# EFEITO COLATERAL CAUSADO PELO EMPREGO DO INTERFERIDOR ANTI-DRONE SCE 0100 (IACIT) EM REDES WI-FI OUTDOOR

**Daniel Roberto Resende[1], Marcelo Carneiro de Paiva[2].**

*Pós-graduado em Engenharia de Sistemas de Radiocomunicação[1], Mestrado em Engenharia Elétrica[2]*

**RESUMO**: O uso de drones em ações terroristas, visando atingir aglomerações de pessoas, principalmente em grandes eventos, tornou-se uma preocupação das autoridades públicas. No Brasil, para garantir a segurança da população em eventos como as olimpíadas, o Exército Brasileiro utiliza bloqueadores de sinais (jammers) de radiofrequência capazes de atuar no sistema de controle da maioria dos drones disponíveis no mercado com o intuito de produzir um "escudo de proteção" nas áreas com maior concentração de pessoas. Este trabalho propõe analisar, por meio de teste de campo e modelos de propagação, qual o impacto do uso desses bloqueadores, dentro de um cenário urbano, em redes Wi-Fi outdoor, tendo em vista que a frequência da maioria dos canais de controle dos modelos atuais de drones trabalham na mesma faixa de frequência que roteadores usados em redes Wi-Fi.

Palavras-chave: Bloqueador Anti-Drone. Interferência em redes Wi-Fi outdoor. Padrão 802.11. SCE 0100 – IACIT.

## INTRODUÇÃO

O uso de drones como atividade recreativa ou mesmo profissional se tornou bastante comum nos dias atuais. Porém, a popularidade desse dispositivo traz a possibilidade de se implementar uma arma que pode ser encarada como uma ameaça terrorista em eventos internacionais de grande porte (OLIVEIRA, 2015). Um ataque terrorista, em um grande evento como a copa do mundo ou as olimpíadas, utilizando um drone, pode ter grandes proporções e expor o despreparo das forças de segurança envolvidas (OLIVEIRA, 2015).

Para este problema existem soluções no mercado. A empresa americana Liteye System, por exemplo, desenvolveu um sistema composto por câmeras de alta definição, radares e bloqueadores direcionados de ondas de rádio que são capazes de detectar, monitorar e impedir o voo de Drones. Esse sistema ficou conhecido como "Raio da Morte" (DEFESANET, 2016).

Nas olimpíadas de 2014 e na copa do mundo de 2016, eventos internacionais sediados pelo Brasil, as forças armadas brasileiras foram as responsáveis pela segurança destes eventos. Com a finalidade de combater ações terroristas que envolvam o uso de drones o exército brasileiro adquiriu um equipamento Interferidor (Jammer), especificadamente desenvolvido para atuar no canal de controle dos principais modelos de drones disponíveis no mercado. Este interferidor é capaz de bloquear o sinal de rádio que controla o drone, fazendo com que o aparelho cesse voo ou simplesmente fique desorientado (DEFESANET, 2016).

Grande parte dos drones utiliza como canal de controle às faixas de frequências não licenciadas destinadas a transmissão de sinais Wi-Fi. Portanto, o uso de interferidores de radiofrequência pode causar interferência em dispositivos Wi-Fi localizados dentro de sua área de atuação (ARAUJO, 2017).

O uso de interferidores foi autorizado pela ANATEL devendo ser restrito em operações específicas, episódicas, urgentes e temporárias em situações de risco potencial ou iminente de ações necessárias à preservação da ordem pública e da segurança das pessoas e do patrimônio (DEFESANET, 2016).

O objetivo desse artigo é mostrar, por meio de testes de campo e modelos de propagação, a atuação de um sinal interferente gerado pelo equipamento SCE 0100, da empresa

IACIT e seu efeito indesejável para uma rede Wi-Fi, causando transtornos para o cidadão comum que está conectado em um roteador Wi-Fi outdoor, ou até mesmo em redes do tipo ponto a ponto que atendem a grandes empresas.

O trabalho encontra-se estruturado em cinco seções. A seção II apresenta uma discussão sobre o uso de drones em ações terroristas evidenciando o uso de interferidores como contra medidas a essas ações. A seção III apresenta um estudo sobre o padrão de redes sem fio IEEE 802.11. O equipamento SCE 0100-D, utilizado como interferidor neste estudo, é apresentado em termos de características técnicas na seção IV. O teste de campo, análise e discussão dos resultados obtidos são apresentados na seção V. Na seção VI, são apresentadas as principais conclusões sobre o trabalho realizado e perspectivas de trabalhos futuros.

## 1 A AMEAÇA DRONE

Os drones ou VANT's (Veículo Aéreo Não Tripulado) podem ser definidos como qualquer objeto que se desprenda do chão e seja capaz de se sustentar na atmosfera com propósito diferente de diversão (OLIVEIRA, 2015). De pequeno porte são capazes de suportar cargas próximas de 8 kg e voar com uma velocidade de 30 km/h, a uma distância de 2000 metros do seu ponto de controle e com uma autonomia de até 25 minutos (OLIVEIRA, 2015). Um aparelho assim, carregando algum componente químico, como um ácido ou até mesmo um explosivo, se usado em locais com grande aglomeração de pessoas, pode causar um grande estrago.

É fácil encontrar exemplos reais do quanto é difícil identificar e interceptar um drone. Em 2015, um drone conseguiu invadir acidentalmente a casa branca, nos EUA, sem que nenhum alarme fosse acionado. Durante o ocorrido, cogitou-se a possibilidade de um ataque terrorista, sendo descartada após a localização do proprietário do aparelho que relatou ter perdido o controle do mesmo (LEONNIG, 2015). Em abril de 2015, no Japão, um drone, carregando material radioativo, conseguiu pousar no telhado do escritório oficial do primeiro ministro japonês. O responsável pelo aparelho era um ativista japonês que queria protestar contra o uso de energia nuclear (SHANKER, 2015).

Devido à grande parte das pessoas usarem seus drones como hobby e com o intuito de baratear e simplificar o sistema, a maioria desses aparelhos utiliza, em seu canal de controle, as faixas de frequências ISM (Industrial Sientific and Medical). Trata-se de bandas reservadas internacionalmente para o desenvolvimento industrial, científico e médico. Essas bandas foram definidas em 1985 pelo FCC (Federal Communications Commission), órgão regulador da área de telecomunicações e radiodifusão. Este órgão reservou uma parte do espectro de frequência para desenvolvimentos livres, sem a necessidade de licenciamento, definindo somente normas para limitação de potência de transmissão e técnicas de modulação dentro destas faixas (TELECO, 2017). No Brasil, a ANATEL (Agência Nacional de Telecomunicações) regulamenta sobre o uso de equipamentos de radiocomunicação de radiação restrita por meio da resolução n º 506 de 1º de julho de 2008, onde são definidas as faixas de frequências ISM, bem como a potência máxima permitida para equipamentos que usem essas frequências.

Alguns drones mais sofisticados dispõem de recursos de navegação por meio de GPS ( Global Positioning System, Sistema de Posicionamento Global) onde seu trajeto pode ser pré-estabelecido e o voo ser executado sem a necessidade de um operador. Esse sistema também é usado em caso de perda do sinal de controle fazendo com que o aparelho possa pousar em local pré-definido. Esse tipo de controle de drones não será alvo de avaliação nesse artigo.

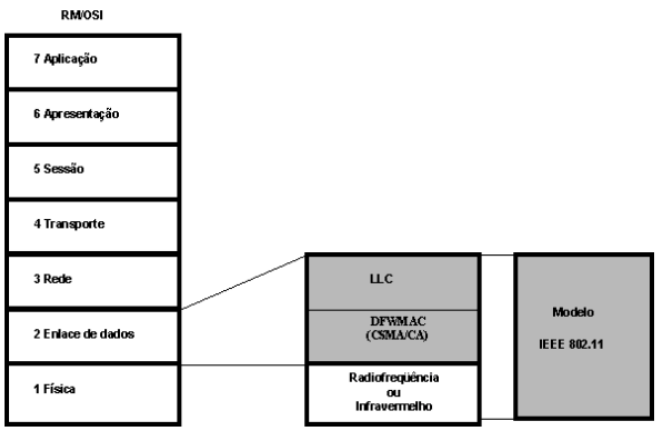
## 2 PADRÃO DAS REDES SEM FIO IEEE 802.11

Devido à implementação de várias tecnologias que permitiram uma maior taxa de transferência de dados por meio de ondas eletromagnéticas, técnicas de segurança mais robustas e a diminuição de custos, as redes sem fio ou Wi-Fi passaram a fazer cada vez mais parte do nosso cotidiano. Além de serem flexíveis e de fácil instalação, é cada vez mais perceptível à substituição das redes cabeadas pelas redes sem fio (NARDIN, 2008).

O IEEE (Institute of Electrical and Electronics Engineers) é o órgão responsável pela definição do padrão usado para redes locais sem fio, denominado WLAN ( Wi-fi Local Area Network), padrão 802.11. Esse padrão deveria atender a algumas premissas básicas, como suportar diversos canais; sobrepor diversas redes na mesma área de canal; apresentar robustez com relação à interferência; possuir mecanismos para evitar nós escondidos; oferecer privacidade e controle de acesso ao meio (BARIZON, 2005).

O padrão 802.11 especifica a camada de nível físico e seu controle de acesso e pode ser comparado com o modelo OSI conforme ilustrado na Figura 1. Os padrões de redes locais sem fio, WLAN, foram definidos pelo IEEE especificando somente a camada física e a camada de enlace. Esse estudo ficará restrito a nível da camada física das redes sem fio.

**FIGURA 1 -** Comparação do padrão 802.11 com o RM-OSI (BARIZON, 2005).




A camada física está relacionada ao serviço de transmissão do rádio. É nela que são definidos os parâmetros do tipo do sinal transmitido, tais como a frequência, a largura de banda do canal, a modulação, a filtragem entre outros (BARIZON, 2005). Basicamente, ela é responsável por transmitir os bits por meio do canal de comunicações, definindo todas as especificações elétricas e mecânicas. Tem como principal função a modulação do sinal para ser transmitido pela onda eletromagnética. Além disso, também realiza a técnica de espalhamento espectral (Spread Spectrum) com o intuito de proteger o sinal contra interferências (SIRUFO, 2004).

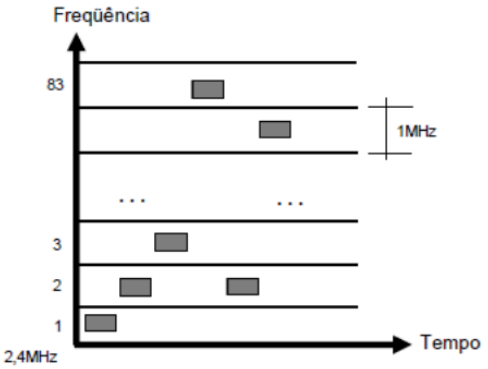
O nível físico pode ser empregado de três formas, sendo duas de radiofrequência baseadas na técnica de espalhamento espectral chamadas de FHSS (Frequency Hopping Spread Spectrum – espalhamento espectral por salto de frequência) e DSSS (Direct Sequence Spread Spectrum – espalhamento espectral por sequência direta) e uma por transmissão de infravermelha difusa (SIRUFO, 2004).

Apesar de permitir uma maior taxa de transferência de dados a transmissão infravermelha possui um comprimento de onda muito pequena o que acaba refletindo em pouco poder de penetração, restringindo seu alcance a cerca de 10 metros em visada direta. Essas características tornam seu uso inviável para redes sem fio fazendo que a transmissão por radiofrequência se torne o padrão adotado em redes sem fio.

A técnica de espalhamento FHSS, ilustrado na Figura 2, consiste na divisão da banda disponível em vários subcanais. A transmissão ocorrerá em curtos intervalos de tempo, onde a estação transmissora e a receptora são sincronizadas para saltar entre os subcanais em uma sequência pseudo-aleatória pré-determinada. No Brasil a largura de banda disponível na faixa de frequência ISM de 2,4 GHz (83,5 MHz) foi dividida em 83 subcanais, nos quais pelo menos 75 desses devem ser utilizados. No caso de um canal estar sobre interferência, os dados são retransmitidos somente no próximo salto ou quando for encontrado um

subcanal limpo. Devido à faixa de frequência utilizada ser bastante poluída pelo uso de aparelho microondas, telefones sem fios e outros equipamentos essa técnica possui baixa taxa de transmissão de dados que podem chegar a no máximo a 2 Mbps (BARIZON, 2005;SIRUFO, 2004).

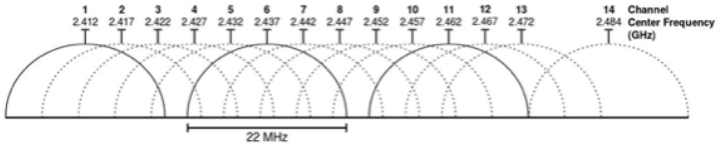
**FIGURA 2 -** Diagrama frequência vs. tempo em FHSS (SIRUFO, 2004).




Na técnica de espalhamento DSSS cada bit recebe um código padrão chamado CHIP antes de ser transmitido. Esse código é conhecido somente pela estação transmissora e receptora o que torna a transmissão mais difícil de ser interceptada. A adição do código torna mais eficiente a correção de erros sem a necessidade de retransmissão e também distribui o sinal ao longo de toda a faixa disponível, tornando-o mais robusto e confiável.

A técnica DSSS também opera na faixa de frequência ISM de 2,4 MHz divididos em 14 canais de 22 MHz de largura de banda com intervalos de 5MHz entre eles. Desse modo as frequências acabam sendo compartilhadas fazendo com que as redes operando em canais muito próximos acabam se interferindo mutuamente (BARIZON, 2005;SIRUFO, 2004).

**FIGURA 3 -** Divisão dos canais na faixa de 2,4 GHz da técnica DSSS (TELECO, 2017).




É importante destacar que essas técnicas de transmissão foram previstas no padrão 802.11 original. Ao longo do tempo, por meio de novas técnicas ou de combinações das já existentes, mudanças na faixa de frequência de operação e dos códigos empregados, vários sub-padrões foram criados pelo próprio IEEE, com a finalidade de se aumentar a velocidade de transmissão, a confiabilidade e a robustez contra interferências do sistema. Entre padrões desenvolvidos, destacam-se como os mais usados os seguintes:

802.11a: trabalha na faixa de frequência ISM de 5 GHz em 8 canais de rádio e permite uma taxa de transferência de dados de até 54 Mbps por canal. Utiliza a técnica OFDM (Orthogonal Frequency Division Multiplexing) onde a largura de banda disponível é dividida em 52 diferentes frequências, sendo 48 para dados e 4 para sincronização. Como vantagem apresenta melhor imunidade por trabalhar a faixa dos 5 GHz (menos sinais interferentes), porém é incompatível com outros padrões 802.11 já existentes além de ter um alcance menor e maior custo dos equipamentos (STANGARLIN, 2012).

802.11b: foi o primeiro padrão utilizado em grande escala (chegou ao mercado antes do 11a) e trabalha na faixa de frequência ISM de 2,4 GHz. Permite uma taxa de até 11 Mbps utilizando a técnica de transmissão DSSS com um alcance máximo estimado em 300 metros. Tem custo dos equipamentos baixo e compatibilidade com outros padrões 802.11 disponíveis. Como desvantagem trabalha em uma faixa de frequência mais poluída sendo assim mais suscetível a interferências (STANGARLIN, 2012).

802.11g: opera na faixa de frequência ISM de 2,4 GHz, associando duas técnicas de modulação, a DSSS e a OFDM (é o que difere do padrão 11b). Permite uma taxa máxima de 54 Mbps adaptativa, onde, ao aumentar a distância de transmissão, a taxa de dados tende a cair mantendo-se a estabilidade do sinal. O emprego da modulação OFDM (melhor eficiência na utilização da banda passante) permitiu velocidades iguais ao padrão 11a mesmo ope-

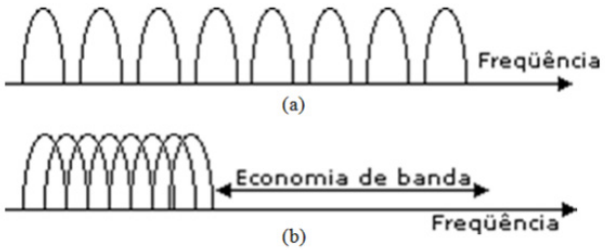
rando na frequência de 2,4 GHz e o mesmo alcance do padrão 11b, o qual é compatível (STANGARLIN, 2012).

802.11n: esse padrão foi criado com o objetivo de atingir velocidades de transmissão maiores do que as redes cabeadas (100 Mbps), além de melhorar o alcance e a confiabilidade. Para isso foi implementado melhorias nos algoritmos de transmissão e a técnica MIMO (Multiple-Input, Multiple-Output) permitindo o uso de vários fluxos de transmissão e recepção de forma paralela (várias antenas para transmitir e receber). Tudo isso aumentou a velocidade de transmissão para 300 Mbps e ainda dobrou o alcance. No padrão 11n pode se operar com canais com largura de banda de 40 ou de 20 MHz (nesse caso com redução da velocidade), e com frequências de 2,4 e 5 GHz, o que o torna compatível com os demais (STANGARLIN, 2012).

Percebe-se que a introdução da técnica de modulação OFDM melhorou substancialmente a velocidade nas transmissões de dados nas redes sem fio.

Ao contrário do que se vê em várias literaturas, o OFDM não se trata de uma técnica de multiplexação como a FDM (Frequence Division Multiplexing) e a TDM (Time Division Multiplexing) que agregam sinais distintos para serem transmitidos por um único meio. Trata-se de uma evolução do FDM. Na multiplexação FDM as frequências das subportadoras necessitam de serem afastadas uma das outras (bandas de guarda), impedindo que os sinais enviados sofram interferência mútua. No OFDM, esse espaçamento não é necessário, uma vez que as frequências das subportadoras se sobrepõem umas nas outras ortogonalmente, tornando-as independentes e possibilitando a identificação de cada subportadora pelo receptor de modo seguro. Na prática, ocorre uma racionalização do uso do espectro, o que permite aumentar a taxa de transmissão de dados com a mesma banda disponível, conforme ilustrado na Figura 4 (CAVALCANTI, 2009). Entre as principais vantagens do uso do OFDM se destacam a maior capacidade de transmissão e a robustez aos ambientes com desvanecimento seletivo em frequência. Como desvantagem apresenta dificuldade de sincronismo das subportadora e sensibilidade aos desvios de frequência (TELECO, 2017).

**FIGURA 4 -** (a) Espectro com oito subportadoras associadas em FDM e (b) Espectro com oito subportadoras associadas em OFDM (TELECO, 2017).




## 3 O INTERFERIDOR SCE 0100 – IACIT

O produto SCE 0100, ilustrado na Figura 5, da fabricante IACIT é apresentado em quatro diferentes modelos. O modelo SCE 0100-D utilizado em aplicações contra drones, SCE 0100-C usado em aplicações contra comunicação celular, SCE 0100-R voltado para aplicações contra RCIED (Remote Controlled Improvised Explosive Device) e o SCE 0100-M empregado em aplicações portáteis contra RCIED e comunicação. Como o foco deste trabalho são aplicações voltadas à interferência de drones o modelo SCE0100-D tem suas características discutidas nesta seção.

O SCE0100–D (DroneBlocker) possui capacidade de bloquear e/ou interferir através dos 6 (seis) canais independentes, Tabela I, e com capacidade de operar simultaneamente, disponíveis ao longo das faixas de frequência comumente utilizada em controles remotos de drones. A ação de bloqueio é realizada por meio de um sinal interferente que realiza uma varredura em toda a faixa de frequência do canal em que estiver operando. A taxa de varredura por cada canal é prevista em manual e também apresentada na Tabela I.

**FIGURA 5 -** Interferidor SCE 0100 (IACIT, 2017)

**TABELA 1 -** Canais de interferência do modelo SCE 0100-D (IACIT, 2016).

| Canal | Faixa de Freq [MHz] | Potência de saída [W] | Taxa de varredura [µs] |
|---|---|---|---|
| 1 | 27-75 | 1/10/100 | 100 |
| 2 | 433-470 | 1/10/100 | 100 |
| 3 | 902-928 | 1/10/50 | 100 |
| 4 | GPS L1/L2/L5 | 1/10 | 20 |
| 5 | 2400-2500 | 1/5/10/25/50 | 150 |
| 6 | 5700-5900 | 1/15 | 50 |

Devido às altas velocidades de varredura a visualização no analisador de espectro mostra uma interferência de barragem em toda a banda do canal em operação, conforme a Figura 6. É importante destacar que, segundo o manual do fabricante, 95% dos drones mais comuns operam nas faixas de frequência de 2,4 e 5,8 GHz (canais 5 e 6). Essas faixas de frequência são as mesmas usadas nas redes sem fios no Brasil e por isso se tornaram alvo desse estudo.

**FIGURA 6 -** Visualização da realização de uma interferência no Canal 1 (IACIT, 2016).


Quanto à antena utilizada para transmissão do sinal interferidor, o equipamento possui dois tipos: uma antena direcional, que atende os dois canais (5 e 6) e duas antenas omnidirecionais, nesse caso uma para cada canal, conforme Figura 7. A antena direcional permite que o operador do interferidor minimize os efeitos colaterais indesejados apontando-a para alvo (drone), poupando dessa forma possíveis redes sem fio que estejam ao redor da antena de transmissão do jammer. Por esse motivo, as análises realizadas nesse estudo serão feitas utilizando antenas omnidirecionais, onde não é possível ter o controle da emissão do sinal interferente. A antena omnidirecional utilizada para o canal 5, conforme Figura 7(a) também atende os canais 2, 3 e 4. Já a antena vista na Figura 7(b) atende somente ao canal 6. Suas características elétricas estão apresentadas na Tabela 2.

**FIGURA 7 -** (a) Antena omnidirecional para a frequência de 2,4 GHz (Canal 5) e (b) Antena omnidirecional para a frequência de 5,8 GHz (Canal 6).

(a)

(b)

**TABELA 2 -** Características elétricas das antenas utilizadas pelo SCE 0100-D (IACIT, 2016).

| Antena omnidirecional para os canais 2,3,4 e 5 | |
|---|---|
| Faixas de frequência | 452-468 MHz (Canal 2)<br>790-960 MHz (Canal 3)<br>1710-2170 MHz (Canal 4)<br>2300-2700 MHz (Canal 5) |
| Ganho | 3 a 6 dBi |
| Polarização | Vertical |
| VSWR | ≤ 2,5:1 |
| Ângulo de meia potência (horizontal) | 360° |

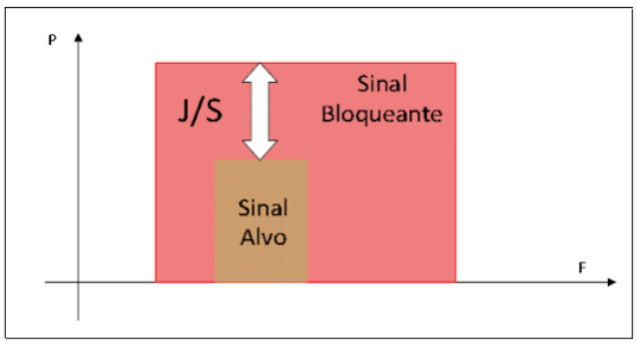
| | |
|---|---|
| Antena omnidirecional para os canais 2,3,4 e 5 | |
| Ângulo de meia potência (vertical): | 25° |
| Antena omnidirecional para o canal 6 | |
| Padrão de irradiação | Omnidirecional |
| Faixa de frequência | 5700-5900 MHz |
| Ganho | 6 dBi |
| Polarização | Vertical |
| VSWR | ≤ 1,5:1 |
| Ângulo de meia potência (horizontal) | 360° |
| Ângulo de meia potência (vertical) | 25° |

## 4 TESTE DE CAMPO

A.Relação Jammer/Signal (J/S)

A relação J/S (Jammer/Signal) determina quantas vezes a potência do sinal interferidor é maior que o sinal alvo, conforme ilustra a Figura 8. Essa relação é comumente expressa em dB. Para ser eficiente em uma interferência sobre um sinal digital, necessita-se que a relação J/S seja igual a 0 dB e que seja realizada pelo menos durante 1/3 do tempo em que o sinal a ser bloqueado esteja transmitindo. Nessas condições, as informações que vão chegar ao demodulador já estarão degradadas o suficiente para que seja interrompida a comunicação de um sinal digital (BRASIL, 2012).

**FIGURA 8 -** Relação J/S (BRASIL, 2012).




B. Setup de Teste

O teste realizado tem como objetivo verificar a possibilidade do equipamento SCE 0100-D interferir em uma comunicação entre dois dispositivos que se comunicam através de uma rede Wi-Fi. Sendo assim, realizou-se a montagem de um setup de teste conforme ilustrado na Figura 9. O equipamento SCE 0100-D foi posicionado a 200 metros de um notebook e um roteador, sendo estes posicionados próximos um do outro uma distância de 1,5 metros. O roteador utilizado foi o modelo D-Link DIR-600, cujas características técnicas são apresentadas na Tabela 3. Em relação ao interferidor, a antena utilizada foi ilustrada na Figura 7 (a). Imagens do Setup de teste podem ser observadas na Figura 10.

**FIGURA 9 -** Esquema de teste de campo.

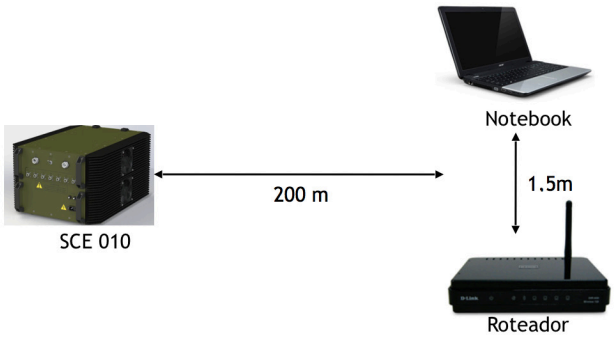



**TABELA 3 -** Características técnicas do roteador D-Link, modelo DIR – 600 (DIR-600, 2010).

| | |
|---|---|
| Fabricante | D-Link |
| Modelo | DIR - 600 |
| Padrões Wi-Fi | 802.11b/g/n |
| Frequência de funcionamento | 2.4 GHz a 2.497 GHz |
| Potência nominal | 14 dBm +/-2 dB |
| Quantidade de antenas | 1 (não removível) |
| Ganho de antena | 5 dBi |

Antes do início do emprego do interferidor realizou-se o teste de conectividade entre o roteador e o notebook, o qual apresentou o resultado esperado de perda nula de pacote de dados, conforme ilustrado na Figura 11.

**FIGURA 10 -** Detalhe antena omnidirecional interferidor SCE 0100 – IACIT e interferidor SCE 0100 – IACIT.

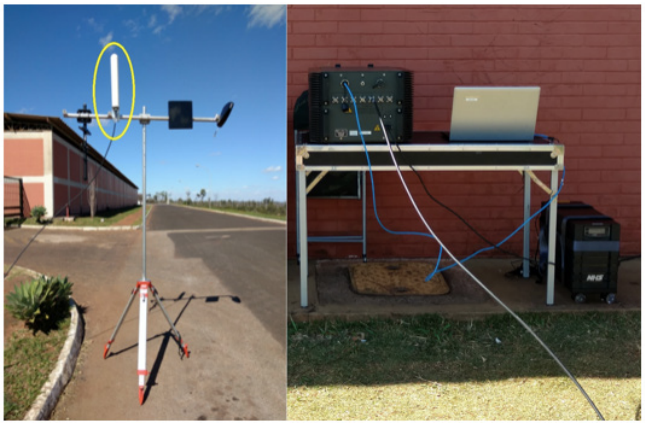
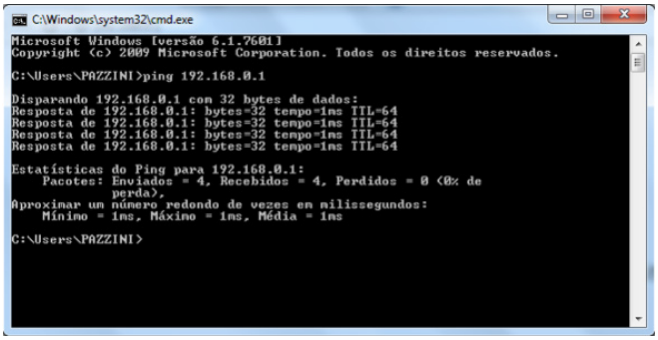


**FIGURA 11 -** Status conexão Wi-Fi com interferidor desligado.




C.Resultados e discussões

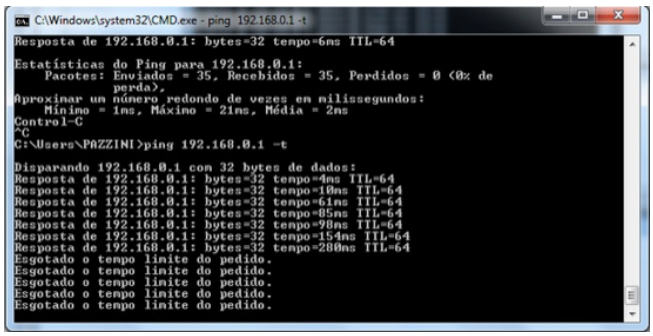
O teste consistiu em observar o status da rede com o interferidor ligado, inicialmente com 1Watt de potência. Em sequência a potência do sinal interferidor, cuja banda foi de 100MHz (2,4 a 2,5 GHz), foi aumentada gradativamente para 5, 10, 25 e 50 Watts. Para cada valor de potência do sinal interferidor um novo teste de conectividade da rede Wi-Fi era realizado entre o roteador e o notebook. Os resultados observados são apresentados na Tabela IV. Observa-se que a comunicação de dados entre o roteador e notebook, sob as condições de setup, sofre interferência para um sinal interferidor com nível de potência maior ou igual a 40dBm. A Figura 12 apresenta o status do teste de conectividade entre o roteador é o notebook para sinal interferidor com nível de potência de 40 dBm.

**TABELA 4 -** Resultados de teste de campo.

| Potência [W] | Potência [dBm] | Distância [m] | Interferência |
|---|---|---|---|
| 1 | 30 | 200 | Não |
| 5 | 37 | | Não |
| 10 | 40 | | Sim |
| 25 | 44 | | Sim |
| 50 | 47 | | Sim |

O teste de campo comprovou que o equipamento SCE 0100 realmente causa interferências em redes Wi-Fi. Percebeu-se ainda que, nem mesmo a técnica de espalhamento espectral utilizada pelos dispositivos Wi-Fi, que oferece certa robustez diante de interferências, foi capaz de permanecer imune ao sinal interferente.

**FIGURA 12 -** Status conexão Wi-Fi sendo interferida.




No manual de operação do software planejador de missões do equipamento SCE 0100, em sua base teórica, encontra-se um modelo de atenuação no espaço livre para distâncias de até 200 metros entre o interferidor e seu alvo, com visada direta, dado por

$$L = 32{,}45 + 20 \cdot \log_{10}[d(\text{km})] + 20 \cdot \log_{10}[f(\text{MHz})], \quad (1)$$

onde d é a distância em km entre o transmissor e o receptor e f a frequência do sinal transmitido em MHz. O manual também apresenta um modelo de propagação dado por

$$P_r = P_t + (G_t + G_r - L_t - L_r) - L, \quad (2)$$

onde Pr é a potência de recepção, Pt é a potência de transmissão Gt e Gr são os ganhos das antenas de transmissão e recepção, respectivamente, e Lt e Lr são as perdas em cabos e conectores dos sistemas de transmissão e recepção, respectivamente (IACIT,

2016).

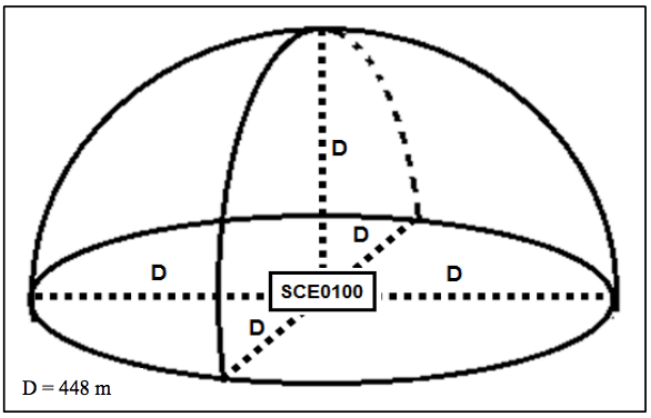
Definida a distância e frequência do sinal pode-se por meio de (1) obter a atenuação no espaço livre para o setup de teste, sendo este valor de 86,254 dB. Em seguida é possível obter a potência recebida pelo roteador por meio de (2). Considerando os valores de ganho, perdas e potência de transmissão apresentados na Tabela V e a atenuação calculada anteriormente, obtém-se como potência de recepção -39,854 dBm. Em tese, de acordo com o teste realizado, essa é a potência necessária no alvo para interromper a comunicação entre o roteador e o notebook. Esse nível de sinal passa a ser o valor de referência para que haja interferência.

**TABELA 5 -** Dados práticos dos equipamentos.

| | |
|---|---|
| Antena Omnidirecional do SCE 0100 | |
| Ganho | 4,5 dBi (valor médio) |
| Antena roteador | |
| Ganho | 5 dBi (data sheet) |
| Cabo de transmissão do SCE 0100 | |
| Atenuação | 0,5 dB/m (5 metros) |
| Conector SCE 0100 | |
| Atenuação | 0,3 dB/conector (2 conectores) |
| Interferidor SCE 0100 | |
| Potência de TX | 10W (40 dBm) |
| Frequência de Operação | |
| SCE 0100 (2,4 a 2,5 GHz) | Roteador (2,45 GHz) Freq. Média |

Após a realização do teste, constatou-se que o equipamento SCE 0100 realmente é capaz de provocar um efeito colateral indesejável em redes Wi-Fi durante o seu uso normal (atuar tendo como alvo os drones). Com a finalidade de se obter a distância máxima que a interferência causada pelo SCE 0100-D pode alcançar, dentro das condições colocadas em teste, por meio de (1) e (2) e com os dados disponíveis é possível encontrar tal distância. Para isso, adota-se o valor de potência recebida que permite causar interferência no alvo, neste caso Pr = -39,854 dBm. Para determinar o máximo alcance utiliza-se a potência máxima fornecida pelo equipamento SCE 0100-D em sua saída, ou seja, 50 W/47 dBm. Logo, obtém-se uma distância de 448 metros o que supostamente seria capaz de gerar uma região de interferência conforme ilustrado na Figura 13.

**FIGURA 13 -** Região de interferência efetiva com 50 W de potência (BARBOSA, 2017).




É importante observar que esses dados, em tese, só teriam validade nas mesmas condições em que foi realizado o teste de campo, no caso, a visada direta entre o interferidor e o roteador, sendo esse com características semelhantes ao D-Link DIR 600.

## CONCLUSÕES

O presente trabalho apresenta um estudo prático sobre a interferência do equipamento SCE 0100- D, utilizado em aplicações contra drones, em redes Wi-Fi próximas. Neste contexto, foram apresentadas algumas situações que demonstram como os drones podem ser utilizados em atividades terroristas. Estudou-se o padrão das redes sem fio IEEE 802.11 e alguns aspectos da camada física deste padrão. O equipamento interferidor SCE 0100-D também teve suas características estudadas. Em sequência foi realizada a configuração de um setup de testes que permitiu obter o nível de potência mínima do sinal interferidor capaz de impedir a comunicação de dados entre um roteador e um notebook.

Durante a realização do teste verificou-se que o equipamento realmente causa interferências em conexões Wi-Fi. O referido teste também trouxe, em tese, uma distância máxima de referência para que haja interferência

quando reproduzidas as condições definidas no teste executado (visada direta e roteador D-Link DIR-600). Essa distância foi definida em aproximadamente 448 metros e pode ser considerada pelos planejadores e operadores quando o equipamento for empregado em um cenário urbano, onde o efeito indesejável de interferências em redes Wi-Fi comerciais e domésticas é mais provável.

O teste de campo levou em consideração a interrupção total da conexão Wi-Fi entre um roteador e um notebook. Porém, em uma interferência externa em uma conexão Wi-Fi que não seja forte o suficiente para causar a interrupção do sinal, pode levar a uma perda considerável na qualidade do canal, causando lentidão para o usuário. Dentro dessa ótica, é válido considerar que os efeitos colaterais podem ser muito superiores aos 448 metros levantados.

Como trabalhos futuros propõe-se a realização de um estudo de interferência acidental em redes Wi-Fi indoor pelo uso do interferidor SCE 0100-D, simulação da área de interferência causada pelo interferidor e o estudo e obtenção da distância máxima de atuação do interferidor com o uso de antena direcional.

## REFERÊNCIAS


ARAUJO Luiz Albert, et al – **Desafios da defesa e segurança frente à nova ameaça do uso ilícito de VANTs**. Disponível em: <http://www. defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xii_cadn/desafios_da_defesa_segurana_vants.pdf> Acesso em: 29 de abril 2017.

BARBOSA, Ricardo Luís; MARINS, Carlos Nazareth Motta – **Análise do campo de ação de um interferidor de RF sobre um receptor GPS de drone**. VI SRST – Seminário de Redes e Sistemas de Telecomunicações, INATEL, Julho 2017.

BARIZON, Ben-Hur Monteiro. PONTIFÍCIA UNIVERSIDADE CATÓLICA, Rio de Janeiro-RJ, 3-Redes locais sem fio IEEE 802.11, Certificação Digital nº 0124845/CA. Disponível em: <https://www.maxwell.vrac.puc-rio.br/5688/5688 _4.PDF> Acesso em: 26 de abril de 2017.

Brasil. Ministério da Defesa. Exército Brasileiro. Centro de Instrução de Guerra Eletrônica – Manual de Ensino de Guerra Eletrônica, Brasília – DF, 2012.

CAVALCANTI Arthur Barreto de Rangel Moreira. **Uma avaliação da interferência entre redes 802.11g**, Recife - PE, 2009.

DEFESANET. DRONES, Novo sistema promete derrubar Drones invasores em até 15 segundos. Agosto de 2016. Disponível em: <http://www.defesanet.com.br/vant/noticia/23362/Novo-sistema-promete-de rrubar--drones-invasores-em-ate-15-segundos/> Acesso em: 22 de dezembro de 2016.

_____. DRONES, Drones assassinos: a maior ameaça terrorista à segurança dos jogos Olímpicos e Para olímpicos. Julho de 2016. Disponível em: <http://www.defesanet.com.br/vant/noticia/22944/Drones-assassinos--a-maior-ameaca-terrorista-a-seguranca-dos--Jogos-Olimpicos-e-Paraolimpicos-/> Acesso em: 22 dezembro de 2016.

_____, Forças Armadas: Autorizadas a usar bloqueadores de celular nas Olimpíadas e GLO. Janeiro 2016. Disponível em: <http://www.defesanet.com.br/eventos/noticia/21411/Forcas-Armadas--Autori zadas--a-usar-bloqueadores-de-celular-nas-Olimpiadas-e--GLO/> Acesso em: 20 de abril de 2017.

IACIT Soluções Tecnológicas S/A - Manual Técnico do Produto equipamento SCE 0100.

_____. Manual de Operação do Software IHM SCE 0100.

_____. Manual de Antenas do equipamento SCE 0100.

_____. Manual Técnico do software planejador de missões para o equipamento SCE 0100.

LEONNIG, Carol D.; WHITLOCK, Craig. Drone incident at White House highlights long-studied, still-unsolved security gap. The Washington Post, 26 jan. 2015. Disponível em: <http://www.washingtonpost.com/politics/drone-incident-at-white-house-highlights-long-studied--still-unsolved-security-gap/20 15/01/26/e d2e7f9e-a-594-11e4-a7c2-03d37af98440_story.html>. Acesso em: 26 de abril de 2017.

OLIVEIRA, Gilberto de Jesus. **O Drone como fator de risco decorrente de condições não previstas na segurança radiológica em Grandes Eventos**, Rio de Janeiro, 2015.

NARDIN, Marcelo de. **Análise comparativa entre redes sem fio locais e metropolitanas**, camada física, Porto Alegre, 2008.

SHANKAR, Sneha. Japan Arrests Yasuo Yamamoto For Landing Radioactive Sand-Laced Drone On Shinzo Abe's Office Roof. International Business Times, 25 abr. 2015. Disponível em: <http://www.ibtimes.com /japan--arrests-yasuo-yamamoto-landing-radioactive-sand-laced-drone-shinzo-abes-office-1896688>. Acesso em: 26 de abril 2017.

SIRUFO, Sergio Henrique. PONTIFÍCIA UNIVERSIDADE CATÓLICA, Rio de Janeiro-RJ, 2-Padrão IEEE 802.11, Certificação Digital nº 0210420/CA. Disponível em: <https://www.maxwell.vrac.puc-rio.br/7589/7589_3.PDF> Acesso em: 26 de abril de 2017.

STANGARLIN Douglas Pegoraro. Análise de desempenho de redes sem fio com diferentes protocolos de criptografia: um estudo de caso, Santa Maria – RS, 2012.

TELECO. Seção Tutoriais Regulamentação – Regulação do Espectro: Uso Não-Licenciado. Disponível em: <http://www.teleco.com.br /tutoriais/tutorialespecradio/pagina_2.asp > Acesso em: 29 de abril de 2017.

_____. Seção Tutoriais Banda Larga. Redes WiFi II: Tecnologias RF para 802.11 Disponível em: <http://www.teleco.com.br/tutoriais /tutori alwifimanaus2/pagina_3.asp> Acesso em: 29 de abril de 2017.

_____._____. Redes WiFi: Espectro de Frequências ISM. Disponível em: <http://www.teleco.com.br/tutoriais/ tutorialredeswifi1/pagina_5.asp> Acesso em: 25 de abril de 2017.