituto Atlântico – Fortaleza – Ceará – Brasil

{joao_brasil, luis_maia, thiago_angelino, alex_ferreira}@atlantico.com.br

Abstract. *The theft of electricity distribution cables is a chronic problem that causes interruptions in energy supply and socioeconomic impacts. Distribution companies face difficulties in accurately identifying these events, resulting in extra costs and delays in resolution. This article proposes SafeCable, an IoT system to identify thefts in real time and notify those responsible, allowing an agile response from energy distributors, reducing the impacts caused by theft.*

Resumo. *O furto de cabos de distribuição de energia elétrica é um problema crônico que causa interrupções no fornecimento de energia e impactos socioeconômicos. As empresas distribuidoras enfrentam dificuldades na identificação precisa desses eventos, resultando em custos extras e atrasos na resolução. Este artigo propõe o SafeCable, um sistema IoT para identificar furtos em tempo real e notificar os responsáveis, permitindo uma resposta ágil por parte das distribuidoras de energia, reduzindo os impactos causados pelo furto.*

1. Introdução

O furto de cabos de distribuição de energia elétrica é um problema crônico e generalizado que afeta áreas urbanas e rurais em todo o país. Apenas na cidade de São Paulo em 2023, foram registrados uma média de 1,4 furtos de cabos a cada hora, segundo a Enel[1]. Este tipo de crime não apenas resulta na perda física dos cabos roubados, mas também desencadeia uma série de consequências adversas que têm um impacto profundo na sociedade. Uma das consequências mais imediatas e visíveis é a interrupção do fornecimento de energia elétrica para as áreas afetadas, o que consequentemente afeta a economia, a saúde, a segurança pública e as atividades cotidianas dos cidadãos. Essas interrupções podem persistir por horas, dias ou até mesmo semanas, dependendo da extensão do furto.

As empresas distribuidoras de energia enfrentam dificuldades na identificação precisa de eventos de furto de cabos, pois muitas vezes não têm sistemas de monitoramento capazes de distinguir esse tipo de ocorrência de outras interrupções na rede. Outros eventos como falhas nos equipamentos, acidentes de trânsito e tempestades podem se assemelhar a uma interrupção causada por furto de cabos, tornando a identificação da causa raiz um desafio significativo. Frequentemente, são necessários deslocamentos de equipes para o local afetado a fim de avaliar a situação. Isso consome tempo e pode levar a retrabalho, pois uma equipe inadequada pode ser alocada para a resolução do problema.

[1]Disponível em https://oglobo.globo.com/brasil/sao-paulo/noticia/2023/10/17/furto-de-fios-explode-em-sao-paulo-crime-se-concentra-na-regiao-central.ghtml

Este artigo propõe o SafeCable, um sistema inovador baseado em Internet das Coisas (IoT) para a identificação de furto de cabos em tempo real. O SafeCable consiste num dispositivo equipado com sensores capazes de coletar e reportar dados em tempo real para uma plataforma na nuvem. Uma heurística é empregada para analisar os dados e inferir se houve um evento anormal no cabo que possa ser relacionado ao furto. Quando essa anomalia é identificada, o SafeCable lança alertas para a empresa de distribuição de energia elétrica, permitindo uma resposta ágil e adequada. É importante ressaltar que o objetivo dessa solução não é evitar o furto em si, mas identificar o evento em tempo real. Isso possibilita que a empresa possa enviar uma equipe ao local para verificar a anomalia e acionar a polícia, reduzindo impactos e prejuízos.

2. Trabalhos relacionados

O estudo realizado por [Lencwe et al. 2018] propõe um método para detectar o furto de cabos subterrâneos através da análise de perturbações de frequência no cabo. O objetivo é desenvolver um sistema capaz de disparar alarmes e localizar rapidamente essas perturbações, visando, em última instância, reduzir falhas de energia, perdas econômicas e interrupções nos serviços essenciais causadas pelo furto de cabos na África do Sul. O sistema proposto utiliza apenas parâmetros de corrente e tensão do condutor para identificar distúrbios de frequência que antecedem o furto. Os autores destacam que os perpetradores frequentemente recorrem a métodos como atear fogo no isolamento dos cabos ou disparar armas de fogo diretamente no cabo, com o intuito de desativar a subestação, desenergizando o condutor e facilitando o corte manual do cabo.

Os autores em [Mohd Chachuli et al. 2020] propuseram um sistema que detecta quedas de tensão e alterações de temperatura, indicativos comuns de tentativas de furto, acionando alarmes para alertar as autoridades. Essa abordagem permite ações de resposta rápidas, como o envio de equipes de segurança, dissuadindo furtos e aprimorando as medidas de segurança. Os principais componentes do sistema incluem um microcontrolador PIC, divisor de tensão, sensor de temperatura e um modem GSM, trabalhando em conjunto para monitorar e comunicar incidentes potenciais de furto. Resultados experimentais destacam a eficiência do sistema em detectar quedas de tensão e alterações de temperatura, evidenciando a capacidade de auxiliar no combater o furto de cabos.

3. Arquitetura do SafeCable

A estratégia utilizada no SafeCable para a detecção do furto de cabos, foi a de detecção da queda física do cabo. A vantagem em usar essa técnica de detecção, ao invés de outras que monitoram sinais de tensão e corrente no cabo, é que essa pode ser usada para redes de distribuição que ainda não estão energizadas. Este é um cenário comum em projetos de expansão da rede elétrica executados pelas companhias de distribuição.

Dessa forma, a arquitetura desenvolvida consiste em três componentes: os nós, os *gateways* e a aplicação em nuvem, como apresentado na Figura 1. Os nós são instalados diretamente nos cabos de transmissão ou distribuição, onde os sensores são instalados para monitoramento dos cabos. Esses nós enviam constantemente dados para um *gateway* usando a tecnologia LoRa [Hwang et al. 2019]. Os *gateways*, em número muito menor, atuam como concentradores. Eles recebem os dados de todos os nós dentro de seu alcance e enviam esses dados para a aplicação em nuvem via HTTP através da Internet. Na

aplicação em nuvem, os dados são analisados por uma heurística de detecção e alerta de furto. Nesse modelo arquitetural, o nó é simplificado, tornando-o mais barato e eficiente em energia.

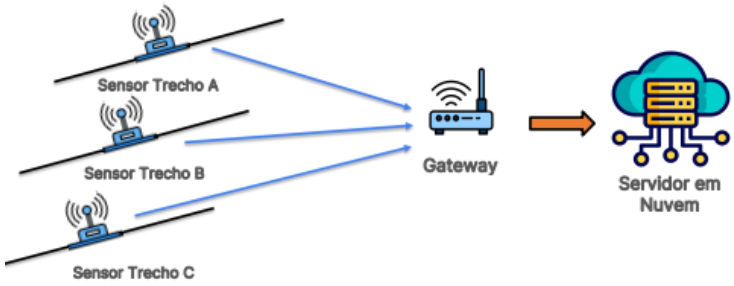

Figura 1. Visão geral dos componentes do SafeCable

3.1. Os Nós

Os nós contém um microcontrolador com um módulo de comunicação LoRa, um barômetro para medir altitude e temperatura, um magnetômetro para detectar mudanças na angulação do dispositivo e um acelerômetro para detectar quedas e movimentos. A ideia por trás do uso desses sensores é possibilitar uma maior variedade de dados para alimentar a heurística de detecção. Há grande preocupação em evitar os falsos positivos, ou seja, casos em que o algoritmo alerta sobre um furto quando não há, o que pode gerar grande descrédito na solução.

O módulo ESP-32 TTGO foi utilizado na construção dos nós, possuindo um microcontrolador ESP32-D0WDQ6 e um rádio LoRa Semtech SX1276. Uma bateria LiPo de 3,4 V e 400 mAh foi utilizada como fonte de alimentação para o dispositivo. A carcaça de todos esses dispositivos, mostrada na Figura 2, foi projetada sob medida e construída por uma impressora 3D. O módulo ESP-32 TTGO e todos os sensores estão contidos no corpo principal da carcaça e a fixação ao cabo é feita por meio de uma tampa que é parafusada na carcaça, com um perfil que pode ser ajustado para se adequar à espessura do cabo.

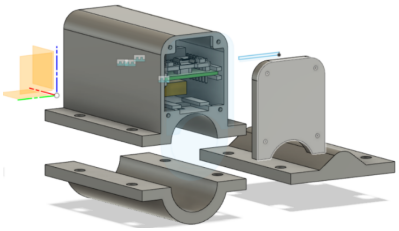

Figura 2. Modelo 3D da carcaça do nó

O funcionamento do dispositivo é descrito a seguir. Inicialmente, o dispositivo está em estado de espera, em modo de baixo consumo de energia, e dois modos de interrupção podem alterar esse estado: a interrupção do temporizador ou a interrupção de detecção de movimento. A interrupção do temporizador garante que o dispositivo mantenha contato periódico com a aplicação em nuvem, enviando dados de todos os sensores, os quais o sistema utilizará posteriormente para alimentar a heurística de detecção e

sinalizar uma possível desconexão do dispositivo. A interrupção de movimento, por outro lado, é causada pelo acelerômetro quando este detecta uma variação súbita em algum dos eixos, possivelmente devido a uma condição de queda livre do dispositivo. Essas duas formas de interrupção movem o dispositivo para o estado de envio de dados, onde ele coleta dados de todos os sensores e os envia para o gateway via LoRa. Após o envio dos dados, o dispositivo retorna ao estado de baixo consumo de energia.

A detecção de queda com suporte de sensores IoT é um tópico amplamente investigado em outras áreas, tanto considerando o uso de acelerômetros [Tong et al. 2013], quando usando barômetros [Bianchi et al. 2010].

3.2. Os gateways

Assim como os nós, para os gateways foram usadas placas de desenvolvimento ESP32 TTGO. A função desse dispositivo é transmitir as mensagens recebidas via LoRa dos sensores para a aplicação em nuvem via WiFi. De acordo com a arquitetura da solução, esses gateways são colocados em pontos estratégicos para alcançar um grande número de nós, graças ao longo alcance que a tecnologia LoRa proporciona. Esses dispositivos não são alimentados por bateria, pois necessariamente terão um consumo de energia maior, necessitando de uma fonte de alimentação externa.

Inicialmente, o dispositivo fica em um estado de espera por mensagens LoRa; quando recebe uma mensagem, ele verifica se o formato da mensagem recebida está de acordo com o protocolo estabelecido e, em caso afirmativo, envia essa mensagem para a aplicação via HTTP e retorna ao estado de espera. O formato de mensagem esperado pelo gateway é ilustrado na Figura 3. Trata-se de um JSON com 16 campos para identificação do dispositivo, contador de mensagens, a causa do envio (temporizador ou acelerômetro) e as métricas de todos os sensores.

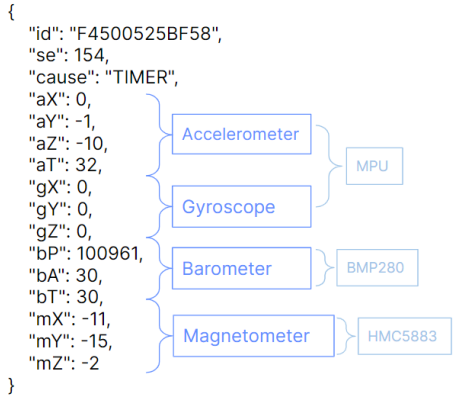

Figura 3. Formato das mensagens recebidas e enviadas pelo gateway

3.3. A Aplicação em Nuvem e a Heurística

A aplicação em nuvem é responsável por receber todas as mensagens enviadas pelos nós através dos gateways. A aplicação mantém um cadastro de cada um dos nós, com seu identificador único e as coordenadas geográficas de instalação. A medida que as mensagens são recebidas, o sistema atualiza o estado atual do respectivo nó no banco de dados, mantendo sempre o histórico atualizado para cada um dos seus sensores. Se a causa da

transmissão do nó foi motivada pela interrupção do temporizador, o fluxo para. Caso seja pela interrupção do acelerômetro, que indica movimento súbito, as métricas atuais de todos os sensores são enviados para a heurística de detecção.

A heurística de detecção consiste numa verificação de anomalias com base no desvio das médias móveis dos valores do termômetro, barômetro, giroscópio e magnetômetro. Para cada sensor, o sistema calcula as seguintes equações para cada uma de suas métricas:

$$MetricAverage = (1 - \alpha) \times MetricAverage + \alpha \times CurrentMetric \quad (1)$$

$$DevMetric = (1 - \beta) \times DevMetric + \beta \times |CurrentMetric - MetricAverage| \quad (2)$$

A Equação 1 consiste numa média móvel exponencial de uma métrica. A Equação 2 consiste na média móvel exponencial da diferença do valor atual da métrica em relação ao resultado da Equação 1, de forma que $DevMetric$ é comparado a um valor T que especifica o limiar de anomalia. Vale salientar que cada sensor possui múltiplas métricas, como exemplificado na Figura 3. Dessa forma, quando um sensor possuir pelo menos uma métrica onde $T < DevMetric$, a heurística considera aquele sensor como anômalo. Finalmente, caso existam X sensores anômalos, a heurística considera que aquele nó em questão está numa situação de furto, realizando o alerta para o usuário.

4. Resultados

O dispositivo foi inicialmente testado em laboratório, onde foram criados seis cenários de teste para verificar a resposta da heurística. Cada um desses cenários foi repetido 6 vezes, gerando um total de 36 testes. Com base nos resultados dos testes, foram calculadas a acurácia, a precisão e a taxa de falsos positivos, servindo como métricas de avaliação de desempenho. Esta última é extremamente importante para evitar o descrédito do dispositivo. A Tabela 1 contém a descrição de cada cenário de teste.

Tabela 1. Cenários de testes realizados

Teste	Descrição	Resultado esperado
1	Cabo puxado em uma extremidade até se soltar da outra e cair no chão, junto com o dispositivo.	Furto
2	Cabo cortado com alicate, causando pouco movimento no cabo antes da queda vertical.	Furto
3	Cabo cortado com uma serra, causando movimento horizontal no cabo antes da queda vertical.	Furto
4	Movimento horizontal no cabo, simulando ventania forte.	Normal
5	Movimento vertical no cabo, simulando queda de galhos no cabo.	Normal
6	Impacto de objetos diretamente no Nó.	Normal

O dispositivo nó foi construído utilizando os sensores MPU6050 (acelerômetro), BMP280 (barômetro e temperatura) e o HMC5883L (magnetômetro). A heurística foi ajustada para os valores $\alpha = 0.5$, $\beta = 0.5$ para todos os sensores, enquanto $T = 1,1$ para o barômetro, $T = 3,75$ para a temperatura e $T = 2,5$ para o magnetômetro. Após a execução dos testes, foi montada uma matriz de confusão para uma melhor visualização dos resultados. A matriz presente na Figura 4 mostra que a heurística atingiu uma precisão de 86% e uma acurácia de 78%, sendo 11% de falsos positivos e 33% de falsos negativos.

Como visto na matriz de confusão, os resultados mostraram-se promissores, apesar de 11% de falsos positivos. Dois fatores chamaram a atenção durante a experimentação. Primeiro, nos testes de laboratório foram usados cabos de energia finos

		Predito		
		Normal	**Furto**	
Real	**Normal**	12	6	Sens.: 0,67
	Furto	2	16	F.P.: 0,11
		Prec.: 0,86	F.N.: 0,33	Acur.: 0,78

Figura 4. Matriz de confusão

e flexíveis, com massa menor do que os usados nas redes de distribuição e transmissão reais, de modo que os utilizados aqui são mais suscetíveis ao movimento e caem com menos violência do que os cabos reais. Em segundo lugar, os testes foram realizados em uma altura significantemente menor devido a limitações de espaço no laboratório, com apenas 3 metros de altura. Em situações reais de queda de cabos, o dispositivo cairá por um tempo maior e, consequentemente, a variação de aceleração durante a queda e no momento do impacto com o solo, facilitando a detecção. Além do mais, o maior diferencial de altura entre o poste e o chão possibilita uma maior mudança nos valores observados pelo barômetro, auxiliando a detecção de valores anômalos.

5. Conclusão

Este trabalho introduziu o SafeCable, um sistema para detecção e alerta de furto de cabos. Os resultados promissores dos testes em laboratório indicam um potencial para a implementação do SafeCable em ambientes reais. Espera-se que essa solução desempenhe um papel fundamental na redução dos impactos sociais causados pelos furtos de cabos, melhorando a eficiência das empresas responsáveis pela rede elétrica em sua resposta a esses incidentes. Embora os resultados tenham sido favoráveis, há espaço para aprimorar a precisão do sistema, especialmente no que diz respeito à redução dos falsos positivos observados nos testes laboratoriais. Como sugestão para trabalhos futuros, recomenda-se a investigação de novas heurísticas e a exploração da Inteligência Artificial para otimizar o desempenho da solução e buscar pela diferenciação entre a queda acidental e por furto.

Referências

Bianchi, F., Redmond, S. J., Narayanan, M. R., Cerutti, S., and Lovell, N. H. (2010). Barometric pressure and triaxial accelerometry-based falls event detection. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 18(6):619–627.

Hwang, L.-C., Chen, C.-S., Ku, T.-T., and Shyu, W.-C. (2019). A bridge between the smart grid and the internet of things: Theoretical and practical roles of lora. *International Journal of Electrical Power & Energy Systems*, 113:971–981.

Lencwe, M., Chowdhury, S. D., and Olwal, T. (2018). Detection of underground power cable theft: Strategies and methods. In *2018 IEEE PES/IAS PowerAfrica*, pages 1–9.

Mohd Chachuli, S. A., Mohd Nazri, S., Yusop, N., and Mohamad, N. R. (2020). Cable theft monitoring system (ctms) using gsm modem. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 2(1):57–66.

Tong, L., Song, Q., Ge, Y., and Liu, M. (2013). Hmm-based human fall detection and prediction method using tri-axial accelerometer. *IEEE Sensors Journal*, 13(5):1849–1856.