Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Faculdade de Engenharia

Rômulo Gon Ferreira

Análise Probabilística de um Sistema de Rastreamento Baseado em RFID

Rio de Janeiro
2019

Rômulo Gon Ferreira

Análise Probabilística de um Sistema de Rastreamento Baseado em RFID

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre em Engenharia Eletrônica, ao Programa de Pós-Graduação em Engenharia Eletrônica, da Universidade do Estado do Rio de Janeiro. Área de concentração: Redes de Telecomunicações.

Orientador: Prof. D.Sc. Marcelo Gonçalves Rubinstein
Orientador: Prof. D.Sc. Rodrigo de Souza Couto

Rio de Janeiro
2019

CATALOGAÇÃO NA FONTE

UERJ / REDE SIRIUS / BIBLIOTECA CTC/B

F383 Ferreira, Rômulo Gon.
Análise probabilística de um sistema de rastreamento baseado em RFID / Rômulo Gon Ferreira. – 2019.
67f.

Orientadores: Marcelo Gonçalves Rubinstein, Rodrigo de Souza Couto.
Dissertação (Mestrado) – Universidade do Estado do Rio de Janeiro, Faculdade de Engenharia.

1. Engenharia Eletrônica - Teses. 2. Sistemas de identificação por radiofrequência - Teses. 3. Sistema de Posicionamento Global - Teses. 4. Sistema global para comunicações móveis - Teses. I. Rubinstein, Marcelo Gonçalves. II. Couto, Rodrigo de Souza. III. Universidade do Estado do Rio de Janeiro, Faculdade de Engenharia. IV. Título.

CDU 681.5

Bibliotecária: Júlia Vieira – CRB7/6022

Assinatura

Data

Rômulo Gon Ferreira

Análise Probabilística de um Sistema de Rastreamento Baseado em RFID

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre em Engenharia Eletrônica, ao Programa de Pós-Graduação em Engenharia Eletrônica, da Universidade do Estado do Rio de Janeiro. Área de concentração: Redes de Telecomunicações.

Aprovada em 28 de fevereiro de 2019.

Banca Examinadora:

Prof. D.Sc. Marcelo Gonçalves Rubinstein (Orientador)
Faculdade de Engenharia - UERJ

Prof. D.Sc. Rodrigo de Souza Couto (Orientador)
PEE/COPPE/UFRJ

Prof. D.Sc. Alexandre Sztajnberg
Faculdade de Engenharia - UERJ

Prof. Dr. Luís Henrique Maciel Kosmalski Costa
PEE/COPPE/UFRJ

Rio de Janeiro

2019

DEDICATÓRIA

Dedico esta dissertação à minha avó Eulália (*in memoriam*) por ajudar na minha criação e ser uma das minhas inspirações durante minha vida e minha trajetória como discente. Dedico também à minha avó Amélia (*in memoriam*) que nos deixou no decorrer dessa dissertação, deixando como exemplo sua simplicidade, carinho, força de vontade e garra.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me dado força e sabedoria para conseguir concluir mais essa etapa enfrentando a difícil tarefa de conciliar minha vida acadêmica com minha vida pessoal e profissional. Agradeço à minha noiva Sayonara C. de Souza do Rosario por todo o carinho, respeito, compreensão e paciência durante todo esse processo. Agradeço aos meus pais Darci Gomes Ferreira e Olália M. Gon Ferreira por todo o incentivo e por todo o sacrifício dedicado a mim e a meus irmãos durante todas as nossas vidas. Agradeço aos meus irmãos Renan Gon Ferreira e Rafael Gon Ferreira pelas palavras de incentivo e pela compreensão de minhas ausências mais prolongadas nesses períodos. Agradeço aos amigos Marcelo Brandão e Eisenhower Rios Santos que foram as pessoas que me incentivaram a iniciar mais essa etapa e me deram todo o suporte dentro da empresa para que tornasse todo esse processo viável. Agradeço aos amigos da área de Implantação da Telefônica Vivo RJ, por todo o apoio, tornando possível minha ausência em vários momentos e batalhando comigo em mais essa etapa. Agradeço ao Programa de Pós-Graduação em Engenharia Eletrônica da Universidade do Estado do Rio de Janeiro pela oportunidade de poder participar do programa de Pós-Graduação. Agradeço aos amigos de classe, em especial ao André Kern, que juntos superamos diversas dificuldades oriundas de aulas e trabalhos. Agradecimento especial aos professores e orientadores Marcelo G. Rubinstein e Rodrigo S. Couto, pelo tempo dedicado, pelas orientações, pela disposição de sempre me ajudar com minhas limitações técnicas e teóricas e principalmente pela paciência. Não existem palavras que possam descrever minha gratidão. Agradeço ainda aos membros da banca examinadora pela disponibilidade e aceite para avaliar esse trabalho. Por fim, um agradecimento a todos que de certa forma participaram, mesmo que indiretamente, desse momento único em minha vida. Muito obrigado!

There is a driving force more powerful than steam, electricity and atomic energy: the WILL.

Albert Einstein

RESUMO

FERREIRA, R. G. *Análise Probabilística de um Sistema de Rastreamento Baseado em RFID*. 2019. 67 f. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2019.

No Brasil, as empresas de telecomunicações enfrentam muitos obstáculos para ter e manter uma rede robusta, com cobertura, capacidade e qualidade. Para conseguir dar qualidade a uma rede de telecomunicações, as empresas buscam sempre reduzir o tempo de indisponibilidade. Essa métrica é muito importante nesse meio, pois é a principal característica avaliada pela agência reguladora (ANATEL - Agência Nacional de Telecomunicações). São muitos os aspectos que podem influenciar essa métrica que vão desde aspectos climáticos até vandalismos. Esse último é um grande problema que as operadoras enfrentam hoje no Brasil assim como os furtos qualificados que, além de trazerem grandes prejuízos, também aumentam a indisponibilidade da rede. Considerando esses problemas, algumas soluções são adotadas visando dificultar esses acontecimentos; outras soluções visam reduzir a médio e longo prazo esse tipo de ação. Esta dissertação propõe uma solução que ajuda na redução desses atos e na recuperação desses equipamentos utilizando uma plataforma de desenvolvimento com microcontrolador, uma placa de GSM/GPS, uma placa com leitor RFID e etiquetas RFIDs. O intuito é transformar os equipamentos em iscas, inserindo neles um rastreador que envia mensagens de sua localização para o NOC *(Network Operations Center)* e, após chegar ao depósito para onde são levados os produtos dos furtos, procura por outros equipamentos que possuam o mesmo sistema. Assim, informa ao NOC a localidade, quantos e quais equipamentos estão próximos a ele. O sistema foi montado com a utilização dos componentes citados anteriormente para funcionar como um rastreador e enviar mensagens para um telefone pré-pago simulando um NOC. O consumo de cada componente foi analisado utilizando um multímetro e os testes foram realizados em um ambiente controlado. Também foi extraído do sistema, o tempo médio de resposta para localização e envio de mensagens. Com esses dados, dois pontos onde já foram registrados furtos foram utilizados para analisar a eficiência do sistema. Esta dissertação se baseou nos cálculos de sistemas estocásticos com propriedade markoviana para demonstrar que o sistema proposto é eficiente e possui alta probabilidade de sucesso nos cenários considerados.

Palavras-chave: Rastreamento; RFID; GPS; GSM;

ABSTRACT

FERREIRA, R. G. *Probabilistic Analysis of a Tracking System Based on RFID*. 2019. 67 f. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2019.

In Brazil, telecommunications companies face many obstacles to have and maintain a robust network, with coverage, capacity and quality. In order to give quality to a telecommunications network, companies always aim to reduce unavailability. This metric is very important in this environment, since it is the main item in the measurements of the regulatory agency (ANATEL - National Telecommunications Agency). There are many aspects that can influence this metric ranging from climatic aspects to vandalism. This last one is a big problem that the operators face in Brazil today as well as the qualified thefts that besides bringing great damages, also increase the unavailability of the network. Considering these problems, some solutions are adopted in order to turn these events more difficult. Other solutions aim at reducing this type of action in the medium and long term. In this dissertation we propose a solution that helps to reduce these acts and to recover these equipments using a development platform with a microcontroller, a GSM/GPS card, a board with an RFID reader and RFID tags. The intention is to insert a simple tracker in the equipment that sends messages from its location to the NOC (Network Operations Center) and after arriving at a warehouse, looks for other equipment that has the same system and informs the NOC of the location, how many and which equipment is close to it. This dissertation is based on the calculations of stochastic systems with Markovian properties to demonstrate that the proposed system is efficient and has a high probability of success in certain scenarios.

Keywords: Tracking; RFID; GPS; GSM;

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	*Alternating Current*
ANATEL	Agência Nacional de Telecomunicações
BTS	*Base Transceiver Station*
GPS	*Global Positioning System*
GSM	*Global System for Mobile communications*
HF	*High Frequency*
IoT	*Internet of Things*
LF	*Low Frequency*
LoRa	*Long Range*
LTE	*Long Term Evolution*
mA	Miliampère
mAh	Miliampère-Hora
NAVSTAR	*Navigation Satellite with Time and Ranging*
NOC	*Network Operations Center*
RF	*Radio-Frequency*
RFID	*Radio-Frequency IDentification*
SMS	*Short Message Service*
UHF	*Ultra High Frequency*
WCDMA	*Wideband Code Division Multiple Access*

SUMÁRIO

INTRODUÇÃO

No Brasil, as operadoras de telefonia móvel vêm enfrentando um grande problema com vandalismos e principalmente roubos e furtos de equipamentos em suas redes. Os custos para reposição desses equipamentos já alcançam 320 milhões de reais ao ano (DUPRAT, 2016). Além dos prejuízos gerados às operadoras de telefonia, a sociedade em geral também é prejudicada, uma vez que o serviço de telefonia é afetado (ONLINE, 2018).

Algumas ideias de segurança têm sido levantadas, como pintar parte do equipamento com o logotipo do proprietário (POUSOALEGRE.NET, 2018). Esta ação exigiria com que o receptor fizesse a raspagem do equipamento acusando assim a posse ilegal do mesmo em uma possível fiscalização. Outra ideia que está em pauta é a instalação de GPS dentro dos equipamentos onde um rastreamento em curto prazo de tempo seria possível. Também está em estudo, pelos próprios fornecedores, uma forma de deixar o equipamento inutilizável caso seja retirado da rede sem programação prévia. Isso reduziria o interesse dos compradores do produto do roubo que, em sua maioria, são pequenos provedores de Internet (POUSOALEGRE.NET, 2018) (SKODOWSKI; SARZI, 2016). Esse tipo de crime geralmente é classificado como furto qualificado, que envolve destruição, vandalismo ou rompimento de obstáculo para execução do crime, abuso de confiança, fraude ou destreza (GUEDES, 2008). Geralmente, o criminoso ou grupo de criminosos, possui um local de armazenamento, como casas e galpões (BRITO, 2017).

Nesta dissertação, a proposta principal é utilizar a tecnologia para transformar um possível equipamento que venha a ser roubado, em isca. Dessa forma, foi utilizada uma rede para coletar informações e enviar para um NOC (*Network Operations Center* - Centro de Operações de Rede). Como não é possível ter uma estrutura no ponto de recepção dos equipamentos furtados e a localização do mesmo é desconhecida, a proposta é utilizar os próprios equipamentos como iscas, inserindo dentro deles uma identidade que possa ser lida e identificada. Para isso foi utilizado um método de identificação automática conhecido como RFID. Para estabelecer uma comunicação entre o equipamento furtado e o NOC, foi incluído no sistema uma placa GSM (*Global System for Mobile communications* - Sistema Global para Comunicações Móveis). Para solucionar o problema da localização, o sistema conta com o GPS (*Global Positioning System* - Sistema de Posicionamento Global).

Nesta dissertação é apresentado um sistema que contém quatro etapas, sendo elas, rastreamento, identificação, coleta de dados e transmissão de dados. As etapas foram implementadas realizando a comunicação entre o sistema e um telefone móvel (para simular o NOC) via GSM. O GPS foi utilizado para extrair a localização do sistema e o RFID para formar uma pequena rede de sensores que tem a função de possibilitar a comunicação entre diferentes etiquetas RFIDs, acusando assim, quais etiquetas estavam próximas. Por este

motivo, o sistema também utilizará etiquetas passivas. Essas etiquetas não possuem fonte de alimentação própria e funcionam a partir da energia enviada pelo sinal do leitor. Dessa forma, é possível que um equipamento energizado que possua leitor RFID encontre essa etiqueta. Quando outra etiqueta é encontrada, o sistema faz um vínculo do ID encontrado em sua mensagem que é novamente transmitido ao NOC. Influenciado por (BARAKA et al., 2013), o sistema foi projetado com o intuito de ampliar seu período de funcionamento mesmo utilizando baterias de baixa capacidade. Sendo assim, esta dissertação inclui um conjunto de condições para que o microcontrolador do sistema possa ativar as funções do mesmo de forma gradual e aplique o modo *standby* em alguns recursos. Dessa forma, foi possível ampliar seu tempo de funcionamento. O sistema obtém sucesso quando é capaz de utilizar objetos roubados como isca para detectar outros objetos roubados. Dessa forma, para calcular a probabilidade de sucesso, foi utilizada uma Cadeia de Markov. Após realizar todos os cálculos e expressar graficamente os resultados, foi possível observar que o sistema é eficiente e viável. Suas limitações são ampliadas conforme a distância entre o local do furto e o local de armazenamento; no entanto, mesmo considerando cenários que trabalham no limite do sistema, ou seja, quando há grande probabilidade de acabar a energia do sistema durante o percurso, o mesmo ainda se mostra viável. O objetivo principal deste sistema é apresentar uma proposta de rastreamento de objetos que, após furtados, possibilite utilizá-los como detectores e rastreadores de outros equipamentos que possuam o mesmo sistema. O funcionamento do sistema é avaliado em diferentes cenários via cálculos de Cadeias de Markov.

Esta dissertação está organizada da seguinte forma. O próximo capítulo, apresenta os trabalhos relacionados que foram utilizados como base para a ideia e implementação do sistema. O Capítulo 2 descreve quais componentes foram utilizados, dados básicos sobre cada tecnologia, como foram utilizadas e como o sistema foi desenvolvido. No capítulo 3, a cadeia de Markov do sistema será apresentada e detalhada em etapas. No capítulo 4, as análises probabilísticas do sistema serão apresentadas em dois cenários distintos, quando a probabilidade de acabar a energia do sistema durante o percurso é nula ou maior que zero. No último capítulo, serão apresentadas as conclusões e quais tópicos foram avaliados como oportunidades de trabalhos futuros.

1 TRABALHOS RELACIONADOS

No Brasil, as operadoras de telefonia vêm sofrendo com vandalismos e furtos em suas redes. Além do prejuízo para reposição de equipamentos, suas redes sofrem valores maiores do índice de indisponibilidade. Para coibir esse tipo de ação, soluções de Internet das Coisas (*Internet of Things* - IoT) já estão sendo utilizadas (PEPINO; DIAS, 2018) e o RFID é um dos dispositivos que já vêm sendo utilizado para esse fim (SENNA; SOARES, 2018). Com o passar do tempo, soluções de IoT se mostram cada vez mais presentes no dia a dia das pessoas, possibilitando formas mais eficientes de controlar dispositivos e abrindo oportunidades para criação de novas soluções tecnológicas para maior comodidade, segurança e bem-estar dos usuários. Segundo (XIA et al., 2012) e (YANG, 2014), o conceito de IoT baseia-se na interconexão em rede de objetos do cotidiano.

Em (ROHOKALE; PRASAD; PRASAD, 2011), a utilização de IoT é proposta para criação de uma rede para monitorar a saúde de pessoas que vivem em áreas rurais com acesso limitado a hospitais. A proposta desta dissertação também é realizar monitoramento, porém, ao invés de monitorar indivíduos, serão monitorados equipamentos. Em (ROHOKALE; PRASAD; PRASAD, 2011), o foco também é transmitir informações básicas sobre a saúde das pessoas. A solução conta com um sistema de coleta de dados via RFID e uma rede estruturada para transmitir esses dados via internet. Também é considerada no sistema a privacidade do indivíduo; logo, não há precisão na localização do indivíduo; é somente utilizada uma identificação da região de presença do indivíduo. Nessa dissertação, diferente do sistema proposto em (ROHOKALE; PRASAD; PRASAD, 2011) a localização é importante e deve ser a mais precisa possível. (MAURYA; SINGH; JAIN, 2012) citam a utilização de GPS e GSM como parte de soluções antifurto para veículos. Nesta dissertação, essas tecnologias foram utilizadas com o mesmo objetivo. Para localizar o equipamento, o GPS será utilizado e para efetuar a transmissão dos dados, o GSM será usado.

Nesta dissertação, o RFID também será utilizado, porém, para identificar o equipamento. O sistema aqui proposto deve ser capaz de identificar demais equipamentos após chegar local de armazenamento, mesmo que os demais equipamentos não estejam energizados. Essa funcionalidade é necessária, pois os tempos entre chegadas de diferentes equipamentos aos locais de armazenamento podem ser muito altos e toda a energia das baterias dos equipamentos que já estão no local pode ter sido consumida. Com isso, apenas a etiqueta passiva que cada equipamento deve possuir poderá ser localizada. Dessa forma, caso um equipamento roubado tenha sua energia completamente consumida, este equipamento se torna um alvo, ou seja, pode ser detectado, de um possível outro sistema que seja furtado e chegue energizado. Para implementação, outro ponto que deve ser

considerado é o custo. O custo deve ser o menor possível. Segundo (SEUFITELLI et al., 2010), o leitor RFID pode identificar etiquetas passivas, ou seja, etiquetas que são alimentadas pelo sistema de leitura através do campo magnético. As etiquetas passivas possuem menor alcance, porém têm baixo custo, são mecanicamente flexíveis e trabalham nas faixas LF (*Low Frequency* - Baixa frequência), HF (*High Frequency* - alta frequência) e UHF (*Ultra High Frequency* - Frequência ultra alta). Ainda segundo (SEUFITELLI et al., 2010), o leitor RFID possibilita a leitura simultânea de etiquetas, o que é importante para possibilitar a identificação simultânea de mais de um equipamento.

Além de seu baixo custo e de ser facilmente encontrado, outro motivo de escolher essa tecnologia é que o sistema baseado em RFID é composto por etiquetas que são anexadas a objetos e leitores e podem ser identificadas sem visada direta de RF. É possível utilizar essa tecnologia em inúmeras aplicações de rastreamento e em locais de diferentes características (YANG et al., 2012). Em (ATZORI; IERA; MORABITO, 2010), é proposto um sistema que pode ser utilizado para monitorar dados de objetos e equipamentos. No entanto, cada objeto deve possuir um rastreador e, diferente desta dissertação, não há possibilidade de monitorá-lo caso não esteja energizado. Nesta dissertação, uma bateria é utilizada para que seja possível o rastreamento do equipamento após o furto. (ROBERTS, 2006) e (EZE et al., 2018) apresentam o RFID como solução antifurto em lojas de varejo e em veículos.

Em (HAYATI; SURYANEGARA, 2017), um sistema de rastreamento de pacientes é proposto considerando GPS e LoRa (*Long Range* - Longo Alcance). Já em (FARGAS; PETERSEN, 2017) LoRa e GPS também foram utilizados, porém, simulando rastreamento de qualquer objeto e armazenando os dados de localização em um banco de dados. LoRa possui maior alcance quando comparado ao RFID, no entanto, RFID é mais barato e mais fácil de se encontrar no mercado. O objetivo desta dissertação é utilizar um equipamento furtado para servir de isca, analisar a probabilidade de rastreá-lo e encontrar outros equipamentos furtados anteriormente. Sendo assim, a escolha do RFID se deve ao fato de que a tecnologia permite fazer todas as análises desejadas com menor custo.

Em (HE et al., 2009), é proposto um sistema de rastreamento utilizando RFID, GPS e GPRS (*General Packet Radio Services*). Em (KUMAR et al., 2016), algumas propostas de segurança são consideradas. Umas delas é um sistema de rastreamento veicular utilizando GPS e GSM. Trata-se de um rastreamento simples e individual do veículo. Outra proposta é a desaceleração automática do veículo em determinadas situações, como por exemplo, quando o GPS identificar que o veículo está transitando em frente a escolas e hospitais. Para realizar esse operação, o sistema utiliza um microcontrolador chamado AT89S52. O escopo apresentado tem objetivo diferente do desta dissertação, no entanto, a forma como o rastreamento foi projetado e como as informações foram processadas ajudaram a desenvolver uma solução para o problema aqui descrito.

Em (JACOBSEN; ALIU; EBEID, 2017), um sistema de rastreamento veicular

também é proposto, porém, visa o baixo custo de implementação e por este motivo utiliza equipamentos COTS (Commercial Off The Shelf) que são dispositivos comerciais prontos para uso, como por exemplo, Raspberry Pi e Arduino. Também é considerada nesse artigo, a utilização de SMS (*Short Message Service* - Serviço de Mensagens Curtas) para informar a localização do veículo. Neste caso, o SMS foi utilizado, pois os autores consideraram que seria o meio mais seguro para realizar o informe. Nesta dissertação, também consideramos módulos de desenvolvimento, GPS, RFID e GSM com baixo custo. A transmissão dos dados via SMS utilizando a rede GSM foi realizada nesta dissertação, pois o GSM é uma rede já consolidada e que possui a maior cobertura no país (TELECO, 2019).

(JIN et al., 2018) propõem um sistema antifurto para *smartphones* cujo modelo se baseia em Cadeias de Markov. Para validar a viabilidade do sistema, também foi proposto nessa dissertação utilizar Cadeia de Markov, dessa forma, foi possível definir as transições necessárias e realizar os cálculos probabilísticos para cada uma delas.

A bateria utilizada no sistema foi uma bateria de lítio de 9 V com capacidade de 380 mAh. Segundo (NETO; OLIVEIRA; NASCIMENTO, 2013), esse bateria possui alta densidade energética, tamanho pequeno, é leve e possui boa resistência a defeitos de efeito de memória. Já segundo (POSSA; PASSOLD, 2006), o efeito de memória de uma bateria é o termo que surgiu para tentar explicar porque as baterias baseadas em níquel (NiCd e NiMH) "viciam". Ainda segundo (POSSA; PASSOLD, 2006), este efeito se deve à cristalização do hidróxido de níquel que compõe o eletrodo positivo. Este foi mais um motivo para empregar, nesta dissertação, a bateria de lítio.

Em (YOUSSEF; YOSEF; EL-DERINI, 2010), um sistema de rastreamento é proposto, no entanto, o objetivo é realizar o rastreamento com a maior economia possível de energia. Para isso, além, a proposta conta com um GPS, um acelerômetro e uma bússola. A ideia principal é combinar as leituras do acelerômetro e da bússola para estimar a localização utilizando a posição inicial e velocidade; dessa forma a bússola determina a direção do movimento enquanto a leitura do acelerômetro é realizada duas vezes para determinar o deslocamento do telefone ao longo do percurso. Devido ao ruído nas leituras do acelerômetro e da bússola, os erros se acumulam com o passar do tempo, então o GPS é brevemente utilizado para obter uma localização precisa. No sistema aqui proposto, a precisão constante do GPS é indispensável nos momentos de busca de localização, logo, o método proposto por (YOUSSEF; YOSEF; EL-DERINI, 2010) não é recomendável para o objetivo dessa dissertação. Sendo assim, outra solução de rastreamento que utiliza GPS deve ser aplicada. Em (SANT'ANNA et al., 2018), é proposto o uso de uma semântica síncrona para que aplicativos, diante de reações ao ambiente, entrem em modo de *standby* pelo máximo tempo possível, obtendo assim economia de energia. Utilizando o mesmo princípio, o sistema aqui proposto também utiliza programação para que os componentes do sistema entrem no modo *standby* quando possível; dessa maneira, é possível reduzir o consumo de energia do sistema e aumentar sua autonomia.

Utilizando essas tecnologias combinadas, um ponto de motivação para a escolha do tema foi apresentar uma solução prática, viável e de baixo custo para um problema complexo que afeta todo território brasileiro. Dessa forma, a dissertação mostra que é possível desenvolver soluções que dificultam a médio e longo prazo ações de vandalismos e furtos.

2 SISTEMA PROPOSTO

Este capítulo descreve como o sistema foi idealizado, detalha como o mesmo foi implementado e aborda as tecnologias e componentes utilizados. Além disso, apresenta uma comparação entre os valores de mercado dos componentes utilizados no protótipo e alguns equipamentos alvos de furtos utilizados pelas operadoras.

2.1 Estrutura do Sistema

Para avaliar a eficiência e a viabilidade do sistema, foi necessário fazer um levantamento de alguns parâmetros. Dessa forma as análises foram realizadas em laboratório, considerando a distância e o tempo de percurso previsto, tempo de funcionamento e consumo de cada componente, consumo total para cada percurso previsto e a autonomia do sistema.

Para conseguir extrair esses valores e chegar a um resultado que possibilite a análise dessa eficiência, se fez necessário implementar um sistema físico considerando diferentes cenários, variando-os em distância e, consequentemente, tempo de percurso. Para implementação física e codificação do sistema, foi necessário definir seu objetivo, levantar as situações às quais o sistema será submetido e modelar o comportamento do mesmo para cada situação.

Para isso, as possíveis situações foram separadas em etapas:

- Acionamento do sistema;
- Rastreamento;
- Busca por outros equipamentos furtados.

Na primeira etapa, o sistema é acionado quando a Corrente Alternada (AC - Alternating Current) que alimenta o equipamento é interrompida. Esse acionamento pode ser realizado com a utilização de um relé. Quando isso ocorre, existem duas possibilidades. Uma delas é a falha na rede elétrica e a outra possibilidade é o furto.

Após o acionamento do sistema, o mesmo envia uma mensagem para o NOC informando o problema. Nesse momento, não é possível identificar qual o motivo da falta de energia. Com isso, para fortalecer o objetivo antifurto do sistema, a mensagem é enviada para que o NOC tenha conhecimento do problema o mais rápido possível. Quanto mais rápido o NOC receber a mensagem, mais rápido poderá averiguar o problema e descobrir, quando for o caso, o furto.

O sistema possui com uma bateria de baixa capacidade e precisa de estratégias que aumentem sua eficiência energética. Por esse motivo, o sistema possui alguns períodos de

pausa (*standby*). Sendo assim, após o envio da mensagem, o sistema entra em *standby*. A partir deste momento, são consideradas duas possibilidades. A primeira corresponde ao (re)estabelecimento da energia que, quando ocorre, faz com que o sistema volte ao seu estado inicial. A segunda possibilidade é a confirmação do furto que acontece com o acionamento do acelerômetro.

Na segunda etapa, a ocorrência do furto é confirmada. Considerando um cenário no qual o equipamento é transportado até um local de armazenamento, o sistema tem a função de informar sua localização periodicamente. Por este motivo, seus módulos de GPS e GSM são ativados e utilizados para que sua localização seja pesquisada e enviada ao NOC.

O objetivo do sistema, como mencionado anteriormente, é servir de isca para descobrir a localização dos pontos de armazenamento e identificar possíveis equipamentos furtados anteriormente e armazenados no mesmo local.

Como o sistema possui uma bateria de baixa capacidade, uma limitação importante do mesmo é seu tempo de funcionamento. Também não é possível prever o tempo de deslocamento entre o local que ocorreu o furto e o local de armazenamento. Sendo assim, após enviar os dados de sua localização no momento em que o deslocamento é iniciado, o sistema entra novamente em *standby* e repete o processo após um tempo pré-estabelecido (trinta minutos nesta dissertação). Dessa forma, o sistema aumenta sua autonomia, aumentando a possibilidade de sucesso no encontro de outros equipamentos, mesmo após grandes deslocamentos.

Na terceira etapa, após chegar ao local de destino e ser armazenado, o leitor RFID é acionado e inicia buscas de outras etiquetas passivas no local. A etiqueta passiva foi escolhida, pois, caso não seja possível rastrear o equipamento por falta de energia, a etiqueta permite que o equipamento acuse sua presença caso algum equipamento energizado seja armazenado no local. Caso encontre, os IDs dessas etiquetas são incluídos na mensagem que é enviada ao NOC. Após o envio, o sistema entra em *standby* e após o tempo de pausa pré-estabelecido, repete as buscas e os envios de informações. Como o sistema completo possui baixo custo, é considerado que todos os equipamentos passíveis de furtos tenham acoplados o sistema completo incluindo além da etiqueta, o leitor RFID.

O fluxograma da Figura 1 mostra, de forma resumida, o comportamento do sistema completo.

Após a definir o sistema que atende as necessidades descritas anteriormente, foi necessário iniciar a construção do protótipo físico e o mesmo foi idealizado considerando o diagrama de blocos da Figura 2.

Na próxima seção, serão apresentadas as tecnologias utilizadas nesse estudo, assim como seus conceitos, funções e características.

Figura 1 - Fluxograma de funcionamento do sistema.

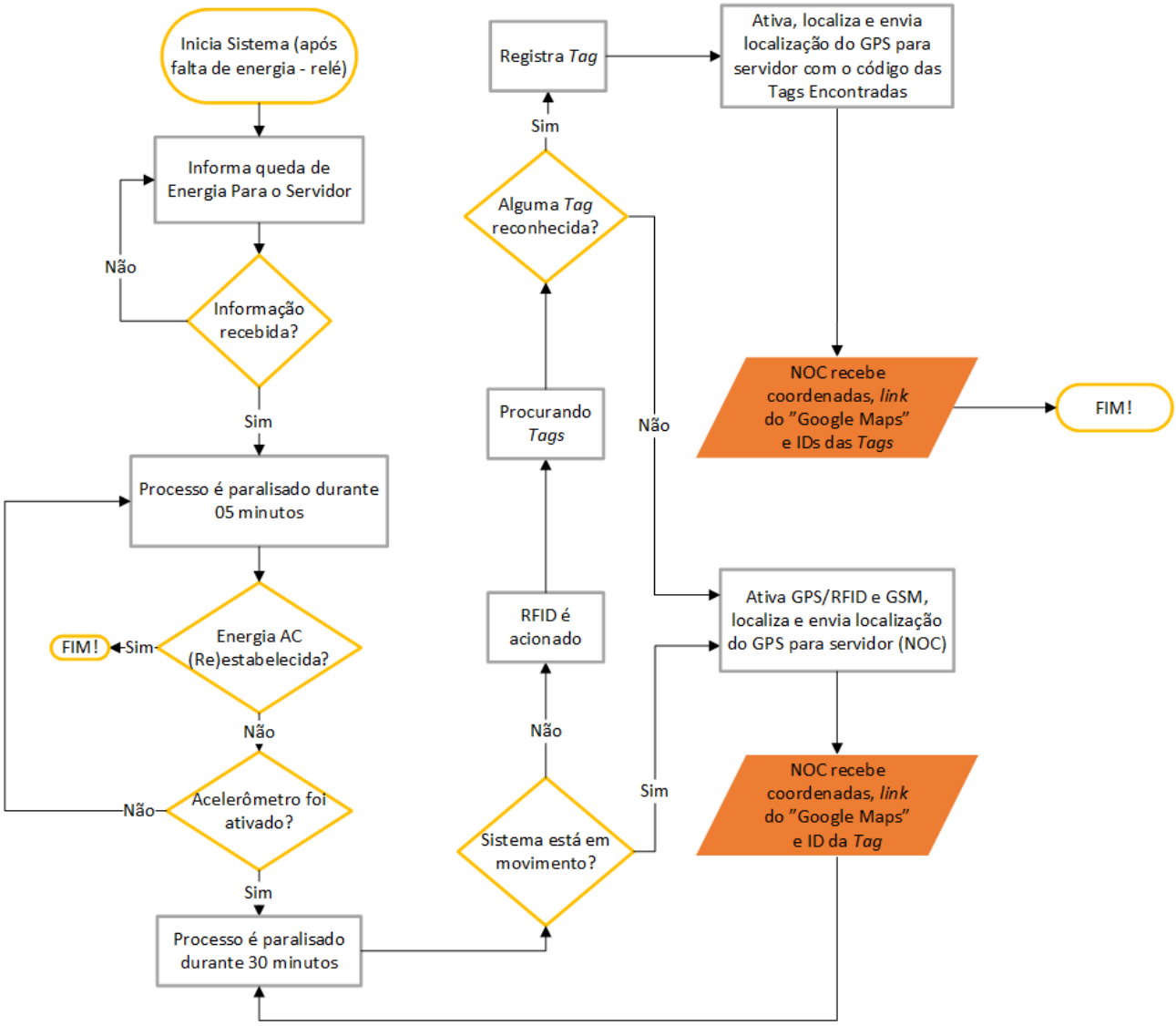
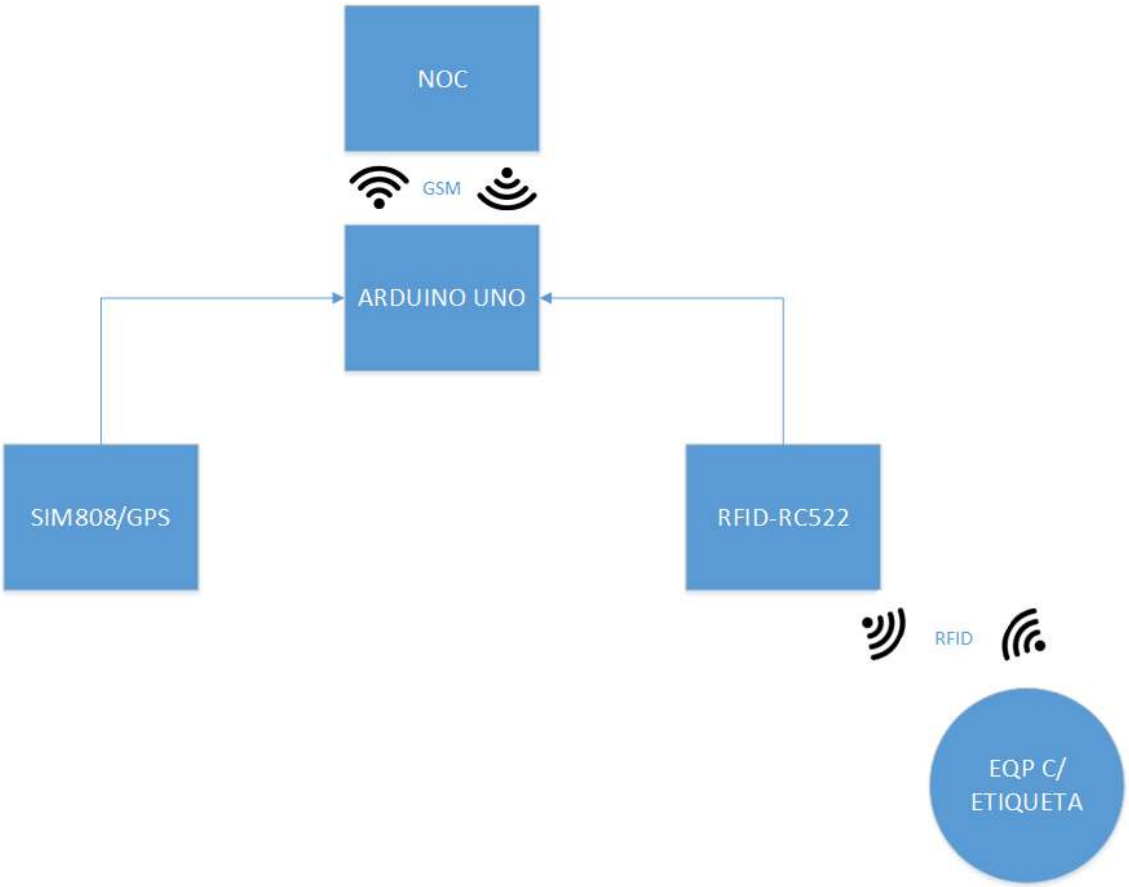


Figura 2 - Diagrama de blocos do sistema.



2.2 Tecnologias e Componentes Utilizados

Essa dissertação foi baseada na combinação das tecnologias de RFID, GSM e GPS. De acordo com (SARDROUD; LIMBACHIYA, 2010), a combinação de RFID com GPS oferece soluções de baixo custo, com identificação de objeto e possibilita a aquisição de dados em áreas que possuem difícil acesso. Ainda segundo (SARDROUD; LIMBACHIYA, 2010), o RFID integrado com o GPS possibilita a coleta e a transmissão de dados usando pouca ou nenhuma mão de obra.

Considerando as tecnologias que foram escolhidas, nesta seção, serão apresentadas algumas definições e conceitos sobre cada uma delas. Também será apresentado, um breve resumo sobre cada *hardware* utilizado nos testes, incluindo justificativas para as escolhas realizadas.

Para implantação do sistema, foi utilizada uma placa com leitor RFID, uma placa com GSM, uma placa com GPS, antenas, uma plataforma de desenvolvimento (microcontrolador) e uma bateria. Os modelos de *hardwares* utilizados são:

- Leitor RFID - RC522;
- Etiqueta Passiva RFID;
- GSM/GPS - SIM808 EVB-V3.2;
- Plataforma de Desenvolvimento - Arduino Uno R3;
- Bateria - ELGIN 9V Recarregável.

2.2.1 Hardware RFID

A RFID é uma tecnologia utilizada para identificar, rastrear e gerenciar materiais, produtos e até mesmo animais ou indivíduos, sem contato e sem a necessidade de um campo visual (MARQUES et al., 2009). O objetivo dessa tecnologia é melhorar a eficiência no rastreamento e na localização de produtos. Essas características atendem parte das necessidades que a proposta dessa dissertação possui e, por este motivo, essa tecnologia foi escolhida.

Segundo (FILHO, 2012), a tecnologia RFID possibilita a leitura de itens que não estejam próximos do leitor, além da leitura simultânea de cerca de mil itens em apenas um segundo. Essa característica garante o funcionamento do sistema, quando o leitor tiver mais de uma etiqueta em seu alcance. Nos testes realizados com o protótipo desta dissertação, foram utilizadas apenas duas etiquetas, por questões de custo.

(GLOVER; BATH, 2007) cita que a utilização da tecnologia se tornou mais intensa para registros de vagões ferroviários, na identificação de chassis de automóveis, na linha

Figura 3 - Diagrama de funcionamento do leitor RFID.

de montagem e também, para registrar criação de gado. Em (GLOVER; BATH, 2007), algumas utilidades para o RFID foram levantadas:

- redução dos custos com estoques devido a maior controle, rastreabilidade e segurança;
- rastreabilidade via internet e mais informações sobre os produtos podem ser obtidas com maior facilidade.

Ambas utilidades estão alinhadas com essa dissertação, pois, além do rastreamento, será possível reduzir custos causados por furtos.

A Figura 3 apresenta um diagrama com o funcionamento de um sistema RFID. Nessa figura, é possível verificar que o leitor transmite um sinal e quando há uma etiqueta próxima, ela recebe o sinal e o utiliza como fonte de energia respondendo com o seu código (ID) pré-definido e único. O leitor recebe esses dados de diferentes etiquetas e os envia diretamente para o seu servidor. Como cada RFID é composto por um código único, o servidor consegue identificar e nomear cada etiqueta.

Segundo o *datasheet* do componente (NXP SEMICONDUCTORS, 2011), o alcance do mesmo deve chegar a 50 mm. O Leitor RFID RC522, utilizado para as análises desta dissertação, é baseado no chip MFRC522 da empresa NXP. Esse módulo é altamente utilizado em comunicação sem contato a uma frequência de 13,56 MHz. Esse módulo, além de pequeno, possui baixo consumo e permite ler e escrever, sem necessidade de contato, em etiquetas que seguem o padrão Mifare, uma tecnologia RFID desenvolvida pela Phillips Semiconductors (hoje NXP Semiconductors) que atende à ISO-14443 (NXP SEMICONDUCTORS, 2018). O cartão utilizado no experimento possui 1 kB de capacidade, porém, etiquetas menores são facilmente encontradas no mercado. As capacidades das etiquetas disponibilizadas são de no mínimo 96 bits conforme (ISO18000-6, 2010), podendo chegar a 2 ou 4 kB. As etiquetas possuem dados de fábrica, como número de série e ID. O código desenvolvido no Arduino para a integração do módulo RFID no sistema de rastreamento está apresentado no Apêndice A.2 e foi baseado em tutoriais de internet (INDULA, 2017a), (INDULA, 2017b) e (LOPES, 2017).

2.2.2 Hardware GSM/GPS

O GSM é um sistema que contempla dois canais de comunicação (*uplink* e *downlink*) entre o terminal móvel e o elemento de rede – BTS (*Base Transceiver Station*), que possui antenas que garantem a cobertura. As bandas de frequências especificadas para o GSM são 890-915 MHz para o canal de *uplink* e 935-960 MHz para o canal *downlink* (LOURENÇO; ISPGAYA; INESC-UTOE, 2000). O GSM é utilizado no sistema proposto para comunicação entre um leitor RFID e o Centro de Operações de Rede.

O GPS é um sistema composto por uma constelação de satélites, orbitando em torno da Terra a uma altura aproximada de 20200 km acima do nível do mar (ALVES, 2006). O sistema consiste em:

- um segmento espacial (satélites);
- um segmento de controle (estações terrestres de gerenciamento);
- um segmento do usuário.

Os satélites e o receptor (segmento de usuário) possuem um relógio interno. Cada um dos satélites transmite um sinal que contém o horário que o mesmo foi enviado. O receptor na Terra (segmento do usuário) recebe esses sinais e utiliza as diferenças entre os horários recebidos e o horário de seu relógio interno para calcular a localização do receptor (MONICO, 2000). No sistema proposto, o GPS é utilizado para identificar a localização dos objetos furtados.

O módulo GSM/GPS SIM808, utilizado nos testes e análises desta dissertação,

utiliza a tecnologia GSM para comunicação com a rede móvel juntamente com a tecnologia GPS para navegação por satélite. A placa apresenta um consumo de energia muito baixo. O receptor GPS é bastante sensível com 22 canais de rastreamento e 66 de aquisição. Também suporta a tecnologia GPS assistido (A-GPS) para localização em ambientes internos (SHANGHAI SIMCOM WIRELESS SOLUTIONS LTD, 2014). A placa é controlada pelo comando AT via UART e suporta alimentação de 3,3 ou 5 V. O código desenvolvido no Arduino para integração do módulo GSM/GPS SIM808 está apresentado no Apêndice A.2.

2.2.3 Microcontrolador - Arduino Uno

O Arduino é uma plataforma *open-hardware* e possui seu próprio ambiente de desenvolvimento baseado na linguagem C (MCROBERTS, 2018). O Arduino Uno R3 é uma plataforma de desenvolvimento que utiliza o microcontrolador ATmega328. Ele possui 14 pinos de entrada/saída digital, seis entradas analógicas, um cristal oscilador de 16 MHz, uma conexão USB, uma entrada de alimentação, uma conexão ICSP e um botão de reset. Ele contém todos os componentes necessários para suportar o microcontrolador e pode ser alimentado pela porta USB, por uma fonte ou por uma bateria. Dentre os seus pinos, destacam-se ainda os seguintes: GND, Vin, 3,3 V e 5 V.

Na próxima seção, a metodologia de medições e testes que foi utilizada será apresentada com o intuito de elucidar como alguns dados foram obtidos. Também será apresentado o sistema consolidado

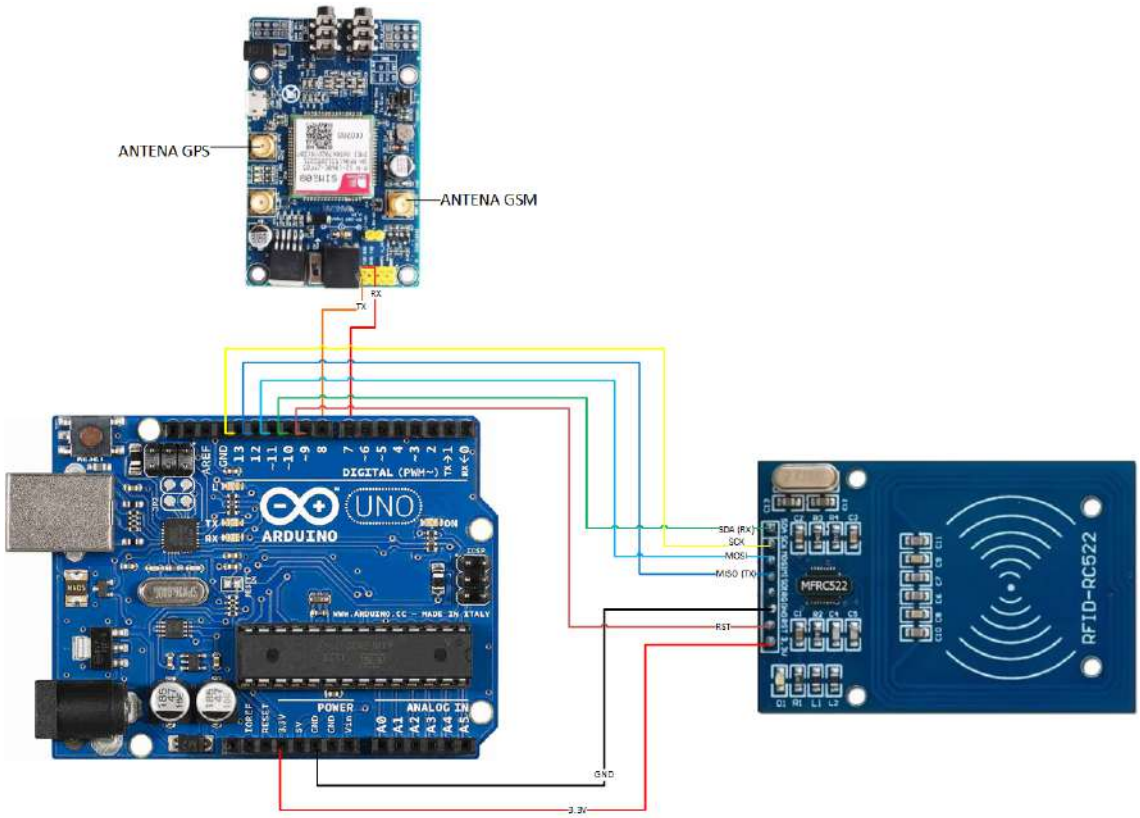
2.3 **Metodologia Aplicada nas Medições**

O protótipo do sistema foi implantado com o objetivo de obter dados como a corrente consumida e verificar a viabilidade do protótipo do sistema com os componentes utilizados.

O primeiro teste teve como objetivo verificar o funcionamento do rastreador. Um protótipo foi montado conforme as imagens do Apêndice B. Após verificar o funcionamento, o sistema foi implantado por completo. As etiquetas RFID passivas foram inseridas próximas ao leitor para validar que ambas poderiam ser lidas. Após serem identificadas, o sistema enviou uma mensagem para um telefone celular (ver o Apêndice B).

Após os testar as funcionalidades, as medições de corrente foram realizadas. Para realizar as medições, um multímetro DT830B foi utilizado. As medições foram realizadas após o acionamento do sistema, no sistema por completo e por componente. Os módulos

Figura 4 - Conexões entre os módulos.



RFID, GPS e GSM foram medidos enquanto ativos e também enquanto estavam em *standby*.

Em todos os casos, a maior corrente foi considerada, pois, dessa forma, o sistema não seria favorecido em nenhum momento.

2.3.1 Sistema Consolidado

Nesta seção, o sistema prático que foi implementado é apresentado em etapas. O sistema possui as funções e as características apresentadas no fluxograma da Figura 1. A primeira etapa corresponde à elaboração do diagrama de blocos apresentado na Seção 2.1. Após os estudos sobre cada componente e a confecção dos códigos de cada módulo, os mesmos foram conectados conforme a Figura 4.

Durante as análises e para avaliar o consumo, limitações e realizar os testes, o sistema foi implementado em partes. Primeiro os testes foram realizados considerando apenas a parte de rastreamento. Nessa etapa, foram utilizados o módulo GPS/GSM (SIM808), o microcontrolador Arduino Uno R3 e para simular o NOC, foi utilizado um celular com linha pré-paga para receber as mensagens. Os testes dessa etapa, foram

realizados localizando o equipamento via GPS e confirmando o recebimento da mensagem no celular, apontando a coordenada correta do local.

Em uma segunda etapa o sistema foi implantado por completo. Para isso, foi acoplado ao Arduino, o módulo RFID. Para teste dessa etapa, foram utilizadas duas etiquetas RFIDs. Ambas funcionavam normalmente entre 0 e 30 mm de distância. Em um primeiro momento, o teste se limitou a ler uma das etiquetas e enviar sua localização para o celular informando na mensagem, o ID da etiqueta e as coordenadas da localização. Em um segundo momento, outra etiqueta foi incluída no teste de forma a enviar os IDs das duas etiquetas junto às suas localizações.

Em um cenário real, os equipamentos são colocados em funcionamento pela operadora em determinada estação, normalmente abrigados por edículas, contêineres e gabinetes. A proposta desta dissertação é acoplar o sistema no maior número de equipamentos, antes de suas ativações. Caso um equipamento seja furtado, a primeira consequência seria a interrupção da energia no equipamento; por este motivo, um dispositivo que consiga identificar essa queda de energia se faz necessário. No protótipo implementado nesta dissertação, não foram utilizados relés; no entanto, o componente é aqui sugerido, pois possui custo baixo e é eficiente para esse tipo de ação. Os testes realizados foram iniciados pressupondo o acontecimento do roubo. Após a identificação da queda da energia, uma fonte de alimentação portátil precisa ser acionada, por este motivo, a bateria é essencial. Após desligar o equipamento e fazer sua desinstalação (furto), o próximo passo seria levar o equipamento para outra localidade. Sendo assim, um rastreador se faz necessário. Para que o sistema ganhe uma maior autonomia e maior tempo em seu rastreamento é sugerido nesta dissertação, o uso de acionamento por acelerômetro; dessa forma é possível reduzir o consumo da bateria em alguns momentos durante o percurso, pois, o mais importante é que o sistema chegue ativo ao seu destino para que possa enviar sua localização e pesquisar a existência de outros equipamentos no local. Em uma próxima etapa, o equipamento chegaria ao seu destino com o rastreador tornando possível identificar sua localização. Porém, como citado anteriormente, normalmente, esses furtos são realizados por grupos que possuem pontos de coleta. Sendo assim, a proposta inclui também obter informações a respeito do tipo de furto (se ocasional ou se realizado por grupos e quadrilhas especializadas). Por este motivo, um leitor RFID foi adicionado ao sistema, para que possa fazer varreduras no local onde foi armazenado e caso identifique outro(s) equipamento(s) (via etiqueta(s) RFID), informe ao NOC quais equipamentos foram encontrados e se é um possível ponto de coleta de quadrilhas especializadas. Dessa forma, o equipamento além de ser rastreável, também se torna uma isca para que, além dele, outros equipamentos também possam ser recuperados.

A próxima seção, descreve como os testes foram realizados e a corrente utilizada por cada módulo.

2.4 **Testes Realizados**

Foi utilizada nos testes e análises uma bateria recarregável da ELGIN de 9 V com capacidade de 380 mAh. O sistema possui basicamente três módulos que consomem energia. Esses módulos são o Arduino (Placa de Desenvolvimento), a placa SIM808 (GSM/GPS) e o leitor RFID. No entanto, o consumo de cada placa varia conforme a maneira como são utilizadas. Foram realizadas medições de corrente do sistema utilizando um multímetro. O leitor RFID possui dois estados no sistema proposto: "ativo e pesquisando" e *"standby"*. O estado ativo e pesquisando corresponde ao momento em que o leitor RFID está buscando etiquetas. O estado *standby* está relacionado ao momento em que, mesmo estando ligado, o leitor não está realizando leituras. Verificando a corrente, obteve-se 13 mA para o *standby* e 26 mA para o ativo e pesquisando.

A placa GSM/GPS também possui dois estados no sistema proposto: "ativo e pesquisando" e *"standby"*. O estado ativo e pesquisando está relacionado ao momento em que a placa está buscando sua localização via GPS e transmitindo informações via GSM. O estado *standby* corresponde ao momento em que, mesmo estando ligada, a placa não está buscando localização, nem transmitindo informações. Verificando a corrente nesses dois cenários, obteve-se 41,5 mA para o *standby* e 68 mA para o ativo e pesquisando.

Considerando-se que o Arduino permanecerá sempre ligado, seu consumo de corrente foi medido durante todo o processo e com todos os módulos conectados. Foi atingida uma corrente máxima de 45,5 mA com variações de até 0,7 mA (para menos) entre as diferentes etapas do sistema. Porém, o sistema também propõe a utilização de um acelerômetro para identificar os momentos em que o equipamento está em movimento. Segundo (ONE TECHNOLOGY WAY, 2010), o acelerômetro modelo ADXL377 possui uma corrente máxima próxima a 1 mA. Dessa forma, essa corrente foi agregada à do Arduino, gerando então uma corrente máxima de 46,5 mA. Como o módulo Arduino não entra em *standby*, foi considerada sua corrente máxima em todos os cálculos.

A Tabela 1 apresenta a corrente máxima medida no sistema em funcionamento. Conforme essa Tabela 1, a corrente total do sistema pode chegar a 140,5 mA. A autonomia total do sistema, considerando o consumo máximo durante todo o tempo e a bateria utilizada, é de duas horas e quarenta e dois minutos. No entanto, também é possível verificar, na Tabela 1, que o módulo GSM/GPS - SIM808 funciona em até 41,5 mA quando está em *standby*. Da mesma forma, o leitor RFID funciona em até 13 mA quando está em *standby*. No período em que o módulo GSM/GPS e RFID permanecem em *standby* o sistema reduz a corrente para 101 mA. Considerando o sistema sempre em *standby*, o mesmo poderia permanecer ativo por até três horas e quarenta e cinco minutos, conforme detalhado na Seção 4.2.

Tabela 1 - Corrente por placa ou módulo.

Placa	Corrente - Ativo e Pesquisando (mA)	Corrente - standby (mA)
Arduino Uno R3	46,5	46,5
RFID - RC522	26	13
GSM/GPS - SIM808	68	41,5
Corrente Total	140,5	101

Tabela 2 - Valor do sistema em relação ao valor de mercado dos equipamentos furtados.

Módulo	Valor de Mercado
Arduino Uno R3	R$ 27,50
RFID - RC522	R$ 18,90
GSM/GPS - SIM808	R$ 167,49
Valor Total	R$ 213,89

2.5 **Custo do Sistema**

Nesta seção, o custo do protótipo foi levantado e comparado com alguns equipamentos utilizados pelas operadoras de telecomunicações no Brasil. Segundo (POUSOALEGRE.NET, 2018) e (SKODOWSKI; SARZI, 2016), um dos destinos dos equipamentos furtados são pequenos provedores de internet. Sendo assim, apenas equipamentos de transmissão como rádios e roteadores foram considerados.

Na Tabela 2, são apresentados os valores dos componentes utilizados nesta dissertação.

Na Tabela 3, são apresentados os valores de alguns tipos diferentes de equipamentos utilizados pelas grandes operadoras de telecomunicações no Brasil e os percentuais desses valores em relação ao custo total do protótipo[1].

Considerando as Tabelas 2 e 3, é possível verificar que o valor do protótipo utilizado nesta dissertação não chega a 0,8% do valor do equipamento mais barato. Na próxima seção, o sistema completo que foi implementado será apresentado.

No próximo capítulo, serão realizadas análises probabilísticas do sistema. O mesmo possui propriedade markoviana, ou seja, o sistema possui diferentes estados que transitam entre si e seu desenvolvimento futuro depende somente do estado presente, não levando em consideração seus estados passados (GRIGOLETTI, 2011). Sendo assim, as análises serão realizadas utilizando cadeia de Markov para que seja possível calcular de forma

[1] Os equipamentos apresentados na Tabela 3 são equipamentos utilizados por uma das grandes operadoras do Brasil e os valores aproximados foram obtidos com o fabricante em 2017.

Tabela 3 - Valor de mercado de equipamentos utilizados pelas grandes operadoras de telecomunicações e percentual desse valor em relação ao custo do sistema.

Tipo de Equipamento	Valor de Mercado	Percentual desse Valor em relação ao custo do Protótipo
Rádio Pequeno Porte	R$ 27.000,00	0,79%
Rádio Médio Porte	R$ 42.000,00	0,51%
Rádio Grande Porte	R$ 150.000,00	0,14%
Roteador Pequeno Porte	R$ 37.000,00	0,58%
Roteador Médio Porte	R$ 45.000,00	0,48%
Roteador Grande Porte	R$ 60.000,00	0,36%

probabilística as transições entre os estados. Dessa forma, pode-se avaliar a probabilidade de se obter sucesso no rastreamento desses equipamentos.

3 CADEIA DE MARKOV DO SISTEMA

Neste capítulo, a cadeia de Markov do sistema será apresentada em etapas. Na Seção 3.1, os estados serão detalhados. Na Seção 3.2, os estados da cadeia de Markov serão codificados de acordo com os *status* de cada módulo do sistema. Na Seção 3.3, as transições entre estados serão definidas e a cadeia de Markov será consolidada.

3.1 Estados da Cadeia de Markov

Baseando-se no cenário apresentado na Seção 2.3.1, possíveis estados foram levantados:

- **Estado A - Início**: Este é o estado inicial e representa o momento em que o equipamento ainda não foi furtado e permanece energizado. Neste momento, nenhum módulo é ativado, pois o relé ainda não foi acionado. A partir desse estado, as transições possíveis são para os estados F e B;
- **Estado B - Interrupção sem furto**: Foi considerada nesta dissertação a hipótese de o relé ser acionado por falha na rede elétrica. Por este motivo, o estado B foi considerado. Neste estado, a energia foi interrompida, o relé foi acionado e, mesmo não sendo furto, a falha de energia é informada ao NOC. Caso seja confirmada a falha na rede elétrica, após (re)estabelecida, a bateria é novamente (re)carregada. A partir desse estado, a única transição possível é voltar para o estado A;
- **Estado F - Interrupção após furto**: Este é o estado em que ocorre o furto. Neste estado, o acelerômetro é acionado, pois o equipamento entrou em movimento. A partir desse estado, as transições possíveis são para os estados G, E e C;
- **Estado C - Envia mensagens do galpão sem RFID vinculado**: Neste estado, o equipamento já não está mais em movimento, ou seja, já chegou ao local de destino. Está enviando mensagens ao NOC, porém, neste momento, nenhum RFID foi encontrado. A partir desse estado, as transições possíveis são para os estados G, E e D;
- **Estado D - Entra em Standby no Galpão**: Este estado representa o momento em que, após chegar ao local e não encontrar outras etiquetas RFID e enviar mensagem ao NOC, o equipamento entra em *standby* para poupar energia. A partir desse estado, as transições possíveis são para os estados G, E e C;

Tabela 4 - *Status* de cada estado da cadeia de Markov.

Estados	Equipamento em movimento	Módulos GSM/GPS e RFID ativos	Enviando mensagens	RFID vinculado
A - Início	Não	Não	Não	Não
B - Interrupção sem furto	Não	Não	Sim	Não
C - Sistema no galpão envia mensagem sem RFID vinculado	Não	Sim	Sim	Não
D - Sistema no galpão entra em *standby*	Não	Sim	Não	Não
E - Sucesso	Não	Sim	Sim	Sim
F - Interrupção após furto	Sim	Não	Não	Não
G - Sistema sem bateria	Não (sem bateria)	Não (sem bateria)	Não (sem bateria)	Não (sem bateria)

- **Estado E - Sucesso**: Este é o estado de sucesso do sistema. Neste estado, após chegar ao local de armazenamento, encontra outra(s) etiqueta(s) RFID e envia mensagem ao NOC com sua localização e com o(s) ID(s) encontrado(s). Esse é um dos estados absorventes, logo, o sistema não deixará esse estado;

- **Estado G - Sem bateria**: Este é o estado de insucesso do sistema. Neste estado, a energia da bateria se esgota. Esse é um dos estados absorventes, logo, o sistema não deixará esse estado;

Como citado anteriormente, o estado E é referente ao momento em que outras etiquetas são encontradas. A principal proposta dessa dissertação é fazer com que o equipamento furtado, se torne uma isca e torne possível o proprietário encontrar equipamentos roubados e locais de armazenamentos destes equipamentos. Por este motivo, este estado foi definido como estado de sucesso do sistema.

Os estados E e G são os estados denominados absorventes. Após um número finito de transições, o sistema entrará em um desses estados e nele ficará definitivamente (GRIGOLETTI, 2011), (NOGUEIRA, 2008) e (HILLIER; LIEBERMAN, 2013).

O sistema possui sete estados, sendo dois deles absorventes. Na Tabela 4, é possível verificar os *status* de cada módulo do sistema em relação a cada estado. São levados em consideração se o equipamento está em movimento (sim ou não), se os módulos GSM/GPS e RFID estão ativados ou não, se o sistema está enviando uma mensagem (sim ou não) e, por último, se o sistema encontrou outra(s) etiqueta(s) RFID no local (característica denominada "RFID vinculado").

Na próxima seção, é apresentada a codificação utilizada na cadeia de Markov do sistema.

Tabela 5 - Codificação preliminar dos estados da cadeia de Markov.

Estados	Equipamento em Movimento	Módulos GSM/GPS e RFID Ativos	Enviando Mensagem	RFID Vinculado
A - Início	0	0	0	0
B - Interrupção sem furto	0	0	1	0
C - Sistema no galpão envia mensagens sem RFID vinculado	0	1	1	0
D - Sistema no galpão entra em *standby*	0	1	0	0
E - Sucesso	0	1	1	1
F - Interrupção após furto	1	0	0	0
G - Sistema sem bateria	0	0	0	0

3.2 **Codificação dos Estados da Cadeia de Markov**

Para facilitar o entendimento da cadeia de Markov do sistema, foi criada uma codificação preliminar conforme a Tabela 5. O *bit* 1 representa um "Sim" para uma das características apresentadas anteriormente na Tabela 4. O *bit* 0 representa um "Não".

A partir da codificação anterior, foi criada uma nova codificação que inclui um quinto bit representando se o sistema foi acionado ou não. Dessa forma, cada estado possui cinco *bits* que retratam os seguintes itens:

- o sistema foi acionado?
- o equipamento está em movimento?
- os módulos GSM/GPS e RFID estão ativos?
- o sistema está enviando mensagens?
- o RFID está vinculado?

O estado A é, por concepção, o único estado inicial. A codificação para cada estado é:

- Estado A - Início - 0,0,0,0,0;
- Estado B - Interrupção sem furto - 1,0,0,1,0;
- Estado C - Envia mensagem do galpão sem RFID vinculado - 1,0,1,1,0;

- Estado D - Entra em *standby* no galpão - 1,0,1,0,0;
- Estado E - Sucesso - 1,0,1,1,1;
- Estado F - Interrupção após furto - 1,1,0,0,0;
- Estado G - Sem bateria - 1,0,0,0,0.

Na próxima seção, as possíveis transições entre estados serão apresentadas e utilizando a codificação apresentada anteriormente, a cadeia de Markov do sistema será consolidada.

3.3 Consolidação da Cadeia de Markov do Sistema

Nas seções anteriores, foram definidos os estados da cadeia de Markov e os mesmos foram codificados para facilitar o entendimento e a apresentação gráfica da cadeia.

Para consolidar a cadeia, é preciso definir quais as possíveis transições que nela ocorrem. E para utilizar a cadeia de Markov para fazer uma análise probabilística, algumas definições foram consideradas. São elas:

- A probabilidade de a bateria apresentar problemas é zero;
- Em algum momento, existe a ocorrência do furto;
- Após ocorrência do furto, é suposto que o equipamento seja despachado diretamente para o local de armazenamento (galpão), sem estados entre esses momentos.

As possíveis transições entre estados são:

- **De A para B - Transição do estado inicial para o estado de interrupção sem furto**: quando ocorre falha da rede elétrica;
- **De B para A - Transição do estado de interrupção sem furto para o estado inicial** : quando a rede elétrica é (re)estabelecida;
- **De A para F - Transição do estado inicial para o estado de interrupção após furto**: quando ocorre o furto e o equipamento entra em movimento;
- **De F para G - Transição do estado de interrupção após furto para o estado de sistema sem bateria**: quando a bateria acaba;
- **De F para E - Transição do estado de interrupção após furto para estado de sucesso**: quando após chegar ao local de armazenamento, identifica outro(s) equipamento(s) imediatamente;

- **De F para C - Transição do estado de interrupção após furto para estado onde o sistema está no galpão e envia mensagem sem RFID vinculado**: quando após chegar ao local de armazenamento, outro equipamento não é identificado em um primeiro momento e o sistema informa apenas sua localização ao NOC;

- **De C para D - Transição do estado onde o sistema está no galpão e envia mensagem sem RFID vinculado para o estado onde o sistema está no galpão e entra em *standby***: quando após busca por outras etiquetas sem sucesso e envio de informações, sistema entra em *standby* para economizar energia e ter oportunidade de fazer nova varredura em outro momento;

- **De C para E - Transição do estado onde o sistema está no galpão e envia mensagem sem RFID vinculado para o estado de sucesso**: quando após busca de outras etiquetas sem sucesso e envio de informações ao NOC, sistema encontra outro(s) RFID(s) e (re)faz a transmissão de informações;

- **De C para G - Transição do estado onde o sistema está no galpão e envia mensagem sem RFID vinculado para o estado onde a bateria do sistema acaba**: quando a bateria acaba;

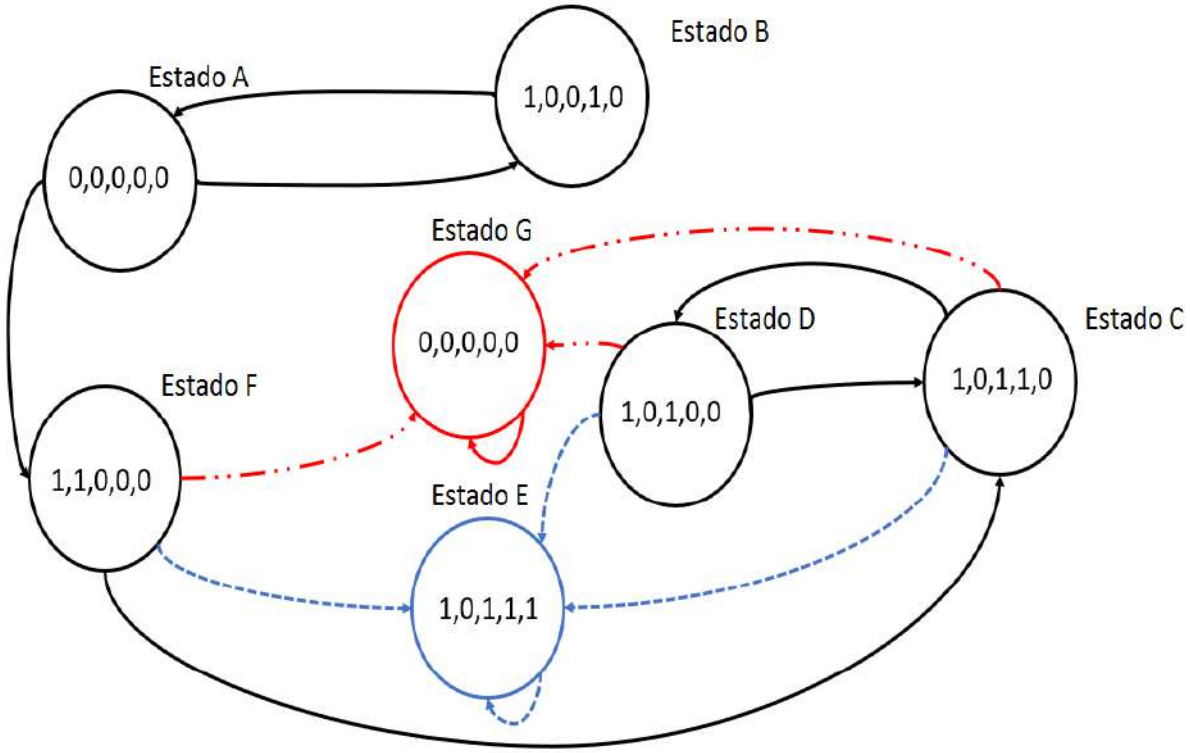
- **De D para G - Transição do estado onde o sistema está no galpão e entra em *standby* para o estado onde a bateria do sistema acaba**: quando a bateria acaba;

- **De D para C Transição do estado onde o sistema está no galpão e entra em *standby* para o estado onde o sistema está no galpão e envia mensagem sem RFID vinculado**: quando após busca de outras etiquetas sem sucesso, envio de informações ao NOC e entrada em *standby*, retoma a varredura e novamente não tem sucesso;

- **De D para E - Transição do estado onde o sistema está no galpão e entra em *standby* para o estado de sucesso**: quando após busca de outras etiquetas sem sucesso, envio de informações ao NOC e entrada em *standby*, retoma a varredura e encontra outra(s) etiquetas e (re)envia uma mensagem com novo(s) ID(s) vinculado(s).

- **De G para G - Estado absorvente onde o sistema se encontra sem bateria**: o estado G é um estado absorvente. Quando o sistema chega a esse estado, significa que sua bateria acabou, logo, após entrar nesse estado, o sistema chega ao fim do seu ciclo.

Figura 5 - Cadeia de Markov do sistema.



- **De E para E - Estado absorvente de sucesso onde o sistema encontra outros equipamentos, vincula ID e envia o mesmo**: o estado E é um estado absorvente. Quando o sistema chega a esse estado, significa que o local de armazenamento foi localizado, existem outros equipamentos furtados no local e o sistema conseguiu identificá-lo. Logo, o sistema atingiu seu propósito.

Os estados citados anteriormente e suas respectivas transições estão apresentados graficamente na Figura 5.

Na cadeia da Figura 5, é importante destacar que o estado E (representado em azul) corresponde ao estado de sucesso, ou seja, neste estado é possível identificar outro RFID que tenha sido furtado anteriormente e armazenado no mesmo local. Já o estado G (representado em vermelho) é o estado no qual o sistema apresenta falha ou insucesso, pois a autonomia do sistema foi menor que o necessário. No próximo capítulo, serão apresentados o método, os testes e análises realizadas utilizando a cadeia de Markov.

4 ANÁLISES PROBABILÍSTICAS UTILIZANDO CADEIA DE MARKOV

Neste capítulo, serão apresentadas as análises probabilísticas em dois cenários distintos. O primeiro é o cenário que considera nula a probabilidade de acabar a energia durante o percurso. O segundo é o cenário em que, utilizando estações reais, existe a probabilidade de acabar a energia do sistema durante o percurso. Os cálculos probabilísticos foram realizados utilizando cadeia de Markov. Para isso, foi utilizada uma ferramenta desenvolvida na Universidade de Otterbein (DENVER; HARPER, 1999) que possibilita calcular as probabilidades considerando infinitas transições.

4.1 Análises Realizadas Considerando Variação nas Probabilidades

Inicialmente, foram variadas algumas probabilidades de transição entre estados enquanto outras foram mantidas fixas. Os cálculos estatísticos também foram realizados considerando as probabilidades reais de furto.

Conforme a Tabela 6[2], no período de dois anos, entre fevereiro de dois mil e dezessete e fevereiro de dois mil e dezenove, a estação de PMC sofreu interrupções sessenta vezes, sendo uma delas por furto e as restantes por falta de energia. No mesmo período, a estação de VRC parou de operar quarenta e oito vezes, sendo uma delas por furto. Ou seja, dado que ocorra uma interrupção em PMC, a probabilidade de a mesma ser proveniente de furto é de 1,67%. Dessa forma, dado que ocorra uma interrupção no site VRC, a probabilidade de a mesma ser proveniente de furto é de 2,13%.

Por este motivo, considerando a estação de PMC, as probabilidades do estado A para o estado B e do estado A para o estado F foram fixadas em 98,33% e 1,67% respectivamente. Considerando a estação de VRC, as probabilidades do estado A para o estado B e do estado A para o estado F foram fixadas em 97,87% e 2,13% respectivamente. A probabilidade de ocorrer transição do estado B para o estado A, foi fixada em 1, pois, após chegar ao estado B, voltar ao estado A é a única transição possível. Após chegar ao estado C, o sistema possui três possíveis transições. Uma delas é a transição para o estado G, outra para o estado E e outra para o estado D. A transição para o estado G é uma das transições que foram variadas, logo, as probabilidades para as transições do estado C para o estado E e do estado C para o estado D foram definidas de acordo com a variação

[2] Os dados da tabela foram obtidos diretamente com a operadora que atua na estação, em um sistema de controle interno, e utilizando o indicador FIC (Frequência de interrupção individual), que corresponde ao número de interrupções ocorridas, disponibilizado na conta de energia de cada estação.

Tabela 6 - Número de ocorrências de falhas de energia e furtos nas estações de PMC e VRC nos últimos dois anos.

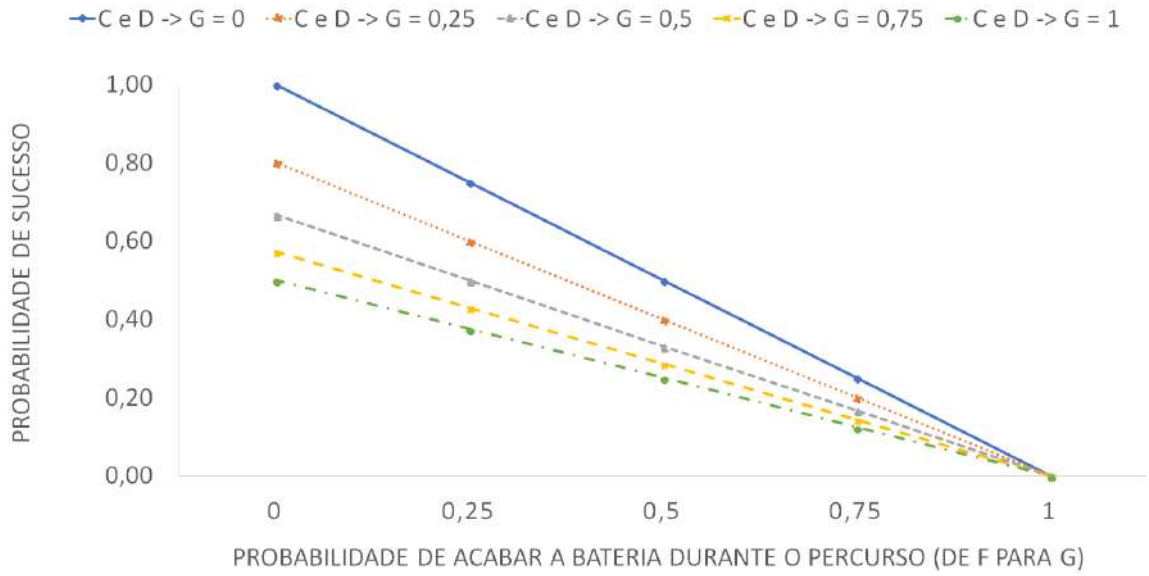
Estação	Falhas de Energia	Furtos Registrados
PMC	59	1
VRC	47	1

de C para G. Por exemplo, se a probabilidade de C transitar para G for igual a X, então define-se, $(1-X)/2$ como probabilidade de C transitar para E e C transitar para D. Após chegar ao estado D, o sistema também possui três possíveis transições. Uma delas é a transição para o estado G, outra para o estado E e outra para o estado C. A transição para o estado G é uma das transições que foram variadas, logo, as probabilidades para as transições do estado D para o estado E e do estado D para o estado C foram definidas de acordo com a variação de D para G. Por exemplo, se a probabilidade de D transitar para G também for igual a X, então define-se, $(1-X)/2$ como probabilidade de D transitar para E e D transitar para C. Da mesma forma, ao chegar ao estado F, o sistema também possui três possíveis transições. Uma delas é a transição para o estado G, outra para o estado E e outra para o estado C. A transição para o estado G é uma das transições que foram variadas, logo, as probabilidades para as transições do estado F para o estado E e do estado F para o estado C foram definidas de acordo com a variação de F para G. Por exemplo, se a probabilidade de F transitar para G for igual a Y, então define-se, $(1-Y)/2$ como probabilidade de F transitar para E e F transitar para C.

O objetivo é calcular a probabilidade de sucesso do sistema, ou seja, a probabilidade de o estado E ser alcançado. Os valores utilizados na variação foram escolhidos para que o comportamento da curva de probabilidade de sucesso do sistema fosse determinado considerando-se diferentes cenários. A probabilidade de acabar a bateria foi variada. As probabilidades de transição dos estados C e D para o estado G foram consideradas iguais e variadas de 0 a 1 em intervalos de 0,25, correspondendo aos casos nos quais a bateria acaba após chegar ao local de armazenamento. A probabilidade de transição do estado F para o estado G também foi variada, correspondendo ao caso em que a bateria acaba durante o percurso até o local de armazenamento.

Antes de utilizar a ferramenta desenvolvida na Universidade de Otterbein (DENVER; HARPER, 1999), foram realizados testes de sanidade do sistema. Para isso, a probabilidade de acabar a bateria durante o percurso foi considerada 1. E como pode ser verificado no gráfico da Figura 6, o resultado esperado foi apresentado pela ferramenta, pois, a taxa de sucesso nesse teste foi igual a 0. Outro teste realizado, foi considerar as probabilidades de acabar a bateria no percurso e após chegar ao local de armazenamento, iguais a 0. Dessa forma, é possível observar também no gráfico da Figura 6, que quando, ambas probabilidades são 0, a probabilidade de sucesso é igual a 1.

Figura 6 - Probabilidade de sucesso do sistema em função da probabilidade de acabar a bateria durante o percurso.



Considerando que o tempo de funcionamento do sistema tenda ao infinito existe uma probabilidade de o sistema ficar transitando eternamente entre os estados C e D, onde o sistema busca por alguma etiqueta RFID no local armazenado, não encontra e entra em *standby*. No entanto, nesta dissertação, foi considerado que o sistema trabalha dentro de sua autonomia e que em algum momento encontrará outra etiqueta RFID.

A partir da Figura 6, é possível observar que, mesmo considerando o pior cenário, o sistema ainda apresenta 50% de chance de sucesso, ou seja, de chegar ao local de armazenamento e encontrar um ou mais RFIDs. Neste caso, para ilustrar o pior cenário, o equipamento roubado não teria bateria suficiente para fazer várias buscas no local de armazenamento.

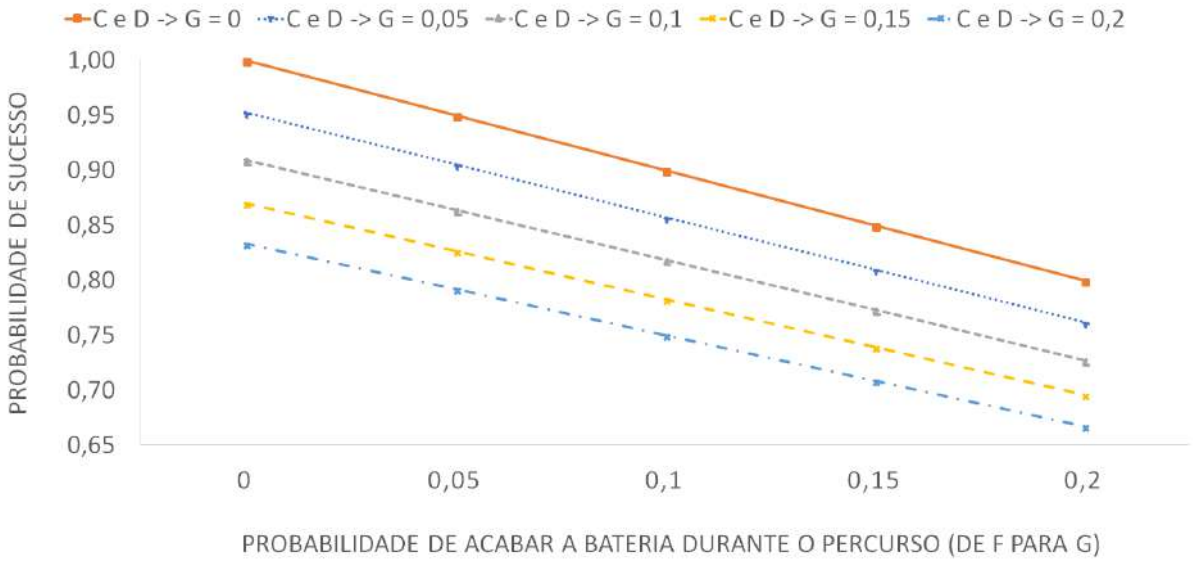
Após o equipamento furtado chegar ao galpão existem três possíveis transições que correspondem a:

- entrar em modo *standby*;
- encontrar outro(s) RFID(s) e enviar a mensagem;
- acabar a bateria.

Sendo assim, como cada estado é completamente independente do passado, pela Cadeia de Markov, a probabilidade de o sistema encontrar outro RFID é de 0,33.

De forma a melhor observar o comportamento do sistema na "região de sucesso", definida neste trabalho como uma probabilidade de sucesso maior do que 0,65, as proba-

Figura 7 - Probabilidade de sucesso do sistema em função da probabilidade de acabar a bateria durante o percurso variando entre 0 e 0,2.



bilidades de transição de C, D (mantidas iguais) e F para G foram gradualmente variadas de 0,05 em 0,05 a partir de 0 até 0,2.

Os resultados obtidos nos testes em que houve variações das probabilidades estão de acordo com o esperado. Os resultados do gráfico da Figura 6, mostram uma relação linear entre a probabilidade de sucesso do sistema e a probabilidade da bateria acabar. Em seus extremos, também é possível confirmar o teste de sanidade do sistema quando as probabilidades de sucesso são iguais a 1 e quando são iguais a 0. Também é possível verificar que a probabilidade de acabar a bateria durante o percurso tem maior influência sobre o gráfico quando comparado a probabilidade de acabar a energia após chegar ao local de armazenamento. Por este motivo, a autonomia do sistema é ponto chave nessa dissertação. De acordo com a Figura 7, apesar da probabilidade de acabar a bateria no percurso ser de 0,2 e a probabilidade de acabar a bateria após chegar ao galpão também ser 0,2, ainda assim, foi possível obter uma probabilidade de sucesso acima do objetivo de 0,65.

4.2 **Análises Realizadas Considerando Cenários Reais**

A probabilidade de sucesso do sistema está ligada diretamente à autonomia que a bateria proporciona ao sistema. Como apresentado na Seção 4.1, considerando a probabilidade máxima de acabar a energia já dentro do galpão igual a 0,2, o sistema apresenta índices muito altos de sucesso que variam entre 0,83 e 1. Porém, para um teste em si-

tuação real, foi utilizado um cenário em que, considerando a distância entre a estação e o local de armazenamento, a probabilidade de acabar a energia do sistema, fique próxima de 0,5. Ou seja, são locais onde, segundo o Google Maps, aproximadamente 50% das vezes o percurso tem estimativa de tempo acima da autonomia do sistema. Conforme apresentada na Seção 2.4, a autonomia do sistema, com a bateria de 9 V, capacidade de 380 mAh e considerando maior consumo possível dos módulos, chega a 02 horas e 42 minutos. Quando o tempo de percurso for inferior ao tempo de autonomia do sistema, a probabilidade de sucesso será de pelo menos 0,83 de acordo com a Figura 7.

Para fazer os testes e análises considerando situações reais, a metodologia a seguir foi aplicada. Conforme reportagem do G1 em março de 2017 (BRITO, 2017) e da BandNews em novembro de 2018 (CAMPBELL, 2018), um ponto de coleta de equipamentos furtados foi encontrado no Bairro de Curicica na cidade do Rio de Janeiro. Dessa forma, foi considerado que existe um ponto de coleta neste local. Uma das operadoras de telefonia móvel do País, possui um cadastro de todos os vandalismos, roubos e furtos de seus equipamentos em um portal interno. Foi definido então que, para simular um cenário real, o local de armazenamento seria em Curicica e algumas dessas estações que estão cadastradas no portal interno da operadora seriam os pontos de furto. Considerando sempre o pior tempo de trajeto, entre um ponto de furto e o local de armazenamento, estimado pelo Google Maps, as estações que em nenhum momento apresentavam tempo de trajeto maior que a autonomia, foram descartadas e estações mais distantes eram pesquisadas. Dessa forma, duas estações foram escolhidas para os testes.

Seguem a seguir, os pontos escolhidos como local de armazenamento de equipamentos furtados e as estações onde os furtos ocorreram:

- local de armazenamento:

  Curicica - RJ - Rua da Consagração, S/N - Latitude: 22 56 59.69 S - Longitude: 43 22 58.19 W;

- local de furto 01:

  VRC - Volta Redonda Coqueiro - R. Deolindo Miguel, 1520 - Vila Brasília, Volta Redonda - RJ, 27280-770 - Latitude: 22 29 18.30 S - Longitude: 44 06 10.70 W;

- local de furto 02:

  PMC - Porto Marisco - Rodovia Rio Santos, km 111 BR 101 - Latitude: 22 55 24.58 S - Longitude 44 21 43.99 W.

Com base nos endereços citados anteriormente, foram realizadas pesquisas no Google Maps com o objetivo de extrair quais as estimativas de tempo entre os pontos de furtos e o local de armazenamento de equipamentos roubados. Foi escolhido o dia dezessete de dezembro de dois mil e dezoito, segunda-feira, para simular o tempo de percurso

Tabela 7 - Tempos mínimo e máximo de trajeto entre a estação VRC e o galpão.

“Horário do furto”	Tempo mínimo	Tempo máximo
00:00	01:50	02:20
01:00	01:50	02:20
02:00	01:50	02:20
03:00	01:50	02:10
04:00	01:50	02:20
05:00	01:50	02:30
06:00	01:50	02:30
07:00	01:50	02:30
08:00	01:50	02:40
09:00	01:50	02:40
10:00	01:50	02:40
11:00	01:50	02:50
12:00	02:00	02:50
13:00	01:50	02:50
14:00	02:00	03:00
15:00	02:10	02:50
16:00	02:00	03:20
17:00	02:10	03:20
18:00	02:10	03:10
19:00	02:10	03:10
20:00	02:00	02:50
21:00	01:50	02:30
22:00	01:50	02:30
23:00	01:50	02:20

Fonte: Google Maps

entre Curicica e os locais de furto 01 (VRC) e 02 (PMC). Para cada dia, foram realizadas 24 pesquisas (de hora em hora) como demonstrado nas Tabelas 7 e 8. Pelo Google Maps, foram retiradas as previsões de tempo máximo e mínimo de percurso; no entanto, para os testes e análises, apenas o tempo máximo foi considerado, ou seja, foi realizada uma análise para o pior caso.

Considerando a Tabela 7, a Figura 8 foi gerada. A figura compara o tempo de autonomia do sistema com os tempos máximo e mínimo estimados para o percurso (por hora) entre Curicica e VRC. Nesse percurso, considerando-se o tempo máximo de trajeto, em 58% das vezes o sistema possui autonomia suficiente para chegar ao galpão sem a bateria acabar no trajeto, ou seja, a probabilidade de a bateria acabar durante o percurso é de 0,42.

A Figura 9 foi gerada a partir da Tabela 8. A figura representa o trajeto entre Curicica e PMC. Nesse percurso, em 50% das vezes o sistema possui autonomia suficiente.

Dados o tempo de autonomia do sistema e a possibilidade de o tempo de percurso

Tabela 8 - Tempos mínimo e máximo de trajeto entre a estação PMC e o galpão.

“Horário do furto”	Tempo mínimo	Tempo máximo
00:00	02:10	02:30
01:00	02:10	02:40
02:00	02:20	02:40
03:00	02:10	02:40
04:00	02:10	02:30
05:00	02:00	02:40
06:00	02:00	02:40
07:00	02:10	02:50
08:00	02:10	02:50
09:00	02:10	02:50
10:00	02:10	02:50
11:00	02:10	02:50
12:00	02:10	02:50
13:00	02:10	02:50
14:00	02:10	02:50
15:00	02:10	02:50
16:00	02:10	02:50
17:00	02:20	03:00
18:00	02:20	02:50
19:00	02:10	02:40
20:00	02:10	02:40
21:00	02:10	02:40
22:00	02:10	02:30
23:00	02:10	02:30

Fonte: Google Maps

Figura 8 - Autonomia e tempos mínimo e máximo de percurso em função do horário do furto - Estação VRC.

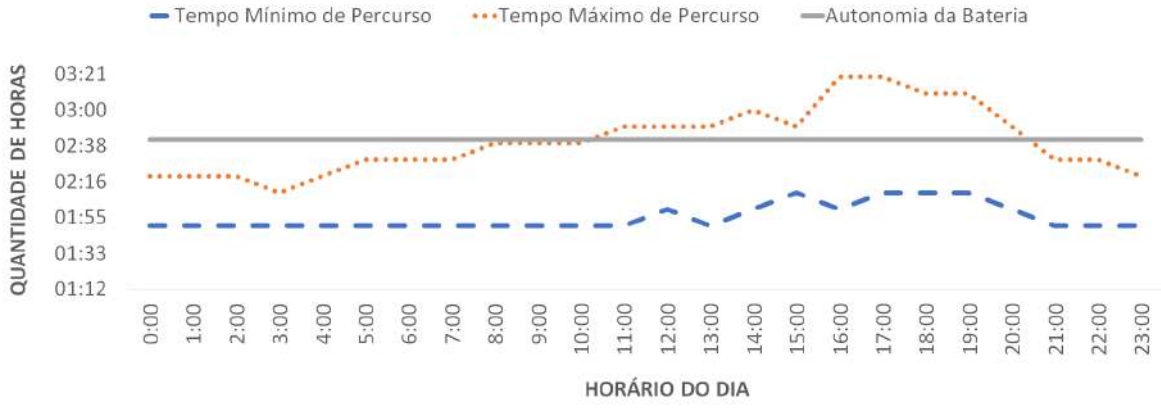
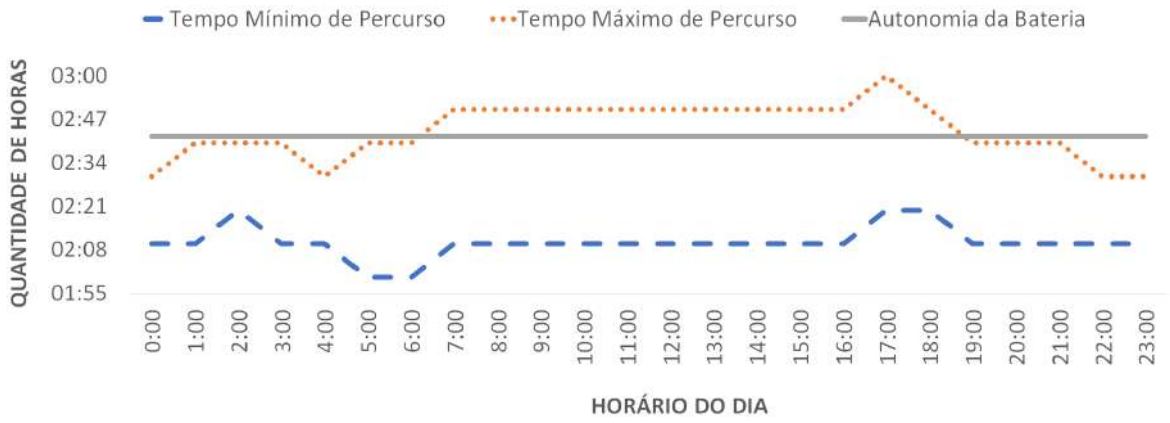


Figura 9 - Autonomia e tempos mínimo e máximo de percurso em função do horário do furto - Estação PMC.



(após o roubo) ser maior do que a autonomia, é necessário avaliar a probabilidade de sucesso do sistema.

Conforme descrito anteriormente, para os cenários reais foram consideradas duas localidades, VRC em Volta Redonda e PMC em Angra dos Reis. Em ambas localidades e para efeito de análise, apenas os tempos máximos de percurso das Figuras 8 e 9 foram considerados.

Em VRC, foi constatado e ilustrado na Figura 8 que em 42% das vezes o tempo de trajeto é maior que a autonomia. Considerando esse valor e utilizando a ferramenta de cálculo de probabilidades de cadeia de Markov, a probabilidade de sucesso varia entre 0,29 e 0,58 como mostra a Figura 10.

Em PMC, foi constatado e ilustrado na Figura 9 que em 50% das vezes o tempo de trajeto é maior que a autonomia. Considerando isso, as probabilidades de sucesso do sistema variam entre 0,25 e 0,50 como mostra a Figura 11.

Os melhores resultados, analisados anteriormente, para as estações de Volta Redonda e Angra dos, tiveram probabilidade de sucesso de 0,58 e 0,50 respectivamente. No entanto, esta dissertação, inclui uma utilização eficiente de energia que, conforme citado na Seção 2.3.1, utiliza códigos de programação e o acelerômetro para que o sistema possa revezar, entre os estados ativo e *standby* durante o percurso. Dessa forma, após entrar em movimento, o sistema fica em *standby* durante praticamente todo o percurso, enviando a cada trinta minutos informações de sua localização. A pesquisa e o envio de sua localização levam em média um minuto.

Apesar de não ser o objetivo principal dessa dissertação, o envio de localização durante esse período foi motivado pela possibilidade de se aproveitar o momento em que o sistema esteja ativo, para que ao menos consiga traçar no mapa alguns pontos pelo

Figura 10 - Probabilidade de sucesso do sistema em função de acabar a bateria no local de armazenamento VRC.

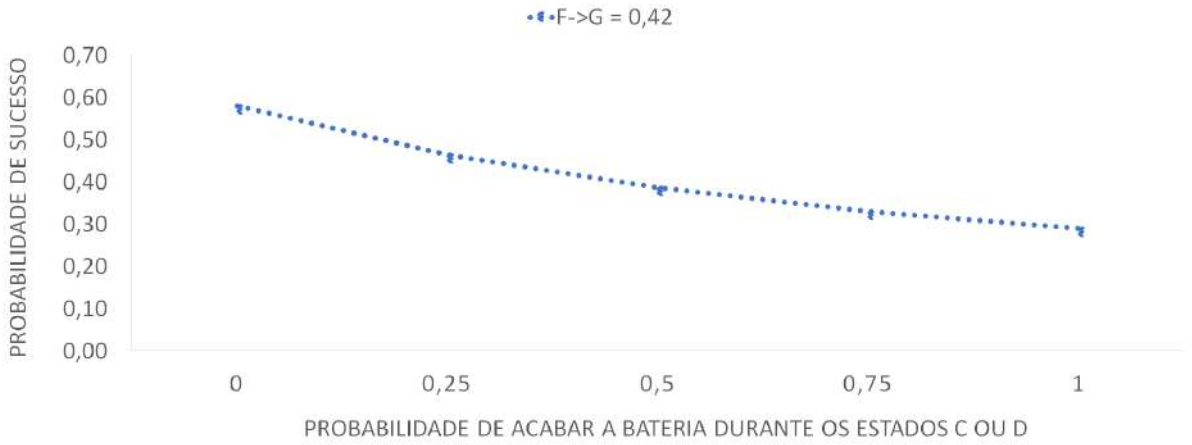


Figura 11 - Probabilidade de Sucesso Considerando Site de PMC.

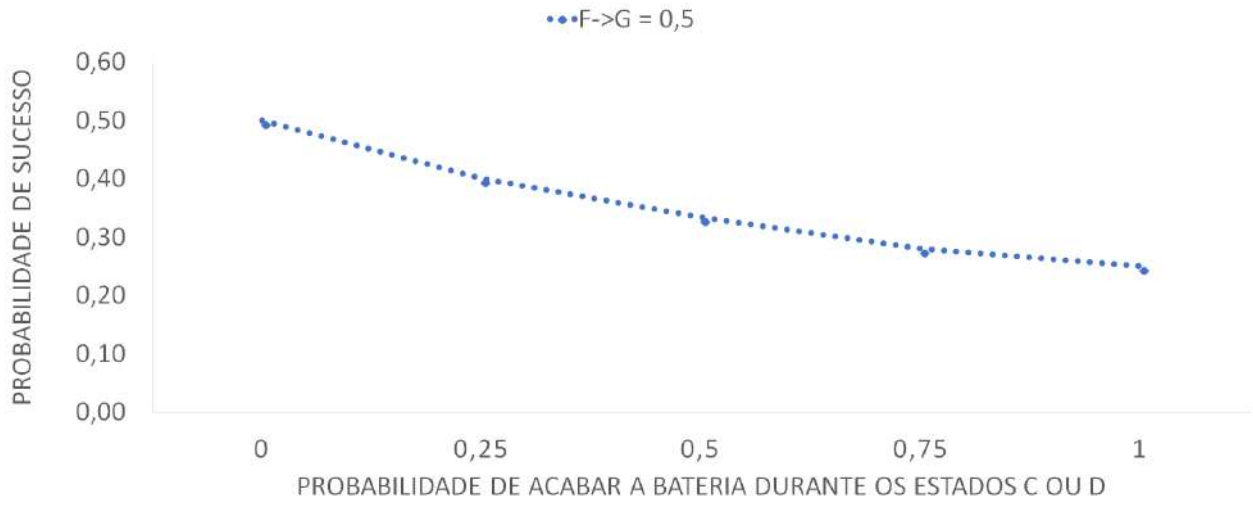


Tabela 9 - Tabela com dados extraídos nas análises utilizando o sistema.

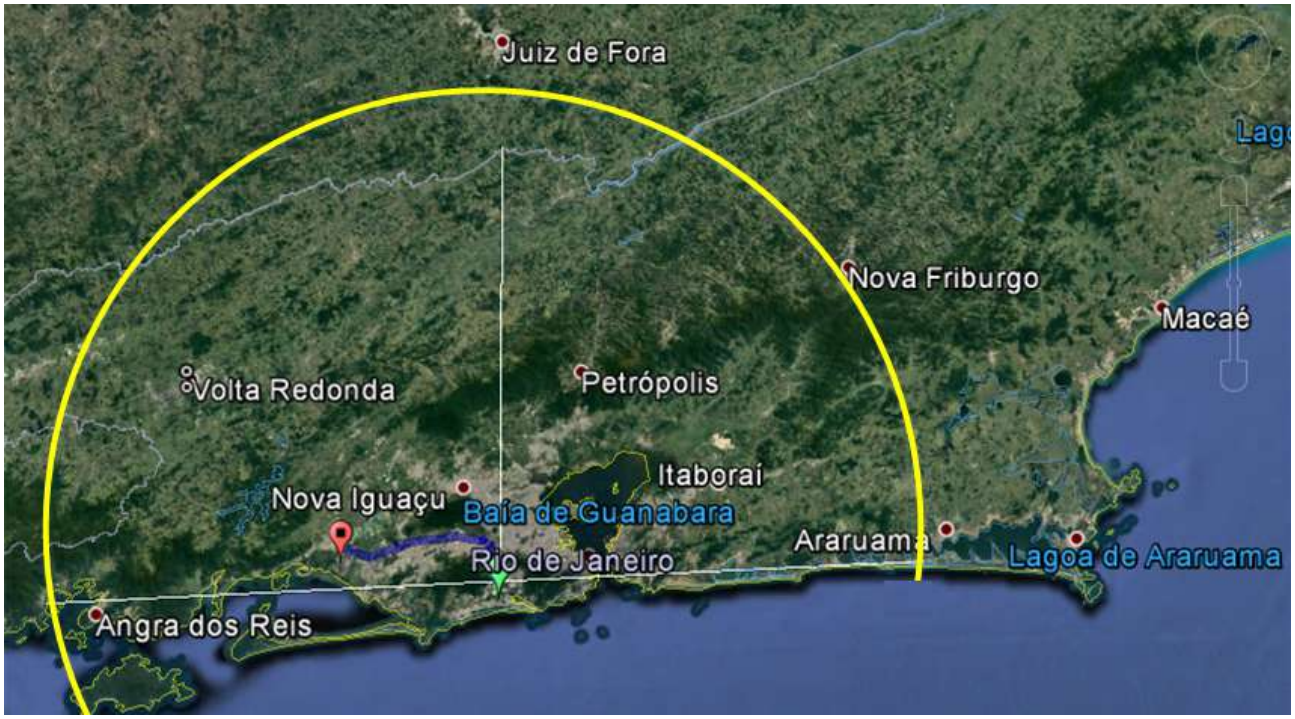
Estação	VRC	PMC
Tempo máximo de percurso (horas)	03:20	03:00
Quantidade de envio de informações durante o percurso (un.)	6	5
Tempo utilizado em pesquisa e envio de informações (min.)	6	5
Tempo em que o sistema permanece em *standby* (min.)	194	175
Consumo durante o *standby* (mAh)	326,56	294,58
Consumo durante a operação (mAh)	14,05	11,71
Consumo total durante o percurso (mAh)	340,61	306,29

qual passou e seus respectivos instantes de tempo. Dessa forma, mesmo em casos onde o sistema não possa ser encontrado por falta de energia, ele contribuirá com informações para futuras investigações.

Sendo assim, a Tabela 9 também mostra que para VRC, o tempo de trajeto mais longo é de três horas e vinte minutos (ver Tabela 7). Nesse tempo, o sistema enviaria informações de localização seis vezes, sendo a primeira trinta minutos após entrar em movimento e a última, cento e oitenta e seis minutos após entrar em movimento. O tempo em *standby* seria de três horas e quatorze minutos, já o tempo de pesquisa com GPS e envio de informação seria de seis minutos. O consumo total neste caso, chegaria a 340,61 mAh, logo, o sistema teria autonomia o suficiente por todo o percurso. Sua probabilidade de sucesso pode ser obtida nas Figuras 6 e 7 quando a probabilidade da bateria acabar durante o percurso é zero, ficando dependente apenas das probabilidades da bateria acabar enquanto o sistema estiver em seus estados C ou D. Nesse caso, sua probabilidade de sucesso variaria entre 0,5 e 1. A Tabela 9 mostra que para PMC, o tempo de trajeto mais longo é de três horas (ver Tabela 8), nesse tempo, o sistema enviaria informações de localização cinco vezes, sendo a primeira trinta minutos após entrar em movimento e a última, cento e cinquenta e cinco minutos após entrar em movimento. O tempo em *standby* seria de duas horas e cinquenta e cinco minutos, já o tempo de pesquisa com GPS e envio de informação seria de cinco minutos. O consumo total neste caso, chegaria a 306,29 mAh, logo, o sistema teria autonomia o suficiente por todo o percurso. Sua probabilidade de sucesso pode ser obtida nas Figuras 6 e 7 quando a probabilidade da bateria acabar durante o percurso é zero, ficando dependente apenas das probabilidades da bateria acabar enquanto o sistema estiver em seus estados C ou D. Logo, a probabilidade de sucesso nesse caso varia entre 0,5 e 1.

Conforme (IBGE, 2017), o estado do Rio de Janeiro possui uma área territorial de 43,781 km^2 aproximadamente. As distâncias em linha reta entre as estações VRC e PMC e o ponto de coleta em Curicica são de aproximadamente 92 e 108 km respectivamente. Assumindo a possibilidade de atuar nesse raio com probabilidade de sucesso igual ou superior a 0,83 e considerando apenas um ponto de coleta e mesmas condições de tráfego,

Figura 12 - Mapa de possível atuação do sistema com sucesso.



é razoável afirmar que, considerando 108 km, que o sistema seja eficiente em uma área de aproximadamente 18000 km^2; ou seja, em cerca de 41% da área territorial conforme demonstrado na Figura 12.

CONCLUSÕES

No Brasil, as empresas de telecomunicações buscam reduzir cada vez mais, seus índices de indisponibilidade. No entanto, os furtos e vandalismos que acontecem na rede são um enorme problema que as operadoras enfrentam hoje. Além de gerar prejuízos, essas ações também aumentam a indisponibilidade da rede. Por este motivo, esta dissertação propõe uma solução que ajuda na redução desses atos e na recuperação desses equipamentos. A solução aqui proposta, tem o intuito de transformar os equipamentos em iscas, rastreando o equipamento roubado e apontando os locais utilizados para armazenamento após identificar outros equipamentos roubados no local onde a isca foi armazenada. Com o intuito de levantar alguns pontos que nos permitam sintetizar a conclusão é necessário enfatizar as seguintes considerações. Uma delas é a utilização de uma bateria de baixíssimo custo e baixa capacidade no sistema. Outro ponto que é importante destacar é que as situações apresentadas foram sempre considerando o pior caso em relação ao tempo de percurso, onde normalmente, o percurso seria realizado em menos tempo. Com isso, o sistema foi avaliado de duas formas. A primeira, foi considerando as estações de VRC e PMC como cenários reais, porém, sem considerar o acelerômetro e as regras incluídas na codificação, onde, foi possível obter probabilidades de sucesso de 0,58 e 0,50 respectivamente. Sendo assim, o sistema se mostra viável em circunstâncias esses valores de probabilidade atendam ao sistema. No entanto, considerando o sistema proposto e incluindo as regras de economia do sistema, as probabilidades de sucesso aumentaram para no mínimo 0,83 em ambos os casos. Além disso, o tempo de autonomia alcançado permite cobrir aproximadamente um raio de 100 km no território do Rio de Janeiro. Diante do exposto, concluímos que o sistema é viável e suas altas taxas de sucesso demonstram que é possível colocar a aplicação em prática.

No entanto, durante a dissertação, foram levantados possíveis pontos de melhorias e desenvolvimentos nessa área. Uma importante proposta para estudos futuros é definir quais os melhores componentes para situações distintas, comparando diferentes modelos de leitores RFIDs e diferentes módulos GSM/GPS quanto a seus alcances, tamanhos e consumo. Nesta dissertação, a tecnologia utilizada para envio de mensagens foi o GSM, no entanto, uma oportunidade de melhoria é comparar diferentes tecnologias (WCDMA ou LTE) para essa mesma finalidade, concluindo assim, qual possui melhor eficiência em relação ao consumo, tamanho e tempo de resposta.

REFERÊNCIAS

ALVES, S. A matemática do gps. *Revista do professor de matemática*, v. 59, p. 17–26, 2006.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer networks*, Elsevier, v. 54, n. 15, p. 2787–2805, 2010.

BARAKA, K. et al. Low cost arduino/android-based energy-efficient home automation system with smart task scheduling. In: IEEE. *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*. [S.l.], 2013. p. 296–301.

BRITO, C. *G1Brito2017*. 2017. Disponível em: ⟨https://g1.globo.com/rio-de-janeiro/noticia/idosa-e-detida-no-rio-com-materiais-de-telefonia-avaliados-em-r-1-milhao.ghtml⟩. Acesso em: 15 Mar. 2018.

CAMPBELL, T. *BandNCampbell2018*. 2018. Disponível em: ⟨http://bandnewsfmrio.band.uol.com.br/editorias-detalhes/operacao-desarticula-quadrilha-especializada⟩. Acesso em: 15 Dez. 2018.

DENVER, D.; HARPER, W. *Mathematics of Decision Making Programs*. 1999. Disponível em: ⟨faculty.otterbein.edu/wharper/markov.xlt⟩. Acesso em: 16 Jan. 2019.

DUPRAT, C. *ROUBO OU FURTO DE ELEMENTOS DE REDE DE TELECOMUNICACOES*. [S.l.: s.n., 2016. 15 p. Disponível em: ⟨http://www.telebrasil.org.br/component/docman/doc_download/1551-23-08-2016-roubo-ou-furto-de-elementos-de-rede-de-telecomunicacoes?Itemid=⟩. Acesso em: 23 ago. 2016.

EZE, P. et al. Anti-theft system for car security using rfid. 2018.

FARGAS, B. C.; PETERSEN, M. N. Gps-free geolocation using lora in low-power wans. In: IEEE. *2017 Global Internet of Things Summit (GIoTS)*. [S.l.], 2017. p. 1–6.

FILHO, R. S. Como entender as tags eletrônicas. *RFID Journal Brasil*, 2012. Disponível em: ⟨https://brasil.rfidjournal.com/artigos/vision?9750⟩. Acesso em: 26 Jan. 2019.

GLOVER, B.; BATH, H. *Fundamentos de RFID*. STARLIN ALTA CONSULT, 2007. ISBN 9788576081395. Disponível em: ⟨https://books.google.com.br/books?id=YV9NYgEACAAJ⟩.

GRIGOLETTI, P. S. Cadeias de markov. *Recuperado em*, v. 19, n. 10, p. 2014, 2011.

GUEDES, S. L. O sistema classificatório das ocorrências na polícia militar do rio de janeiro e a organização da experiência policial: Uma análise preliminar. *A análise criminal e o planejamento operacional*, p. 53, 2008.

HAYATI, N.; SURYANEGARA, M. The iot lora system design for tracking and monitoring patient with mental disorder. In: IEEE. *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*. [S.l.], 2017. p. 135–139.

HE, W. et al. A solution for integrated track and trace in supply chain based on rfid & gps. In: IEEE. *2009 IEEE Conference on Emerging Technologies & Factory Automation*. [S.l.], 2009. p. 1–6.

HILLIER, F. S.; LIEBERMAN, G. J. *Introdução à pesquisa operacional*. [S.l.]: McGraw Hill Brasil, 2013.

IBGE. *Cidades e Estados*. IBGE - Instituto Brasileiro de Geografia e Estatística, 2017. Disponível em: ⟨https://www.ibge.gov.br/cidades-e-estados/rj.html?⟩ Acesso em: 30 Dez. 2018.

INDULA, M. *SIM808 EVB-V3.2 GPS+GSM+Source Code Part1*. 2017. Disponível em: ⟨https://www.youtube.com/watch?v=mvfTxRGTHWc⟩. Acesso em: 08 Ago. 2018.

INDULA, M. *SIM808 EVB-V3.2 GPS+GSM+Source Code Part2*. 2017. Disponível em: ⟨https://www.youtube.com/watch?v=mFgn9BqN9nQ⟩. Acesso em: 08 Ago. 2018.

ISO18000-6. ISO - International Organization for Standardization, 2010. Disponível em: ⟨https://www.iso.org/standard/46149.html⟩. Acesso em: 08 Dez. 2018.

JACOBSEN, R. H.; ALIU, D.; EBEID, E. A low-cost vehicle tracking platform using secure sms. In: *IoTBDS*. [S.l.: s.n.], 2017. p. 157–166.

JIN, M. et al. iguard: A real-time anti-theft system for smartphones. *IEEE Transactions on Mobile Computing*, IEEE, 2018.

KUMAR, B. H. et al. Vehicle monitoring and tracking system using gps and gsm technologies. *International Research Journal of Engineering and Technology (IRJET)*, v. 3, n. 4, p. 2395–0072, 2016.

LOPES, M. *Como utilizar o leitor RFID com o Arduino para sua Automação*. 2017. Disponível em: ⟨http://www.experimentosdegaragem.com.br/2017/01/04/como-utilizar-o-leitor-rfid-com-o-arduino-para-sua-automacao/⟩. Acesso em: 09 Ago. 2018.

LOURENÇO, J. M.; ISPGAYA, R. A. R. d. R.; INESC-UTOE, R. d. C. A. Aspectos técnicos do gsm. *Politécnica*, p. 8, 2000.

MARQUES, C. A. et al. A tecnologia de identificadores de rádio freqüência na logística interna industrial: pesquisa exploratória numa empresa de usinados para o setor aeroespacial. *Gepros: Gestão da Produção, Operações e Sistemas*, Universidade Estadual Paulista-UNESP Bauru, Depto de Engenharia de Produção, v. 4, n. 2, p. 109, 2009.

MAURYA, K.; SINGH, M.; JAIN, N. Real time vehicle tracking system using gsm and gps technology-an anti-theft tracking system. *International Journal of Electronics and Computer Science Engineering. ISSN*, v. 22771956, p. V1N3–1103, 2012.

MCROBERTS, M. *Arduino básico*. [S.l.]: Novatec Editora, 2018.

MONICO, J. F. G. *Posicionamento pelo Navstar-GPS*. [S.l.]: Unesp, 2000.

NETO, S. A.; OLIVEIRA, R. de; NASCIMENTO, V. E. do. Avaliação de autonomia de baterias recarregáveis para aplicação em rede de sensores sem fio. Simpósio Brasileiro de Redes de Computadores, 2013.

NOGUEIRA, F. Modelagem e simulação-cadeias de markov. *Notas de Aula UFJF Juiz de Fora-2008*, 2008.

NXP SEMICONDUCTORS. *Contactless reader IC*. [S.l.], 2011. Rev. 3.6.

NXP SEMICONDUCTORS. *MF1S50YYX_V1*. [S.l.], 2018. Rev. 3.2.

ONE TECHNOLOGY WAY. *Accelerometer - ADXL337*. [S.l.], 2010. Rev. 0.

ONLINE, G. *Vivo diz que sinal ruim é culpa de 'vandalismo' e 'queda de energia'*. 2018. Disponível em: ⟨https://www.gazetaonline.com.br/noticias/cidades/2018/01/vivo-diz-que-sinal-ruim-e-culpa-de--vandalismo--e--queda-de-energia-1014115964.html#⟩. Acesso em: 15 Jan. 2019.

PEPINO, C. B.; DIAS, G. *Pocket guard: dispositivo portátil de segurança IoT*. Dissertação (B.S. thesis) — Universidade Tecnológica Federal do Paraná, 2018.

POSSA, P. R.; PASSOLD, F. Recarregador inteligente de baterias. In: *VII International Conference on Industrial Aplications (INDUSCON 2006)*. [S.l.: s.n.], 2006.

POUSOALEGRE.NET. *Polícia apreende equipamentos roubados usados por provedora de internet em Pouso Alegre e região*. 2018. Disponível em: ⟨https://pousoalegre.net/noticia/2018/04/policia-apreende-equipamentos/⟩. Acesso em: 15 Jan. 2019.

ROBERTS, C. M. Radio frequency identification (rfid). *Computers & security*, Elsevier, v. 25, n. 1, p. 18–26, 2006.

ROHOKALE, V. M.; PRASAD, N. R.; PRASAD, R. A cooperative internet of things (iot) for rural healthcare monitoring and control. In: IEEE. *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. [S.l.], 2011. p. 1–6.

SANT'ANNA, F. et al. Transparent standby for low-power, resource-constrained embedded systems: a programming language-based approach (short wip paper). In: ACM. *Proceedings of the 19th ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems*. [S.l.], 2018. p. 94–98.

SARDROUD, J. M.; LIMBACHIYA, M. Effective information delivery at construction phase with integrated application of rfid, gps and gsm technology. In: *Proceedings of the World Congress on Engineering*. [S.l.: s.n.], 2010. v. 1.

SENNA, C. C. L. d.; SOARES, P. I. E. Estudo de aplicações rfid na plataforma de iot. Niterói, 2018.

SEUFITELLI, C. B. et al. Tecnologia rfid e seus benefícios. *Vertices*, Directory of Open Access Journals, v. 11, n. 1, p. 19–26, 2010.

SHANGHAI SIMCOM WIRELESS SOLUTIONS LTD. *SIM808 Hardware Design V1.00*. [S.l.], 2014. Rev. 1.

SKODOWSKI, T.; SARZI, L. *Polícia faz uma das maiores apreensões de materiais furtados de telefonia do Brasil*. 2016. Disponível em: ⟨https://www.tribunapr.com.br/painel-do-crime/policia-faz-uma-das-maiores-apreensoes-de-materiais-furtados-de-telefonia-do-brasil/⟩. Acesso em: 15 Jan. 2019.

TELECO. *Cobertura das Operadoras e Populacao Atendida*. Teleco, 2019. Disponível em: ⟨http://www.teleco.com.br/cobertura.asp⟩. Acesso em: 10 Mar. 2019.

XIA, F. et al. Internet of things. *International Journal of Communication Systems*, Wiley Online Library, v. 25, n. 9, p. 1101–1102, 2012.

YANG, K. Wireless sensor networks. *Principles, Design and Applications*, Springer, 2014.

YANG, L. et al. A hybrid method for achieving high accuracy and efficiency in object tracking using passive rfid. In: IEEE. *Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on*. [S.l.], 2012. p. 109–115.

YOUSSEF, M.; YOSEF, M. A.; EL-DERINI, M. Gac: energy-efficient hybrid gps-accelerometer-compass gsm localization. In: IEEE. *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. [S.l.], 2010. p. 1–5.

APÊNDICE A – Códigos Utilizados nos Testes

A.1 Código Desenvolvido no Arduino para a Integração do Módulo RFID RC-522

```
#include <deprecated.h>
#include <MFRC522.h>
#include <MFRC522Debug.h>
#include <MFRC522Extended.h>
#include <MFRC522Hack.h>
#include <require_cpp11.h>
#include <SPI.h>
#include <LiquidCrystal.h>

//Pinos Reset e SS módulo MFRC522
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);

LiquidCrystal lcd(6, 7, 5, 4, 3, 2);

#define pino_botao_le A2
#define pino_botao_gr A3

MFRC522::MIFARE_Key key;

void setup()
{
  pinMode(pino_botao_le, INPUT);
  pinMode(pino_botao_gr, INPUT);
  Serial.begin(9600);   //Inicia a serial
  SPI.begin();      //Inicia  SPI bus
  mfrc522.PCD_Init();   //Inicia MFRC522

  //Inicializa o LCD 16x2
  lcd.begin(16, 2);
  mensageminicial();
```

```
  //Prepara chave - padrao de fabrica = FFFFFFFFFFFFh
  for (byte i = 0; i < 6; i++) key.keyByte[i] = 0xFF;
}

void loop()
{
  //Verifica se o botao modo leitura foi pressionado
  int modo_le = digitalRead(pino_botao_le);
  if (modo_le != 0)
  {
    lcd.clear();
    Serial.println("Modo leitura selecionado");
    lcd.setCursor(2, 0);
    lcd.print("Modo leitura");
    lcd.setCursor(3, 1);
    lcd.print("selecionado");
    while (digitalRead(pino_botao_le) == 1) {}
    delay(3000);
    modo_leitura();
  }
  //Verifica se o botao modo gravacao foi pressionado
  int modo_gr = digitalRead(pino_botao_gr);
  if (modo_gr != 0)
  {
    lcd.clear();
    Serial.println("Modo gravacao selecionado");
    lcd.setCursor(2, 0);
    lcd.print("Modo gravacao");
    lcd.setCursor(3, 1);
    lcd.print("selecionado");
    while (digitalRead(pino_botao_gr) == 1) {}
    delay(3000);
    modo_gravacao();
  }
}
void mensageminicial()
{
  Serial.println("nSelecione o modo leitura ou gravacao...");
  Serial.println();
```

```
  lcd.clear();
  lcd.print("Selecione o modo");
  lcd.setCursor(0, 1);
  lcd.print("leitura/gravacao");
}

void mensagem_inicial_cartao()
{
  Serial.println("Aproxime o seu cartao do leitor...");
  lcd.clear();
  lcd.print(" Aproxime o seu");
  lcd.setCursor(0, 1);
  lcd.print("cartao do leitor");
}

void modo_leitura()
{
  mensagem_inicial_cartao();
  //Aguarda cartao
  while ( ! mfrc522.PICC_IsNewCardPresent())
  {
    delay(100);
  }
  if ( ! mfrc522.PICC_ReadCardSerial())
  {
    return;
  }
  //Mostra UID na serial
  Serial.print("UID da tag : ");
  String conteudo = "";
  byte letra;
  for (byte i = 0; i < mfrc522.uid.size; i++)
  {
    Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfrc522.uid.uidByte[i], HEX);
    conteudo.concat(String(mfrc522.uid.uidByte[i]<0x10 ? " 0" : " "));
    conteudo.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
  Serial.println();
```

```
//Obtem os dados do setor 1, bloco 4 = Nome
byte sector         = 1;
byte blockAddr      = 4;
byte trailerBlock   = 7;
byte status;
byte buffer[18];
byte size = sizeof(buffer);

//Autenticacao usando chave A
status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
                                trailerBlock, &key, &(mfrc522.uid));
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("PCD_Authenticate() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}
status = mfrc522.MIFARE_Read(blockAddr, buffer, &size);
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("MIFARE_Read() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
}
//Mostra os dados do nome no Serial Monitor e LCD
lcd.clear();
lcd.setCursor(0, 0);
for (byte i = 1; i < 16; i++)
{
  Serial.print(char(buffer[i]));
  lcd.write(char(buffer[i]));
}
Serial.println();

//Obtem os dados do setor 0, bloco 1 = Sobrenome
sector         = 0;
blockAddr      = 1;
trailerBlock   = 3;

//Autenticacao usando chave A
status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
```

```
                                    trailerBlock, &key, &(mfrc522.uid));
  if (status != MFRC522::STATUS_OK)
  {
    Serial.print(F("PCD_Authenticate() failed: "));
    Serial.println(mfrc522.GetStatusCodeName(status));
    return;
  }
  status = mfrc522.MIFARE_Read(blockAddr, buffer, &size);
  if (status != MFRC522::STATUS_OK)
  {
    Serial.print(F("MIFARE_Read() failed: "));
    Serial.println(mfrc522.GetStatusCodeName(status));
  }
  //Mostra os dados do sobrenome no Serial Monitor e LCD
  lcd.setCursor(0, 1);
  for (byte i = 0; i < 16; i++)
  {
    Serial.print(char(buffer[i]));
    lcd.write(char(buffer[i]));
  }
  Serial.println();

  // Halt PICC
  mfrc522.PICC_HaltA();
  // Stop encryption on PCD
  mfrc522.PCD_StopCrypto1();
  delay(3000);
  mensageminicial();
}

void modo_gravacao()
{
  mensagem_inicial_cartao();
  //Aguarda cartao
  while ( ! mfrc522.PICC_IsNewCardPresent()) {
    delay(100);
  }
  if ( ! mfrc522.PICC_ReadCardSerial())    return;
```

```
//Mostra UID na serial
Serial.print(F("UID do Cartao: "));    //Dump UID
for (byte i = 0; i < mfrc522.uid.size; i++)
{
  Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
  Serial.print(mfrc522.uid.uidByte[i], HEX);
}
//Mostra o tipo do cartao
Serial.print(F("nTipo do PICC: "));
byte piccType = mfrc522.PICC_GetType(mfrc522.uid.sak);
Serial.println(mfrc522.PICC_GetTypeName(piccType));

byte buffer[34];
byte block;
byte status, len;

Serial.setTimeout(20000L) ;
Serial.println(F("Digite o sobrenome,em seguida o caractere #"));
lcd.clear();
lcd.print("Digite o sobreno");
lcd.setCursor(0, 1);
lcd.print("me + #");
len = Serial.readBytesUntil('#', (char *) buffer, 30) ;
for (byte i = len; i < 30; i++) buffer[i] = ' ';

block = 1;
//Serial.println(F("Autenticacao usando chave A..."));
status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
                                block, &key, &(mfrc522.uid));
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("PCD_Authenticate() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}

//Grava no bloco 1
status = mfrc522.MIFARE_Write(block, buffer, 16);
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("MIFARE_Write() failed: "));
```

```
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}

block = 2;
//Serial.println(F("Autenticacao usando chave A..."));
status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
                                  block, &key, &(mfrc522.uid));
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("PCD_Authenticate() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}

//Grava no bloco 2
status = mfrc522.MIFARE_Write(block, &buffer[16], 16);
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("MIFARE_Write() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}

Serial.println(F("Digite o nome, em seguida o caractere #"));
lcd.clear();
lcd.print("Digite o nome e");
lcd.setCursor(0, 1);
lcd.print("em seguida #");
len = Serial.readBytesUntil('#', (char *) buffer, 20) ;
for (byte i = len; i < 20; i++) buffer[i] = ' ';

block = 4;
Serial.println(F("Autenticacao usando chave A..."));
status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
                                  block, &key, &(mfrc522.uid));
if (status != MFRC522::STATUS_OK) {
  Serial.print(F("PCD_Authenticate() failed: "));
  Serial.println(mfrc522.GetStatusCodeName(status));
  return;
}
```

```
  //Grava no bloco 4
  status = mfrc522.MIFARE_Write(block, buffer, 16);
  if (status != MFRC522::STATUS_OK) {
    Serial.print(F("MIFARE_Write() failed: "));
    Serial.println(mfrc522.GetStatusCodeName(status));
    return;
  }

  block = 5;
  //Serial.println(F("Authenticating using key A..."));
  status=mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A,
                                  block, &key, &(mfrc522.uid));
  if (status != MFRC522::STATUS_OK) {
    Serial.print(F("PCD_Authenticate() failed: "));
    Serial.println(mfrc522.GetStatusCodeName(status));
    return;
  }

  //Grava no bloco 5
  status = mfrc522.MIFARE_Write(block, &buffer[16], 16);
  if (status != MFRC522::STATUS_OK) {
    Serial.print(F("MIFARE_Write() failed: "));
    Serial.println(mfrc522.GetStatusCodeName(status));
    //return;
  }
  else
  {
    Serial.println(F("Dados gravados com sucesso!"));
    lcd.clear();
    lcd.print("Gravacao OK!");
  }

  mfrc522.PICC_HaltA(); // Halt PICC
  mfrc522.PCD_StopCrypto1();  // Stop encryption on PCD
  delay(5000);
  mensageminicial();
}
```

A.2 Código Desenvolvido no Arduino para a Integração do Módulo GSM/GPS SIM808

```
#include <DFRobot_sim808.h>
#include <sim808.h>

#include <DFRobot_sim808.h>
#include <SoftwareSerial.h>

#define MESSAGE_LENGTH 160
char message[MESSAGE_LENGTH];
int messageIndex = 0;
char MESSAGE[300];
char lat[12];
char lon[12];
char wspeed[12];

char phone[16];
char datetime[24];

#define PIN_TX 07
#define PIN_RX 08
SoftwareSerial mySerial(PIN_TX,PIN_RX);
DFRobot_SIM808 sim808(&mySerial);//Connect RX,TX,PWR,

void sendSMS();
void getGPS();
void readSMS();

void setup()
{
  mySerial.begin(9600);
  Serial.begin(9600);

  //******** Initialize sim808 module *************
  while(!sim808.init())
  {
      Serial.print("Sim808 init error\r\n");
      delay(1000);
```

```
  }
  delay(3000);

  Serial.println("SIM Init success");

  Serial.println("Init Success, please send SMS message to me!");
}

void loop()
{
  //************ Detecting unread SMS ************************
   messageIndex = sim808.isSMSunread();

   //************ At least, there is one UNREAD SMS ***********
   if (messageIndex > 0)
   {

      readSMS();
      getGPS();
      sendSMS();

      //************** Turn off the GPS power ************
      sim808.detachGPS();

      Serial.println("Please send SMS message to me!");
   }
}

void readSMS()
{
  Serial.print("messageIndex: ");
  Serial.println(messageIndex);

  sim808.readSMS(messageIndex, message, MESSAGE_LENGTH, phone, datetime);

  //In order not to full SIM Memory, is better to delete it
  sim808.deleteSMS(messageIndex);
  Serial.print("From number: ");
  Serial.println(phone);
```

```
  Serial.print("Datetime: ");
  Serial.println(datetime);
  Serial.print("Recieved Message: ");
  Serial.println(message);
}

void getGPS()
{
  while(!sim808.attachGPS())
  {
    Serial.println("Open the GPS power failure");
    delay(1000);
  }
  delay(3000);

  Serial.println("Open the GPS power success");

  while(!sim808.getGPS())
  {

  }

  Serial.print(sim808.GPSdata.year);
  Serial.print("/");
  Serial.print(sim808.GPSdata.month);
  Serial.print("/");
  Serial.print(sim808.GPSdata.day);
  Serial.print(" ");
  Serial.print(sim808.GPSdata.hour);
  Serial.print(":");
  Serial.print(sim808.GPSdata.minute);
  Serial.print(":");
  Serial.print(sim808.GPSdata.second);
  Serial.print(":");
  Serial.println(sim808.GPSdata.centisecond);
  Serial.print("latitude :");
  Serial.println(sim808.GPSdata.lat);
  Serial.print("longitude :");
  Serial.println(sim808.GPSdata.lon);
```

```
  Serial.print("speed_kph :");
  Serial.println(sim808.GPSdata.speed_kph);
  Serial.print("heading :");
  Serial.println(sim808.GPSdata.heading);
  Serial.println();

  float la = sim808.GPSdata.lat;
  float lo = sim808.GPSdata.lon;
  float ws = sim808.GPSdata.speed_kph;

  dtostrf(la, 4, 6, lat);
  //put float value of la into char array of lat.
  //4 = number of digits before decimal sign.
  //6 = number of digits after the decimal sign.
  dtostrf(lo, 4, 6, lon);
  //put float value of lo into char array of lon
  dtostrf(ws, 6, 2, wspeed);
  //put float value of ws into char array of wspeed

  sprintf(MESSAGE, "Latitude : %s\nLongitude\nMy Module Is Working.
  Mewan Indula Pathirage. Try With This Link.
  //nhttp://www.latlong.net/Show-Latitude-Longitude.
  html\nhttp://maps.google.com/maps?q=%s,%s\n",
  lat, lon, wspeed, lat, lon);
}

void sendSMS()
{
  Serial.println("Start to send message ...");

  Serial.println(MESSAGE);
  Serial.println(phone);

  sim808.sendSMS(phone,MESSAGE);
}
```

APÊNDICE B – Imagens adicionais do protótipo

B.1 **Fotos do Sistema em Funcionamento**

A seguir, são apresentadas fotos do sistema em funcionamento.

Figura 13 - Foto do rastreador em funcionamento e mensagem de localização.

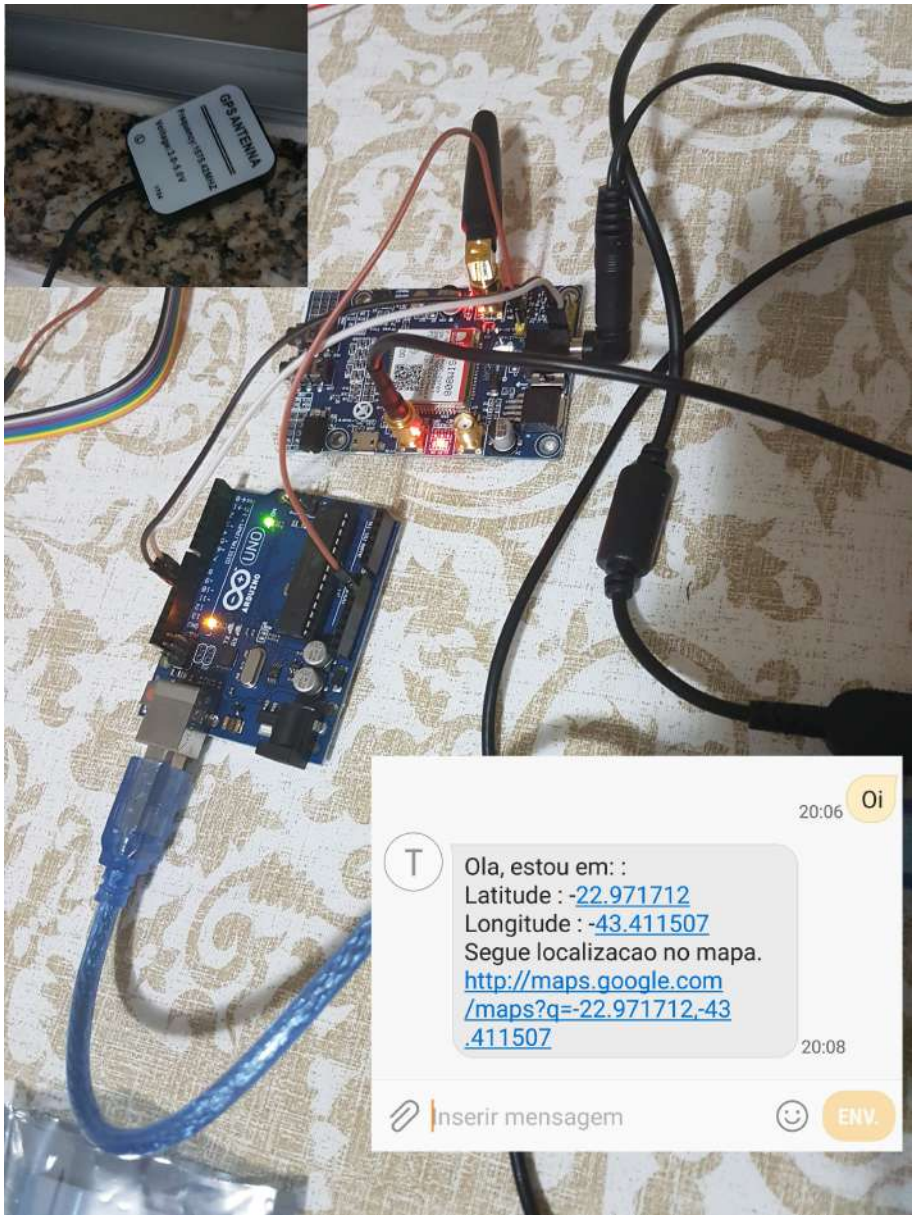


Figura 14 - Foto do sistema completo e mensagem com IDs vinculados.