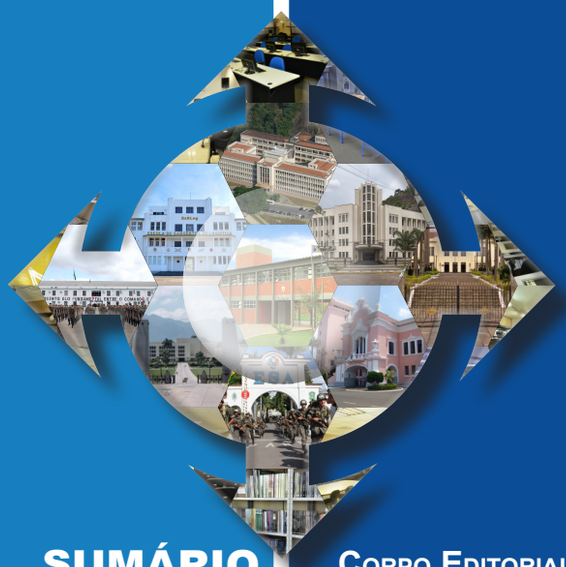
ISSN 2594-3952



O Comunicante

SUMÁRIO

Revista Científica da Escola de Comunicações
Escola Coronel Hygino Corsetti

VOLUME 9 - Nº 2
Junho 2019

ISSN 2594-3952

O Comunicante

SUMÁRIO

Revista Científica da Escola de Comunicações

Escola Coronel Hygino Corsetti

VOLUME 9 - Nº 2

Junho 2019

O COMUNICANTE
Revista Científica da Escola de Comunicações

Ano 9 - Nº 2

Junho 2019

ISSN 1968-6029

ISSN 2594-3952 (Digital)

Escola de Comunicações - EsCom

Escola Coronel Hygino Corsetti

EDITORIAL

A presente edição da Revista “O Comunicante” contém uma ampla variedade de artigos, contemplando diversas áreas de interesse das comunicações militares como telecomunicações, cibernética e doutrina. Todos esses temas são de extrema relevância para atividade de Defesa Nacional.

Nesta publicação, é dada a devida importância à atividade Cibernética, peça fundamental para a capacidade operativa da Força que vem adquirindo notoriedade, quer seja pelo seu alto grau de complexidade ou pela busca incansável da geração de capacidades que possibilitarão ao Exército Brasileiro atingir o estágio condizente a uma Força militar da era do conhecimento.

O desenvolvimento de novas tecnologias que contribuem para a evolução das telecomunicações é abordado em textos de fácil leitura, contribuindo para a atualização dos conhecimentos técnicos dos leitores que lidam com o desafio de prover o apoio de comunicações ao exercício do Comando e Controle.

Destaca-se, ainda, a apresentação de conteúdos relacionados à Doutrina Militar Terrestre que resgatam a experiência de militares do Exército Brasileiro que recentemente estiveram em atividades no exterior e somam ao nosso conhecimento aspectos relacionados ao Comando e Controle de outras Forças Armadas.

O Comando da Escola de Comunicações agradece a contribuição de todos que submeteram os artigos para análise e aproveita para convidar o público em geral a contribuir com trabalhos acadêmicos nas futuras edições desta revista.

Uma boa leitura a todos.

RODOLFO ROQUE SALGUERO DE LA VEGA FILHO - Cel
Comandante da Escola de Comunicações

EXPEDIENTE

A Revista Científica, O Comunicante, publicada pela Escola de Comunicações, busca incentivar pesquisas científicas nas áreas afetas à Defesa e que contribuam para o desenvolvimento da Arma de Comunicações.

OBJETIVOS

Promover o viés científico em áreas do conhecimento que sejam de interesse da Arma de Comunicações e, consequentemente, do Exército Brasileiro.

Manter um canal de relacionamento entre o meio acadêmico militar e civil.

Trazer à reflexão temas que sejam de interesse da Força Terrestre e que contribuam para a Defesa.

Publicar artigos inéditos e de qualidade.

Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos Corpos de Tropa.

PÚBLICO-ALVO

A revista está voltada a um amplo espectro de pesquisadores, professores, estudantes, militares, bem como profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, Informática, História Militar, com ênfase em Comunicações e Equipamentos de Comunicações, Instrução Militar, Gestão, Meio Ambiente, Operações Militares Conjuntas e Singulares.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo a outra revista, ele deverá consultá-la e certificar-se de não estar ferindo direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

Os artigos submetidos são avaliados pela Comissão Editorial, no que se refere ao seu mérito e adequação às regras de apresentação de trabalhos científicos.

Em seguida, os textos são encaminhados aos pareceristas que terão o prazo de 30 dias para fazerem a avaliação. Os pareceristas não são remunerados e, caso aceitem participar, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista. A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos, além de sugerir mudanças eventuais de modo a adequar os textos.

Os textos submetidos devem vir acompanhados de carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de estar concorrendo a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta revista.

Outrossim, nenhum dos organismos editoriais, organizações de ensino e pesquisa ou pessoas físicas envolvidas nos conselhos, comitês ou processo de editoração e gestão da revista se responsabilizam pelo conteúdo dos artigos seja sob forma de ideias, opiniões ou conceitos, devendo ser de inteira responsabilidade dos autores dos respectivos textos.

PERIODICIDADE

A revista tem periodicidade quadrimestral (fevereiro, junho e outubro) e se reserva ao direito de realizar edições especiais, além das previstas.

O Comunicante - Revista Científica da Escola de Comunicações - Volume 9, Nº 2 (Jun/2019)
Brasília-DF: Escola de Comunicações. 2019 47p; 29,7 cm X 21,0 cm

Publicação Quadrimestral
ISSN 1968-6029 ISSN 2594-3952(Digital)
Revista Científica da Escola de Comunicações
1. Escola de Comunicações 2. Defesa 3. Cibernética 4. Ciência & Tecnologia 5. Doutrina 6. Direito 7. Educação 8. Informática 9. Instrução Militar 10. Gestão 11. Meio Ambiente 12. Operações Militares Conjuntas e Singulares.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

A GUERRA CIBERNÉTICA E O VÍRUS STUXNET: TRATA-SE DE USO DA FORÇA?

Vinícius Chitolina
Graduado em Ciências Militares

RESUMO: Um ataque cibernético pode ser definido como uma ação direcionada a redes ou qualquer outro meio de comunicação e informação, podendo ser considerados atores estatais e atores não estatais. Contudo, o fato de essas ações serem consideradas como uso da força segundo a cartilha da Organização das Nações Unidas ainda é um ambiente nebuloso, ou seja, não há definições exatas. O objetivo desse artigo é analisar o uso da força em ataques cibernéticos. Levando em consideração o "Critério de Schmitt" para análise, o artigo visa verificar se o vírus Stuxnet pode ser classificado como tal. Uma possível hipótese é que ataques cibernéticos podem ser considerados uso da força, segundo o que normatiza a própria cartilha da Organização das Nações Unidas. Esta análise indicará que poderia importante ser ampliado o escopo do artigo 2 inciso 4 da cartilha da ONU, a qual apresenta uma estrita visão do que seria considerado uso da força, especialmente quando levamos em consideração o espaço cibernético, onde uma simples ação de pequeno custo pode causar um dano gigantesco. Além disso, o "Critério de Schmitt" provou ser uma importante ferramenta para analisar o uso da força em ataques cibernéticos, mesmo com diversos problemas como a origem da ação, a mensurabilidade dos efeitos cinéticos do ataque a e severidade da ação que se faz difícil de determinar. Muitas das vezes ataques cibernéticos não destroem o objetivo, mas somente danificam ou roubam informações do alvo, e consequentemente os efeitos podem ser muito piores que a destruição. A hipótese que os ataques cibernéticos podem ser considerados como uso da força foi parcialmente confirmada, tendo em vista a dificuldade em qualificar no contexto do ataque o uso da força, devido as várias variáveis que o envolvem.

Palavras-chave: Analisar. Ataque Cibernético. Escopo. Stuxnet. Uso da força

INTRODUÇÃO

Um dos principais problemas que encontramos em qualificar e quantificar ataques cibernéticos dentro do contexto do recurso à guerra, que seria o que motiva um país à guerra, ou o também chamado uso da força (como denominado na Carta das Nações Unidas) é a falta de literatura e manuais existentes sobre o assunto e também a regulação do escopo que a própria Carta de São Francisco (outro nome dado ao acordo que formou a Organização das Nações Unidas) nos dá, que não engloba ainda ataques cibernéticos para estes fins, podemos atribuir isso ao fato de o tema ser relativamente novo e estar sob intenso debate ao redor do mundo.

Um ataque cibernético pode ser definido como qualquer ação direcionada a redes ou qualquer outro meio de comunicação (ZIOLKOWSKI, 2012) podendo ser considerados atores estatais e não estatais. De qualquer modo, a definição se ele pode ser verificado como uso da força, ou um recurso ou arma da guerra ainda não foi bem definido, o ambiente ainda é de certa forma nebuloso.

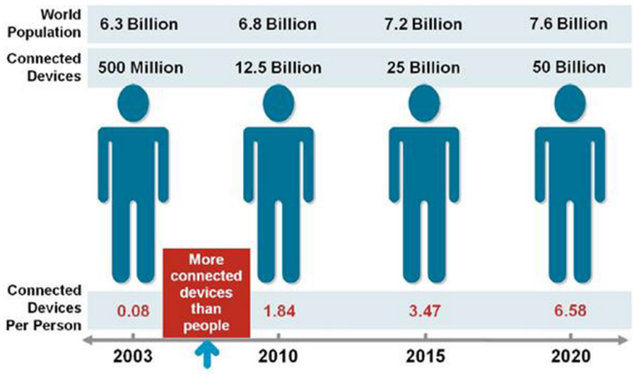
O objetivo desse artigo é analisar se ataques cibernéticos podem ser enquadrados como uso da força segundo o que regulamenta a Carta das Nações Unidas, gerando assim o direito à legítima defesa por parte do atacado, por exemplo. Levou-se em consideração o "Critério Schmitt" para esta análise. O artigo visa checar se o ataque com o vírus Stuxnet pode ser considerado neste contexto.

Esse tema é relevante tendo em vista a crescente importância dada ao assunto em vários países ao redor do mundo, os quais têm investido bilhões de dólares em defesa cibernética (SPUTNIK BR, 2017) depois de ter sofrido diversas ações cibernéticas em seus

sites na internet – como por exemplo os sofridos pelos países da Organização do Tratado do Atlântico Norte, durante a guerra de Kosovo (NATO REVIEW, 2017).

Vive-se em um mundo imerso em tecnologia e sendo guiado para o que se chama de Internet das Coisas, a qual estima-se que até 2020 haverá cerca de 50 bilhões de dispositivos conectados na internet (ALECRIM, 2016). Portanto, faz-se importante o desenvolver deste artigo, baseando-se na Carta da Organização das Nações Unidas, mais precisamente no Artigo 2, inciso 4.

FIGURA 1 Gráfico Comparativo População Mundial x Dispositivos Conectados



Fonte: Cisco IBSG, 2011.

A hipótese é que ataques cibernéticos podem ser enquadrados como uso da força, de acordo com a Carta de São Francisco e suas características.

1 METODOLOGIA

Foi desenvolvida uma pesquisa bibliográfica. Nossas maiores referências são: a própria Carta da Nações Unidas, mais precisamente o artigo 2, inciso 4; o Manual Tallinn em Operações Cibernética; e a opinião de especialistas no assunto como Michael N. Schmitt (MICHAEL, 2013).

2 FUNDAMENTAÇÃO TEÓRICA

O trabalho baseou-se primordialmente na própria Carta de São Francisco da ONU, que teve como objetivo transferir o monopólio da força legítima de cada Estado para um gendarme mundial. Muitas vezes legitimando guerras e atos hostis.

Sustentou-se também na Regra 11 do "Tallinn Manual on the International Law Applicable to Cyber Warfare", que versa sobre a aplicabilidade da lei internacional na resolução de ciberconflitos. Mais especificamente no jus ad bellum (dita sobre as razões aceitáveis para um país entrar em guerra) e o jus in bello (regula as condutas aceitáveis nos conflitos armados).

Artigo 2, inciso 4 da Carta da Organização das Nações Unidas, que afirma:

> "Todos os membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas." (NAÇÕES UNIDAS, 1945)

Regra 11 do "Tallinn Manual on the International Law Applicable to Cyber Warfare", o qual provém o "Critério Schimitt" para análises de uso da força. Ele afirma que para se afirmar se a ação pode ser considerada uso da força, devemos responder uma série de perguntas as quais são encontradas no próprio manual (transcrição não literal, adaptada e traduzida para Português):

> Fatores propostos que influenciam assertivas sobre o uso da força (não é um critério formal). Severidade: quantas pessoas morreram? Quão grande foi a área afetada? Imediatividade: quão breve foram sentidos os efeitos da operação cibernética? Diretividade: a ação tem proximidade com os efeitos causados? Invasividade: a ação cibernética penetrou em uma rede que deveria ser segura? Foi o loco da ação o país atingido? Mensurabilidade dos efeitos: como os efeitos podem ser quantificados? Os efeitos são uma ação distinta ou provém de ações paralelas? Caracterização militar: a ação foi conduzida por militares? Envolvimento estatal: o Estado está diretamente ou indiretamente envolvido na ação em questão? Presunção de legitimidade: essa ação pode ser ca-

racterizada como uso da força, ou não pode ser caraterizada como uso da força? (MICHAEL, 2013).

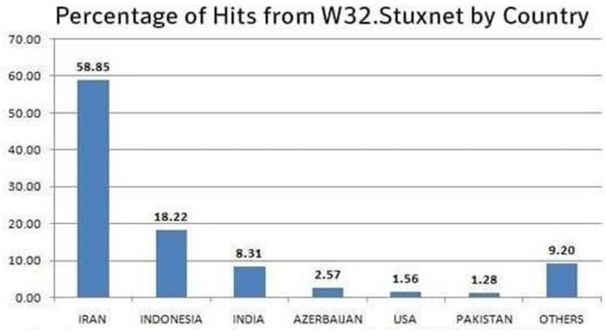
O critério acima exposto é de suma importância para o desenvolvimento do artigo, tendo em vista ser utilizado para a verificação se uma ação cibernética é cabida no contexto de uso da força. E a qualificação da ação, sob égide da ONU, iria legitimar ou não uma ação cibernética. O trabalho desenvolveu-se em cima desses dois documentos, procurando verificar e analisar a ação do vírus Stuxnet e suas consequências.

3 ANALISANDO O STUXNET VÍRUS PELO "CRITÉRIO SCHMITT". FUNDAMENTAÇÃO TEÓRICA

O vírus Stuxnet pode ser considerado como um divisor de águas, podendo ser definido como um dos primeiros ataques cibernéticos em tempos de paz. De acordo com reportes, o vírus foi especificamente desenvolvido para atingir instalações nucleares no Irã, atrasando em anos o programa nuclear iraniano.

Na figura abaixo verificamos a porcentagem de máquinas infectadas por país, e verifica-se que grande parte dos ataques se direcionaram para o Irã, país onde estavam as usinas nucleares alvo dos ataques.

FIGURA 2 Porcentagem de máquinas infectadas por país



Fonte: Symantec, 2017

Severidade: considerando este critério, o Stuxnet pode ser considerado como uso da força, pelo fato dos severos danos cinéticos causados às instalações nucleares do Irã.

Imediatividade: o ataque levou considerado tempo para atingir seu alvo, demorou certo tempo para ser descoberto, então não pode ser considerado como uso da força.

Diretividade: há ligação direta do vírus Stuxnet com a danificação das centrífugas, então pode ser considerado como uso da força. “Os principais alvos do vírus são sistemas de controle de automação e monitoramento industrial, conhecidos pela sigla SCADA” (ROHR, 2011).

Invasividade: foi extremamente invasivo, uma significante intrusão na soberania iraniana que atingiu uma rede não conectada na rede mundial de computadores e um sistema extremamente seguro. Logo, pode ser considerado como uso da força. “Cada tipo de usina de enriquecimento de urânio usa esse sistema numa configuração particular. E o vírus foi programado para atacar só a configuração que as usinas do Irã usam” (VERSIGNASSI, 2011).

Mensurabilidade: houve uma considerável taxa de falha nas centrífugas, logo pode ser considerado como uso da força. “Foi nessas centrífugas que foi testada a eficiência do worm Stuxnet, malware de computador que teria danificado cerca de um quinto das centrífugas iranianas” (TEIXEIRA, 2011).

Caracterização militar: não há evidências que comprovem engajamento militar no ataque, até mesmo devido à própria natureza de ações cibernéticas, onde há uma grande dificuldade de verificar de onde o ataque surgiu, então, não pode ser considerado uso da força se baseando nesse aspecto.

Envolvimento estatal: não há evidências de que houve um país envolvido no ataque, mas pelas marcáveis características do vírus, há a possibilidade de algum envolvimento estatal, contudo, no caso, o Stuxnet não pode ser considerado uso da força. “O malware Stuxnet reconhecidamente foi a mais sofisticada ciber-arma já desenvolvida e aparentemente foi uma obra conjunta de diversos autores espalhados em vários continentes.” (TEIXEIRA, 2011).

Presunção de legitimidade: o uso do Stuxnet não há presunção de legitimidade, devido a ação não ter sido desencadeada devido a propósitos de auto defesa nem autorizado pelo Conselho de Segurança da Organização das Nações Unidas. E até mesmo nestes casos, pode ser considerado como não amparado, ou fora da regulamentação, considerando que não há qualquer consentimento da comunidade internacional em ataques que causem danos a instalações nucleares de outros Estados.

Baseando-se nessas assertivas, nós podemos concluir que muitos Estados provavelmente considerariam o vírus Stuxnet como sendo uso da força, principalmente pelas suas características únicas e sua severidade, a qual destruiu cerca de mil reatores nucleares. (SHUBERT, 2011).

Os critérios, acima adotados para a análise, são subjetivos, cabendo a cada Estado a aplicabilidade deles. Tais critérios servem como um direcionamento para que no futuro possam ser definidas, de maneira mais clara e objetiva, as ações cibernéticas que podem ou não serem consideradas como arma de guerra e uso da força.

CONCLUSÃO

Esta pesquisa visou analisar o uso da força em ataques cibernéticos, de acordo com o “Critério Schmitt”. Assumindo que ataques cibernéticos podem ser considerados como uso da força, nós aplicamos esses critérios para analisar o ataque do vírus Stuxnet, com a intenção de classificá-lo como uso da força, se aplicável.

A hipótese de que ataques cibernéticos podem ser considerados como uso da força foi parcialmente confirmado, devido às dificuldades em qualificar o contexto do ataque como uso da força, dado as diversas variáveis que o envolvem.

Apesar de tudo isso, o “Critério Schmitt” provou ser uma importante ferramenta para analisar o uso da força em ataques cibernéticos. Entretanto, problemas tais como: definir a origem do ataque; a mensurabilidade dos efeitos cinéticos; e a severidade da ação;

dificultam essa análise. Isso se deve, principalmente, ao fato de que muitas vezes os ataques cibernéticos não destroem, mas tão somente desabilitam ou roubam informações do alvo em questão, e os efeitos podem ser muito mais danosos do que a destruição propriamente dita.

Finalmente, a análise realizada indica que seria importante expandir o escopo do artigo 2, inciso 4 da Carta da Organização das Nações Unidas, que apresenta uma visão estrita do que pode ser considerado como uso da força. Especialmente quando nós levamos em consideração as características do espaço cibernético, onde uma ação simples e de baixo custo pode gerar um grave poder de destruição.

THE CYBER-WAR AND THE STUXNET VIRUS: IS IT A USE OF FORCE?

ABSTRACT: A cyber-attack could be defined as some action directed to networks or any other means of communication and information considering state actors and non-state actors. However, whether this should be seen as use of force is still undetermined. This article's objective is to analyze the use of force in cyber-attacks. Taking into account the "Schmitt Criteria" for analysis, it aims at checking if the Stuxnet virus attack could be classified as it. The hypothesis is that cyber-attacks can be considered according to the UN Charter due to its characteristics. The analysis indicated that it would be important to expand the scope of the Article 2(4) UN Charter, which presents a strict view of what may be considered use of force. Especially when we take into account the cyberspace, where a simple and low cost action can have a great power of destruction. Although "Schmitt Criteria" proved to be an important tool to analyze the use of force in cyber-attacks, issues such as the origin of the attack, the measurement of the kinetic effects and severity of the action were difficult to determine. Mainly because sometimes a cyber-attack do not destroy but only disable or steal information from the target, and the effects of it may be even worse than the destruction. The hypothesis that the cyber-attacks could be considered use of force was partially confirmed, because of the difficulties in qualifying the context of the attack as use of force, due to the many variables involved in it.

Keywords: Analyze. Cyber-Attack. Stuxnet. Use of Force.

REFERÊNCIAS

ALECRIM, Emerson, O que é Internet das Coisas (Internet of Things)? 2016. Disponpivel em: . Acesso em 3 de novembro de 2017;

MICHAEL N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge, NY: Cambridge, 2013;

NATO REVIEW. New threats: the cyber-dimension. Disponível em . Acesso em: 1 de novembro de 2017;

NAÇÕES UNIDAS, Carta das Nações Unidas. San Francisco, CA: UN, 1945;

ROHR, Altieres. Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. 2010. Disponível em: . Acesso em 2 de novembro de 2017.

SHUBERT , Atika. Cyber warfare: A different way to attack Iran's reactors. 2011. Disponível em . Acesso em 2 de novembro de 2017.

SPUTNIK BR. Segurança cibernética e satélites custarão à otan 3 bilhões de euros. Disponível em . Acesso em: 1 de novembro de 2017;

TEIXERA, Carlos Alberto. Vírus Stuxnet, que atacou usinas nucleares no Irã, foi criado em parceria por EUA e Israel. 2011. Disponível em: . Acesso em 2 de novembro de 2017;

VERSIGNASSI, Alexandre. Vírus entra em programa nuclear e salva o mundo. 2011.Disponível em: . Acesso em 2 de novembro de 2017.

ZIOLKOWSKI, Katharina. Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-criteria" for Use of Force, Tallinn, EE: NATO, 2012

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras – Resende – RJ. Atualmente, está servindo no 1° Batalhão de Guerra Eletrônica e pode ser contactado pelo email: chitolina.vinicius@eb.mil.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

GEOPOSICIONAMENTO DE SMARTPHONE NO C2 EM COMBATE 6.0: UM INTEGRADOR EM LINGUAGEM DE PROGRAMAÇÃO PYTHON

Adrian Lima Corcino dos Santos[1], Osvaldo Tenorio Vilela da Costa[2]

Pós-graduado em Gestão de Sistemas Táticos de Comando e Controle[1], Pós-graduado em Gestão de Sistemas Táticos de Comando e Controle[2]

RESUMO: Este documento apresenta uma sugestão de desenvolvimento de aplicativo que seja capaz de geoposicionar um smartphone no programa C2 em Combate 6.0, assim como é realizado no sistema Pacificador. Para isso foram realizadas capturas de tráfego de rede do rádio Harris 7800V-HH enquanto transmitia informações de coordenadas geográficas para um servidor emulado do C2 em Combate, as quais foram extraídas e armazenadas. Em seguida foi desenvolvido um script em linguagem de programação Python que captura as coordenadas geográficas reais do smartphone e o envia, no mesmo formato transmitido pelo rádio, para o servidor de posições do C2 em Combate, que o detecta como um equipamento rádio ativo e geoposicionado. Este estudo teve como propósito demonstrar a possibilidade de se realizar a mesma funcionalidade fornecida pelo aplicativo Pacificador Móvel, que até o momento inexiste oficialmente no sistema do C2 em Combate. Concluiu-se, portanto, que é possível replicar a utilidade do aplicativo Pacificador Móvel para outros sistemas de comando e controle do Exército, fornecendo um meio de alternativo de equipamento, além do rádio, economizando recursos e ampliando as capacidades de consciência situacional do sistema.

Palavras-chave: Comando e Controle, C2 em Combate, Python, Geoposicionamento.

INTRODUÇÃO

O presente trabalho trata sobre comando e controle, campo de pesquisa inserido na área de concentração Ciência e Tecnologia, conforme a Portaria nº 734, Art. 4º, inciso VI, de 19 de agosto de 2010, do Comandante do Exército.

Esta pesquisa tem como justificativa a inexistência de um aplicativo que integre dispositivos móveis ao software C2 em Combate, semelhante ao Pacificador Móvel no sistema Pacificador.

Com isso estabeleceu-se o objetivo de sugerir o desenvolvimento de um aplicativo capaz de, ao menos, geoposicionar smartphones no software C2 em Combate, ampliando as possibilidades de emprego e economizando equipamentos rádios.

Mais especificamente, este trabalho demonstra que é possível interoperar entre o software e o dispositivo móvel, mesmo que não tenha sido projetado para isso.

Dessa forma, o escopo do tema visa contribuir com elementos de consciência situacional aplicados no software de comando e controle do Exército

Contudo, este trabalho se limita a fornecer uma aplicação simplificada ao propósito de geoposicionamento do dispositivo móvel e deixa aberta para futuras pesquisas que queiram desenvolver a aplicação ou simplesmente incrementar funcionalidades ao código exposto.

1 METODOLOGIA

Este trabalho utilizou o método indutivo para formulação da pesquisa, iniciando-se por uma pesquisa documental e exploratória a

respeito da linguagem de programação em Python e suas aplicações

Após isso, foram feitas pesquisas laboratoriais onde foi emulado um servidor de C2 em Combate, versão 6.0, no programa VirtualBox e em seguida realizadas as capturas de tráfego de rede entre o Equipamento Rádio Harris 7800V-HH e o servidor.

Primeiramente, os dados coletados da captura foram analisados de forma a compreender efetivamente o que significava cada informação para que pudessem ser utilizadas posteriormente.

Após a completa compreensão dos dados, foi escrito um script em Python, para que os enviasse ao servidor de posições do C2 em Combate, simulando o Equipamento Rádio Harris 7800V-HH, e foi verificado que o servidor o reconhecia como um rádio legítimo e ativo.

Para atingir o objetivo de se replicar a funcionalidade do aplicativo Pacificador Móvel, o script foi adaptado para a plataforma Android em que, ao mesmo tempo que captura as informações geográficas do GPS do smartphone, as envia para o servidor do C2 em Combate, que também o detecta como um rádio e o geoposiciona em seu mapa.

2 DISCUSSÃO E RESULTADOS

2.1 C2 EM COMBATE

O programa C2 em Combate é um software de Comando e Controle pertencente ao Sistema Militar de Comando e Controle (SISMC²) (BRASIL, p. 20) que tem por finalidade fornecer dados em tempo real sobre as operações correntes provendo consciência situação e servindo de apoio à decisão às autoridades que comandam as operações.

Esse software é capaz de prover recursos de planejamento e gerenciamento de operações militares, por ser capaz de fornecer serviços de apresentação de mapas digitais, cartas topográficas ou imagens georreferenciadas ao mesmo tempo que dispõem sobre eles instalações, unidades, veículos, pessoas e equipamentos de emprego militar.

Outra capacidade é que o C2Cmb fornece a possibilidade de interoperar com equipamentos rádios que enviam suas coordenadas geográficas e são dispostos, em tempo real, no mapa, além de ser capaz de emitir relatórios e documentos oficiais de operação.

Não obstante, o software é escalonado hierarquicamente, permitindo que informações sejam inseridas no contexto em que as frações de subordinadas possam replicá-las aos escalões superiores, que as visualizam e as filtram se assim desejarem.

Neste trabalho, foi criada uma máquina virtual com 80 Gb de HD e 3 Gb RAM e instalado o Windows 10 utilizando-se o software VirtualBox e, em seguida, instalado o servidor do C2 em Combate, versão 6.0064986, que funcionou perfeitamente.

2.2 CAPTURA DE TRÁFEGO DE REDE

Com a finalidade de entender como o rádio Harris 7800V-HH transmitia as coordenadas geográficas para o servidor de posições do C2 em Combate, foi utilizado o software Wireshark para realizar a leitura dos pacotes enviados.

Antes de realizar a captura, o rádio 7800V-HH foi renomeado com o nome de VITIMA, para que fosse mais fácil identificação, e assim foram capturados pacotes UDP (User Datagram Protocol) de destino do rádio para a máquina virtual do C2 em Combate.

2.2.1 User Datagram Protocol (UDP)

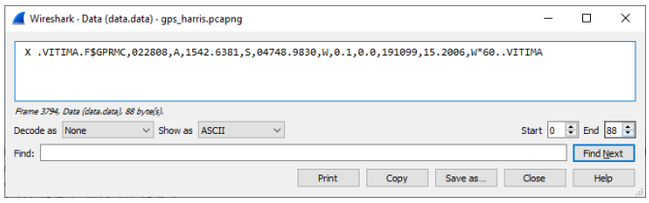
Segundo Neto (2017, p. 29), o UDP é um protocolo que não é orientado à conexão, pois ele não exige uma resposta de confirmação pelo receptor.

Esse protocolo é adequado para a transmissão de dados de GPS pois o contro-

le da transmissão é realizado pela aplicação do C2 em Combate, devido ao fato de que uma conexão TCP exigiria que as instâncias se mantivessem conectadas durante todo o processo, enquanto que a transmissão UDP se assemelha à característica de transmissão half-duplex do rádio, que exigem chaveamento do canal de transmissão e recepção.

2.2.1 Pacote UDP Capturado

FIGURA 1 Pacote Capturado pelo Wireshark.



Fonte: os autores, 2019

TABELA 1 Dados do pacote capturado.

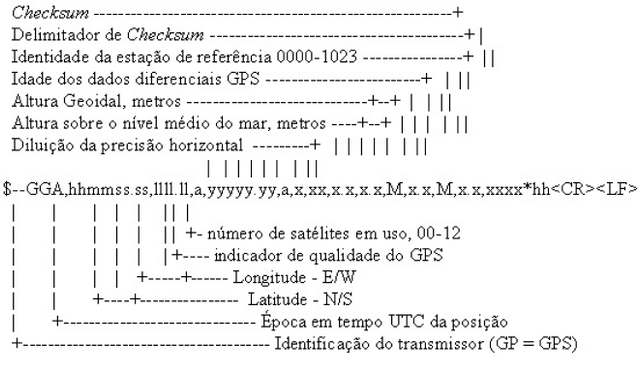
DADOS	INFORMAÇÃO
X.	Início do pacote
VITIMA	Nome do rádio
.F	Não identificado
$GPRMC	Identificador do padrão internacional NMEA (Especificação de dados de GPS mínima)
022808	Hora (No formato: HHMMSS H: Hora M: Minuto S: Segundo)
A	Aviso de navegação: Aviso de navegação: (No formato: A: Ok V: Aviso)
1542.6381	Latitude (No formato: GGMM.SS G: Graus M: Minutos S: Segundos em decimal)
S	Latitude (S: Sul, N: Norte)
04748.9830	Longitude (No formato: 0GGMM.SS G: Graus M: Minutos S: Segundos em decimal)
W	Longitude (W: Oeste, E: Leste)
0.1	Velocidade de deslocamento
0.0	Azimute
191099	Data (No formato: DDMMAA D: Dia M: Mês A: Ano)
15.2006	Declinação Magnética
W	Orientação da Declinação (W: Oeste, E: Leste)
*60..	Checksum (hexadecimal)
VITIMA	Nome do rádio
,	Separador (vírgula)

Fonte: os autores, 2019.

2.2.3 Padrão internacional NMEA

Após pesquisas, foi identificado que as informações do pacote pertencem ao padrão internacional de formato de dados NMEA (National Marine Electronics Association), padrão, esse, desenvolvido visando a conexão de dispositivos eletrônicos marinhos (MundoGEO, 2004).

FIGURA 2 Padrão NMEA 0183



Fonte: MundoGEO <https://mundogeo.com/blog/2004/01/01/gps-21-11/ >, 2019.

O padrão é constituído por até 82 caracteres ASCII, iniciando, sempre, com o símbolo $, termina com o verificador de soma *checksum* e todas as informações são separadas por vírgulas.

Mais especificamente, o padrão utilizado pelo rádio segue o padrão de informações mínimas GPRMC (*Recommended Minimum Specific GPS Data*), que significa, recomendação de informações específicas mínimas de GPS. (BADDELEY, 2001)

FIGURA 3 GPRMC.

$GPRMC

Recommended minimum specific GPS/Transit data

```
eg1. $GPRMC,081836,A,3751.65,S,14507.36,E,000.0,360.0,130998,011.3,E*62
eg2. $GPRMC,225446,A,4916.45,N,12311.12,W,000.5,054.7,191194,020.3,E*68


           225446       Time of fix 22:54:46 UTC
           A            Navigation receiver warning A = OK, V = warning
           4916.45,N    Latitude 49 deg. 16.45 min North
           12311.12,W   Longitude 123 deg. 11.12 min West
           000.5        Speed over ground, Knots
           054.7        Course Made Good, True
           191194       Date of fix  19 November 1994
           020.3,E      Magnetic variation 20.3 deg East
           *68          mandatory checksum


eg3. $GPRMC,220516,A,5133.82,N,00042.24,W,173.8,231.8,130694,004.2,W*70
                 1    2    3    4    5     6    7    8      9     10  11 12


      1   220516     Time Stamp
      2   A          validity - A-ok, V-invalid
      3   5133.82    current Latitude
      4   N          North/South
      5   00042.24   current Longitude
      6   W          East/West
      7   173.8      Speed in knots
      8   231.8      True course
      9   130694     Date Stamp
      10  004.2      Variation
      11  W          East/West
      12  *70        checksum
```

Fonte: Gleen Baddeley. <http://aprs.gids.nl/nmea/#rmc>, 2019.

Com as informações acima tornou-se possível reproduzir os pacotes no mesmo formato com informações obtidas de outro dispositivo, em nosso caso, com informações do GPS de um dispositivo móvel, somente sendo necessário adaptar as informações no formato adequado.

2.3 LINGUAGEM DE PROGRAMAÇÃO EM PYTHON

Python é uma linguagem de programação classificada como de altíssimo nível, de código aberto, disponível para diversos sistemas operacionais (Windows, Linux, Macintosh e Android) (NETO, 2007, p. 33) e interoperável com diversas outras linguagens de programação (Java, PHP, R, C++, etc).

Essa linguagem não exige compilação para ser executada, só necessita de um interpretador que leia o código escrito, porém nada a impede de ser compilada caso necessário.

Para Neto (2007, p. 40), Python "[..] oferece excelentes mecanismos para modularizar o código-fonte.", devido a sua capacidade de importar bibliotecas, ou módulos, que são conjuntos de código pré-escritos que realizam funcionalidade específicas de modo que o programador não tenha que recriar os códigos.

2.3.1 Biblioteca Socket

A biblioteca Socket é um conjunto de funções que permitem a comunicação entre máquinas na rede ou entre processos internos.

Neto (2007, p. 26) explica que sockets são utilizados para implementar aplicações que envolvem comunicações em redes TCP/IP e devem ser criados antes de criar sockets antes de iniciar qualquer tipo de comunicação.

Para reproduzir a comunicação do rádio com o servidor do C2 em combate, utilizamos o SOCK_DGRAM como tipo de socket para comunicação UDP.

Extraímos a parte do código que realiza a conexão e o envio das informações:

FIGURA 4 Conexão Socket UDP.

```
91  sockobj = socket(AF_INET, SOCK_DGRAM)
92  try:
93      resultado = sockobj.connect((self.destino, self.porta))
94      sockobj.send(gps.encode('utf-8'))
95  except:
96      continue
97  sockobj.close()
```

Fonte: Os autores, 2019.

No código acima é aberta um socket UDP (SOCK_DGRAM), em seguida, tentamos conexão com o ip e porta de destino e enviamos a informação de gps codificada em bytes no formato utf-8, após o envio a conexão é finalizada.

2.3.2 Biblioteca Kivy

A biblioteca Kivy é um framework para desenvolvimento multiplataforma escrito majoritariamente com a linguagem Python e, com alguns trechos escritos em Cython (Cython é um subconjunto da linguagem Python e seu objetivo é a conversão de código Python para código C “nativo”, Cython é o nome de uma linguagem e também, o nome do compilador). O framework permite o desenvolvimento de aplicações para os sistemas operacionais Microsoft Windows, Linux, Mac OSX, Android, iOS e Raspberry utilizando um mesmo código Python. O projeto é composto por vários subprojetos, cada um especializado numa determinada tarefa, como por exemplo, a geração de executáveis para determinada plataforma, uma API genérica para o fácil acesso ao hardware em plataformas diferentes, desenvolvimento de games etc.

O projeto Kivy, cujo site é http://kivy.org, é composto por vários subprojetos, dentre estes, a biblioteca Kivy (FILHO, 2018).

2.3.2.1 Plyer

Nessa pesquisa utilizou-se API (Application Programming Interface) Plyer para acesso ao recurso de geolocalização do sistema Android.

Plyer <https://github.com/kivy/plyer> é uma API de plataforma independente usado para acessar recursos comumente encontrados em várias plataformas, principalmente as plataformas móveis. A ideia é fazer com que o seu aplicativo possa invocar funções simplesmente Plyer, seja para apresentar uma notificação ao usuário, enquanto o Plyer cuidará de como conversar com a plataforma corretamente, e isso tudo, independentemente da plataforma ou sistema operacional (EXCRIPT, [2018?]).

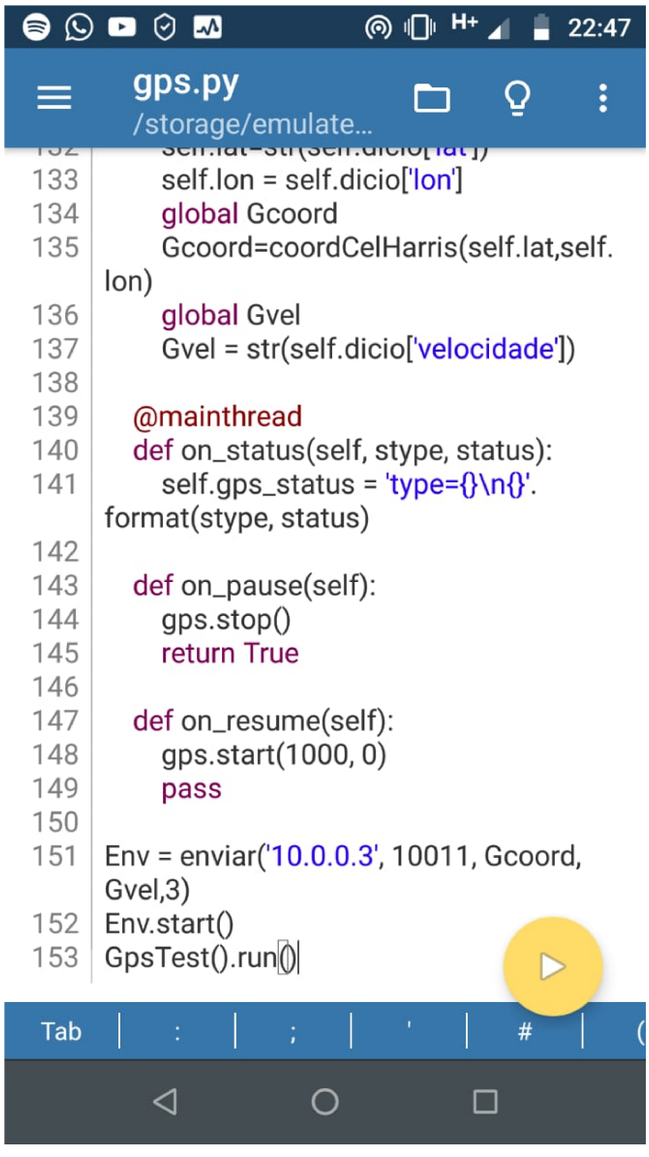
Nessa pesquisa utilizou-se como base, para desenvolvimento do aplicativo de geolocalização, um script da GitHub, desenvolvido na linguagem python com Kivy e Plyer, esse aplicativo, basicamente tem a função de exibir as coordenadas geográficas na tela de um smartphone (GITHUB, 2017).

2.4 GEOPOSICIONAMENTO DO SMARTPHONE

Para executarmos o script de geoposicionamento no Android foi necessário instalar um aplicativo interpretador de Python no smartphone.

Baixamos e instalamos o Pydroid3 e o Pydroid *Permission Plugin* para permitir ao aplicativo o acesso as informações de gps do smartphone, com isso conseguimos executar o script sem problemas.

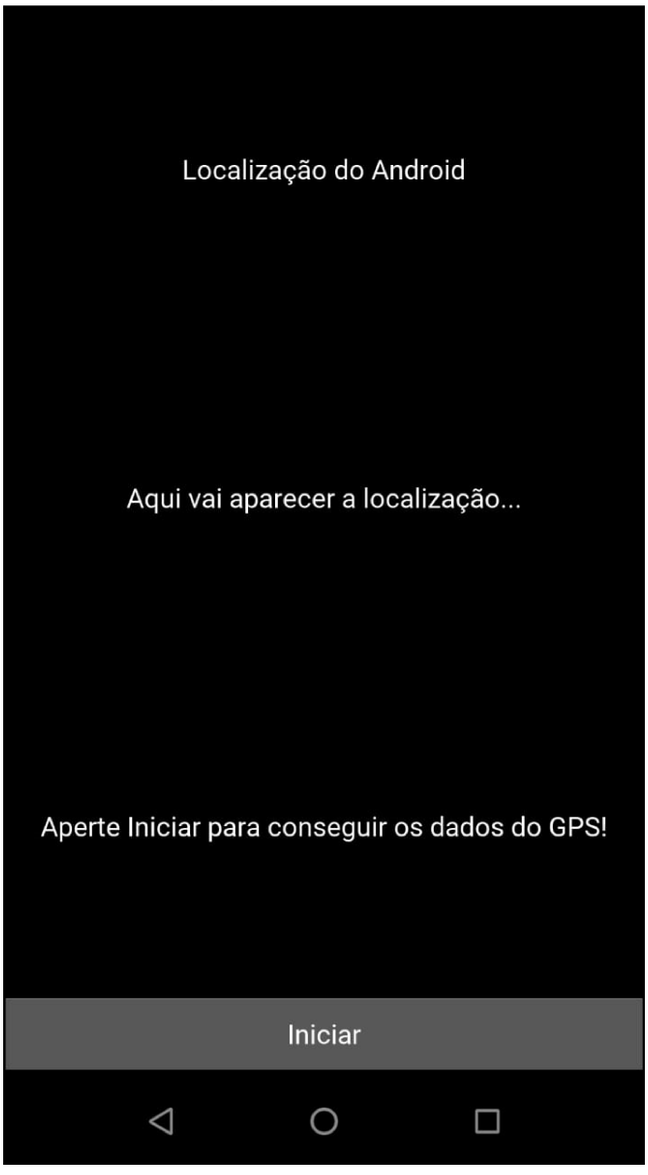
FIGURA 5 Script Python no Pydroid.



Fonte: Os autores, 2019.

Ao executarmos o script é iniciada a instância gráfica a qual é necessário pressionar o botão iniciar para que os dados sejam carregados e enviados.

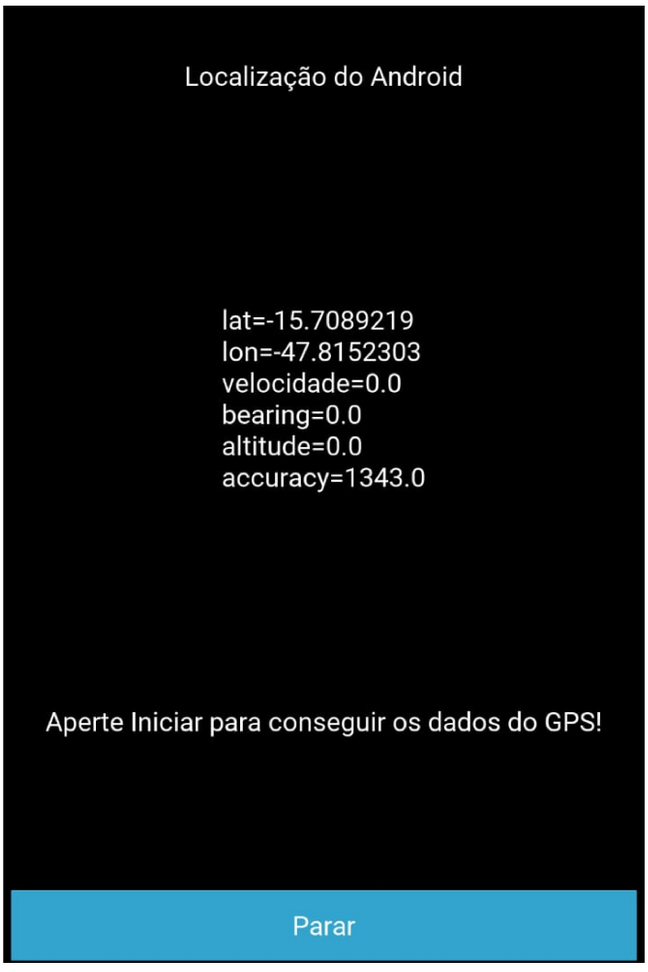
FIGURA 6 Aplicação Kivy iniciada.



Fonte: Os autores, 2019.

Ao pressionarmos o botão iniciar são carregadas as informações de gps do smartphone e inicia-se o envio para o ip do servidor de C2 em Combate configurado. O servidor do C2 em Combate detecta efetivamente as informações como um rádio e projeta a visualização do objeto geoposicionado com a localização exata do dispositivo móvel, confirmando a funcionabilidade do código.

FIGURA 7 Dados de GPS e envio



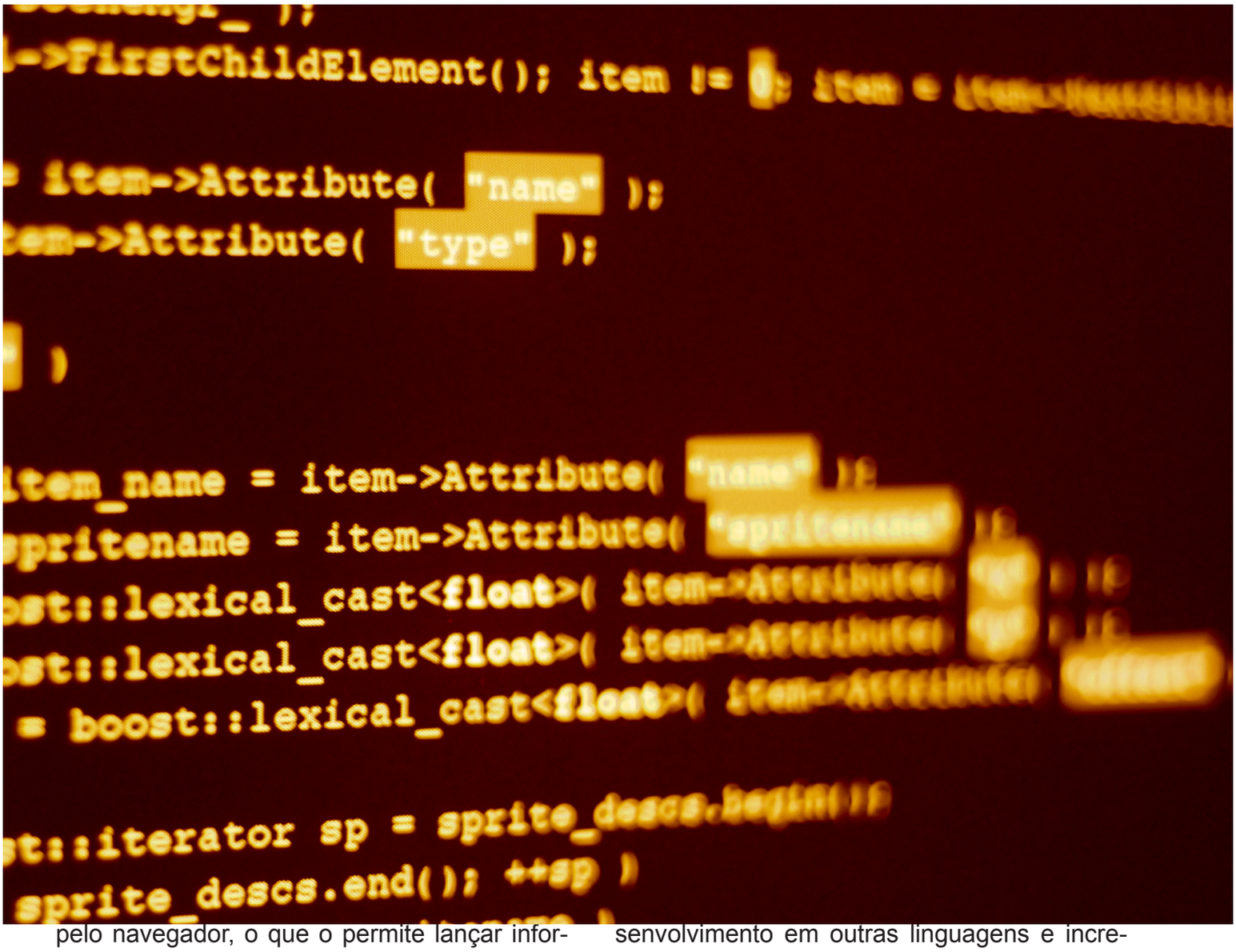
Fonte: Os autores, 2019.

CONCLUSÃO

Diante do exposto verificamos que a execução do código foi capaz de cumprir o objetivo de enviar a localização do smartphone para o servidor de C2 em combate, reproduzindo a funcionalidade do seu semelhante, o Pacificador Móvel.

Essa simples funcionalidade soluciona o problema inicial dessa pesquisa que é a inexistência de um aplicativo que integre dispositivos móveis ao software C2 em Combate e possibilita a economia de equipamentos rádio e flexibiliza o uso em localidades onde o militar sai do alcance da rede, sendo possível operar em áreas com cobertura de telefonia móvel em dados e acesso VPN à rede EBNet.

Com isso o usuário do smartphone, reporta sua localização em tempo real e tem a possibilidade de acessar o C2 em combate



pelo navegador, o que o permite lançar informações dos incidentes ocorridos. Isso pode ser uma melhora no conceito de emprego do C2 em combate, pois dessa forma não é necessário que o militar no terreno faça um relatório para o COp para que os operadores do COp reportem as informações pelo C2 em Combate ao escalão superior, mas a informação é lançada no programa diretamente do militar no terreno, de forma semelhante ao Pacificador móvel. A desvantagem é que o C2 em Combate não possui página responsiva que se adapta ao tamanho da tela, o que dificulta a operação pelo smartphone.

O escopo do trabalho se limitou ao geoposiconamento de dispositivo móvel, mas existem diversas aplicações que podem ser exploradas utilizando-se das informações descritas nesta obra.

Com isso, o trabalho deixa de legado o código fonte para futuras pesquisas que desejem aprimorá-lo, ou mesmo, de base para desenvolvimento em outras linguagens e incremento de novas funcionalidades ao sistema.

SMARTPHONE GEO-POSITIONING IN C2 EM COMBATE 6.0 SOFTWARE: AN INTEGRATOR IN PYTHON PROGRAMMING LANGUAGE

ABSTRACT: This document presents a suggestion of application development that is able to geolocate a smartphone in the program C2 em Combate 6.0, as it is carried out in the Pacificador system. For this purpose, network traffic captures of the Harris 7800V-HH radio while transmitting geographic coordinate information to a emulated server of C2 em Combate, which were extracted and stored. Next, a script was developed in Python programming language that captures the real geographical coordinates of the smartphone and sends it, in the same format transmitted by the radio, to the position server of the C2 em Combate, which detects it as active. This study aimed to demonstrate the possibility of performing the same functionality provided by the Pacificador Móvel applica-

tion, which has not officially existed in the C2 em Combate system. It was therefore concluded that it is possible to replicate the usefulness of the Pacificador Móvel application to other command and control systems by providing an alternative means of equipment in addition to the radio, saving resources and enhancing the situational awareness capabilities of the system .

Keywords: Command and Control, C2 em Combate, Python, Geo-positioning.

REFERÊNCIAS

BADDELEY, Gleen. GPS - NMEA sentence information. 2001. Disponível em: <http://aprs.gids.nl/nmea/#rmc>. Acesso em: 19 jun. 2019.

BRASIL, ESTADO-MAIOR DO EXÉRCITO; Compreensão das Operações (COMOP) nº 01/2019, Apoio de Comunicações à Força Terrestre. Portaria nº 023-EME, de 31 de janeiro de 2019. Brasília, DF, 2019. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=1662&act=bre>. Acesso em: 17 jun. 2019.

EXCRIPT. Kivy: Documentação. [2018?] Disponível em: <http://excript.com/downloads/kivy-pt_br-excript.pdf>. Acesso em: 16 jun. 2019.

FILHO, Cláudio Rogério Carvalho. Biblioteca kivy. Excript, 21 jun. 2018. Disponível em: <http://excript.com/python/kivy.html>. Acesso em: 16 jun. 2019.

GITHUB. 2017. Disponível em:<https://github.com/kivy/plyer/blob/master/examples/gps/main.py>. Acesso em: 16 jun. 2019

MUNDOGEO. GPS 21. 2004. Disponível em: < https://mundogeo.com/blog/2004/01/01/gps-21-11/>. Acesso em: 19 jun. 2019.

NETO, Jahyr Gonçalves. Desenvolvimento de uma Plataforma Multimídia Utilizando a Linguagem Python. 2007. p. 89. Dissertação de mestrado (Engenharia Elétrica). Disponível em: <http://repositorio.unicamp.br/jspui/bitstream/REPOSIP/259651/1/GoncalvesNeto_Jahyr_M.pdf>. Acesso em: 16 jun. 2019.

PYTHON. Disponível em: <https://www.python.org/about/>. Acesso em: 16 jun. 2019.

SEITZ. Justin. Black Hat Python: Programação Python para hackers e pentesters. 1. ed. São Paulo: Novatec Editora, 2015. ISNB 978-85-7522-420-5.

WIRESHARK. Disponível em: <https://www.wireshark.org/index.html#aboutWS>. Acesso em: 16 jun. 2019.

Os autores são bacharéis em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN)e são pós-graduandos em Gestão de Sistema Táticos de Comando e Controle pela Escola de Comunicações.

Atualmente, o 1° Ten Adrian exerce a função de Chefe da 3ª Seção da 8ª Companhia de Comunicações, Bento Gonçalves-RS e pode ser contactado pelo e-mail: adrian.santos@eb.mil.br.

Atualmente, o 1° Ten Tenorio exerce a função de Chefe da Seção de Tecnologia da Informação do 9° Batalhão de Comunicações e Guerra Eletrônica, Campo Grande-MS e pode ser contactado pelo e-mail: tenorio.costa@eb.mil.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

IMPLANTAÇÃO DE *SMART GRID* NO BRASIL: POSSIBILIDADES E LIMITAÇÕES

André Ricardo Silva Vieira dos Santos
Graduado em Engenharia Elétrica-Eletrônica

RESUMO: O setor elétrico brasileiro está em constante mudança e em iminência de grandes transformações tecnológicas em larga escala. Esta transição tecnológica caracteriza-se na modernização das tecnologias aplicadas à energia elétrica na geração, transmissão, distribuição, visando melhorar o aproveitamento dos recursos da própria rede elétrica com a possibilidade de proporcionar ao usuário final maior participação no planejamento e operação do sistema. Essa nova concepção tecnológica é conhecida como Redes Elétricas Inteligentes ou *Smart Grid*. Mesmo a matriz elétrica brasileira sendo renovável, com cerca de 90% da energia gerada oriunda de fontes renováveis e interligada, contemplando geração e transmissão com dimensões gigantescas, observa-se que grande parte dessa energia gerada e transmitida é tecnicamente perdida antes de chegar ao destino final. Com o objetivo de evitar essas perdas técnicas e alcançar de forma satisfatória a eficiência energética, desde 2011 vem sendo estudado a implementação da tecnologia *Smart Grid* no Brasil. Isso tem motivado concessionárias de energia elétrica, empresas públicas e privadas para que essa transformação tecnológica seja uma realidade o mais rápido possível. Essa tecnologia envolve diversos setores tecnológicos, como por exemplo: Internet das Coisas e medidores inteligentes ou *Smart Meters*. A implantação de *Smart Grid* poderá trazer facilidades para controle dos consumidores, identificação e resolução de defeitos remotamente, bem como poderá favorecer a sociedade mediante benefícios tais como: uma educação mais avançada com relação à economia de energia e profissionalização de parcela dos seus integrantes. Sendo assim, este trabalho foi elaborado através de levantamento bibliográfico sobre *Smart Grid* com objetivo de apresentar as principais vantagens, desvantagens, viabilidade e dificuldades para a inserção de redes elétricas inteligentes no cenário nacional.

PALAVRAS-CHAVE: Perdas técnicas, redes elétricas inteligentes, eficiência energética, medidores inteligentes.

INTRODUÇÃO

O setor elétrico brasileiro está em constante mudança e em iminência de grandes transformações tecnológicas em larga escala. Esta transição tecnológica caracteriza-se na modernização das tecnologias aplicadas na energia elétrica na geração, transmissão, distribuição, visando melhorar o aproveitamento dos recursos da própria rede elétrica com a possibilidade de proporcionar ao usuário final maior participação no planejamento e operação do sistema. Essa nova concepção tecnológica é conhecida como *Smart Grid* (FALCÃO, 2009).

Tendo em vista os novos desafios e as necessidades por qualidade, segurança, flexibilidade e sustentabilidade, as Smart Grid constituem-se em uma revolução tecnológica na indústria de energia elétrica. As tecnologias envolvidas nas áreas de eletrônica, de telecomunicação e de tecnologia da informação são aplicadas para a automação e a melhoria dos serviços de energia elétrica.

Essa revolução no setor elétrico brasileiro, em especial no segmento de distribuição, permite uma série de possibilidades: participação mais ativa dos consumidores, disponibilização de mais informações, prestação de novos serviços, aperfeiçoamento da gestão de ativos, eficiência energética, melhoria da qualidade da energia e o combate de alguns problemas vivenciados no Brasil como as perdas não técnicas.

Os benefícios das Smart Grid espalham-se por toda a sociedade e abrangem tanto as empresas distribuidoras quanto os consumidores, além de possibilitar ganhos fora do setor elétrico. No Brasil, a implantação é objeto de análise tanto pelas distribuidoras quanto pela Agência Nacional de Energia Elétrica (ANEEL), que regula as Diretrizes do Sistema Elétrico Brasileiro (LAMIN, 2013).

2 METODOLOGIA

Com o objetivo de apresentar as principais vantagens, desvantagens, viabilidade e dificuldades para a implantação de Redes Elétricas Inteligentes, este estudo foi elaborado através de levantamento bibliográfico acerca do referido assunto.

Os critérios de inclusão foram os estudos baseados no Plano Nacional de Energia Elétrica (PNE), além de artigos, periódicos de congressos e capítulos de livros, publicados entre 1992 e 2017, que versem sobre *Smart Grid* ou Redes Elétricas Inteligentes. Estudos publicados anteriormente ao ano de 1992 foram utilizados como critério de exclusão.

3 RESULTADOS E DISCUSSÕES

3.1 CONCEITO DE *SMART GRID*

O conceito *Smart Grid* possui sentido amplo e deve ser compreendido como uma inovação tecnológica do que simplesmente um medidor ou equipamento específico. Baseia-se na utilização intensiva de tecnologia de automação, computação e comunicações para monitoração e controle da rede elétrica, as quais permitirão a implantação de estratégias de controle e melhoria da rede de forma muito mais eficiente que as atualmente em uso (FALCÃO, 2009).

O que caracteriza uma rede elétrica como “inteligente” é a capacidade de integrar as ações de todos agentes a ela conectados, sejam geradores de energia, consumidores ou os chamados “*prosumers*” (do inglês “*productor and consumer*”) (BONALDO et al., 2013).

As redes elétricas inteligentes (REI) proporcionam de forma eficaz a produção, distribuição e consumo de energia, facilitando a concorrência e inclusão de equipamentos ou consumidores nas redes, com melhorias relevantes em monitoramento, administração de forma geral, automação e qualidade da energia disponibilizada, por meio de uma rede elétrica caracterizada pelo uso intensivo das tecnologias de informação e comunicação (TIC).

O conceito de *Smart Grid* (SG), ou simplesmente redes elétricas inteligentes (REI), que foi embasado em Amin e Wollenberg (2005), apresenta um novo modelo do setor elétrico brasileiro, considerando a necessidade de tornar o sistema de fornecimento de energia mais dinâmico e interativo, por razões específicas em cada país ou região.

O principal motivo que justifica esse sistema baseado em um modelo interativo, dinâmico e inteligente ser adotado em qualquer lugar do mundo é a necessidade de que o consumidor final possa escolher um tipo de energia, alternativa e sustentável, que esteja ao seu alcance e que possua característica descentralizada e intermitente, além de possibilitar que o próprio cliente consiga obter informações e possa inserir novos equipamentos e eletrodomésticos inteligentes que se comuniquem com esse sistema. Dessa forma, haveria comunicação e cooperação entre si, de modo que ocorreria uma autoconfiguração ou autocorreção caso fosse adicionado um novo elemento ou componente (plug and play) na rede. (AMIN E WOLLENBERG, 2005).

A implantação das *Smart Grid* pode ser compreendida em três dimensões complementares e independentes (BANDEIRA, 2012):

a) A consolidação da inteligência ao sistema de geração, transmissão e distribuição, será realizada nas primeiras intervenções, consequentemente trazendo robustez, segurança e velocidade na rede;

b) Substituição dos medidores eletromecânicos por medidores eletrônicos inteligentes com várias funções embutidas trazendo facilidades para o consumidor como transparência e uma educação para que uso da energia elétrica fique mais racional;

c) inteligência nos consumidores, caracterizada por residências com eletrodomésticos inteligentes submetidos aos medidores, melhor administração do consumo energético, comunicação bidirecional de energia, por meio da geração distribuída com fonte de geradora solar, eólica ou biomassa.

A extensão do mercado e os ganhos previstos com a implantação das REI podem

ser alcançados para outros serviços públicos, desenvolvendo o conceito de cidades inteligentes (*Smart Cities*), onde a infraestrutura de informação e automação existente permitirá o uso ideal dos recursos, como concessionárias de energia, água, gás, segurança, trânsito etc. e por consequência a melhoria na qualidade desses outros serviços oferecidos a população.

A possibilidade de implantação das *Smart Grid e Smart Cities*, está extremamente ligada aos avanços tecnológicos da eletrônica, e armazenamento de dados, como também do desenvolvimento nos sistemas de controle. Esse fenômeno possibilitará não somente a implantação de cidades inteligentes, mas também de ambientes onde todos os objetos podem ser unicamente reconhecidos e identificados, localizados e endereçados, o que vem sendo chamado de Internet of Things (IoT), ou Internet das Coisas, de sensoriamento. (BANDEIRA, 2012).

3.2 VISÃO DA IMPLANTAÇÃO DO CONCEITO DE *SMART GRID* NO BRASIL

A matriz energética brasileira é renovável, com cerca de 90% da energia gerada de fontes renováveis, e interligada por meio de um complexo sistema que está conectado a todo país tanto as subestações geradoras como as subestações de transmissão.

O consumo de energia per capita no país é significativamente inferior a 2.200 kWh/habitante, contra, por exemplo, 12.884 kWh/habitante nos Estados Unidos, segundo International Energy Agency (IEA).

O potencial de recursos renováveis e não renováveis não explorados é alto e as tarifas de energia estão entre as mais altas do mundo. Consequentemente, no Brasil, a formulação de política energética concentra esforços nos objetivos associados à garantia de suprimento com moderação nas tarifas, sobrepondo-se os objetivos de política industrial e tecnológica (ANEEL, 2010).

A abundância no Brasil de recursos renováveis competitivos (como a geração hidrelétrica e eólica) impede o estímulo a tecnologias inovadoras, relacionadas à geração distribuída e ao desenvolvimento das REI, como ocorre no Hemisfério Norte para o caso de energia solar.

A implantação das REI no Brasil teria como principais motivadores: a busca das eficiências comercial e energética, o aumento da confiabilidade do sistema elétrico em geral, a segurança operacional e sistêmica e sustentabilidade econômica e ambiental (ANEEL, 2010).

Eficiência comercial e energética seriam obtidas por meio da redução de perdas técnicas e comerciais, melhoria na qualidade da energia disponibilizada ao consumidor e gestão do horário de consumo de energia pelo consumidor.

A confiabilidade do sistema elétrico aumentaria com a interoperabilidade entre os diversos componentes da rede e as subestações, gestão de ativos e do planejamento da capacidade de geração, transmissão e distribuição de energia.

A segurança operacional e sistêmica seria atingida por meio do controle de acesso dos usuários de rede, da redução de energia não distribuída e das perdas por fraudes, bem como viabilizaria a geração distribuída e a gestão para contingências e autorrecomposição.

Além dos motivadores expostos, de acordo com o Plano Nacional de Energia (PNE) 2030, está previsto a redução do consumo final de energia elétrica em pelo menos 10% em 2030 por meio de medidas sólidas de eficiência energética (MME, 2010).

O nível de perdas não técnicas e técnicas são elevados, sobretudo em áreas urbanas. Segundo Bloomberg (2012), cerca de US$ 5 bilhões são perdidos anualmente em furtos, erros de faturamento e medição, e 16% da energia produzida não é vendida por razões técnicas e não técnicas.

A atenuação de perdas tem sido fator orientador de investimentos para concessionárias. Algumas concessionárias têm desenvolvido experiências de REI em regiões que representam até 1% de suas bases instaladas. Haveria, ainda, a possibilidade de fluxo bidirecional de energia para o uso mais intensivo da microgeração distribuída.

O Regime Especial de Tributação do Programa Nacional de Banda Larga para a implantação de redes de telecomunicações (REPNBL-Redes) é considerado um estímulo para antecipação de investimentos em REI no Brasil. Nesse sentido, basta as empresas interessadas submeterem os projetos de implantação incluindo os medidores de energia eletroeletrônicos inteligentes, com capacidade de telecomunicação e de fornecimento de comunicação de dados em banda larga. (BLOOMBERG, 2012).

3.3 POPULARIZAÇÃO DAS *SMART GRID*

A sincronização com as políticas energética e regulatória conduzidas pelo Ministério de Minas e Energia e ANEEL é de fundamental importância. Essa sincronização estipulará o ritmo de substituição de medidores e como será feito o abatimento destes, a intensidade do uso da geração distribuída que são abastecidos pela rede, além da possibilidade de conduzir o comportamento do consumidor para inclusão e acesso às novas tecnologias.

Essas políticas, em conjunto com instrumentos do uso do Poder de Compra do Estado, além do entendimento aprofundado da resposta dos consumidores finais à implantação das REI, são decisivas para determinar o ritmo o crescimento da demanda e, em última instância, dos investimentos e difusão das tecnologias e produtos desenvolvidos (ANEEL, 2010).

A partir do aumento do controle e da inserção da eletrônica, um resultado de destaque é o avanço na medição e no faturamento, propiciando a redução de perdas não técnicas, como fraudes dos próprios consumidores ou de terceiros. Outra possibilidade é aprimorar o uso da energia elétrica (eficiência energética).

No Brasil, os três principais motivadores para a popularização das *Smart Grid* são: atenuação e eliminação de perdas não técnicas ocasionadas por fraudes; constância da continuidade; e eficiência energética. No contexto global, podem ser encontrados outros motivadores, dentre eles: o aumento da competitividade e ampliação do mercado livre; diminuição de custos operativos; diminuição do impacto ambiental; prestação de novos serviços; e gerenciamento de ativos. (LAMIN, 2013).

Para Falcão (2009), algumas das características geralmente atribuídas à *Smart Grid* que favorecem sua popularização são:

a) Autorestabelecimento;

b) Autodiagnóstico, autorecuperação de falhas na rede;

c) Autonomia dos Consumidores: inclusão de equipamentos e comportamento dos consumidores nos processos de planejamento e operação da rede;

d) Transigência a Ataques Externos: capacidade de mitigar e resistir a ataques físicos e cyber-ataques;

e) Qualidade de Energia;

f) Capacidade de acomodação de uma grande variedade de fontes e demandas.

f) Flexibilidade para acesso a uma variedade de fontes de energia de várias dimensões e tecnologia;

g) Garantia da sustentabilidade, reduzindo perdas técnica e utilizando fontes sustentáveis;

h) Resposta instantânea da demanda conforme a atuação remota em dispositivos instalados nos consumidores; e

i) Estimulo à concorrência de produtos e serviços no mercado de energia.

Dentre as várias tecnologias que propiciam a inserção de uma *Smart Grid*, pode-se citar:

a) Geração Distribuída e Microgeração. Aplicada mediante necessidade dos consumidores e com o objetivo de atender a sustenta-

bilidade. Energia solar e eólica são exemplos de aplicação de geração distribuída;

b) Infra-Estrutura Automática de Medição (AMI). Consiste em sistemas autônomos de coleta de dados através de medidores inteligentes, permitindo análises e respostas imediatas a respeito de demandas, sem intervenção humana e sim através da atuação em dispositivos nas instalações dos consumidores. Utilizam-se os chamados *Smart Meters*, os quais são medidores eletrônicos com funcionalidade ampliada e capacidade de comunicação bidirecionais.

c) Equipamentos Prediais e Eletrodomésticos Inteligentes. São equipamentos elétricos para uso em residências e estabelecimentos comerciais que estão sendo equipados com recursos de controle capazes de alterar sua demanda em função de sinais de preço ou relacionados com a confiabilidade do sistema elétrico.

O Sistema Elétrico de Energia (SEE) é divido em três segmentos físicos: geração, transmissão e distribuição. É um segmento virtualizado, mas com grande relevância econômica, a comercialização de energia. As tecnologias que compõem a *Smart Grid* permeiam todos os segmentos do setor elétrico embora esteja evoluindo com diferentes velocidades em cada um deles. (FALCÃO, 2009).

De acordo com Falcão (2009), para os consumidores finais, com a introdução do conceito de *Smart Grid*, particularmente devido à introdução dos *Smart Meters* e da microgeração (geração de pequeno porte instalada em residências e pequenos edifícios), as tarefas antes passivas agora sendo ativas e podendo ser de forma instantânea e dinâmica, as principais modificações virão de:

a) Equipamentos Prediais e Eletrodomésticos Inteligentes: permitirão o controle da demanda dos consumidores mediante o envio de sinais através dos sistemas de comunicações bidirecional;

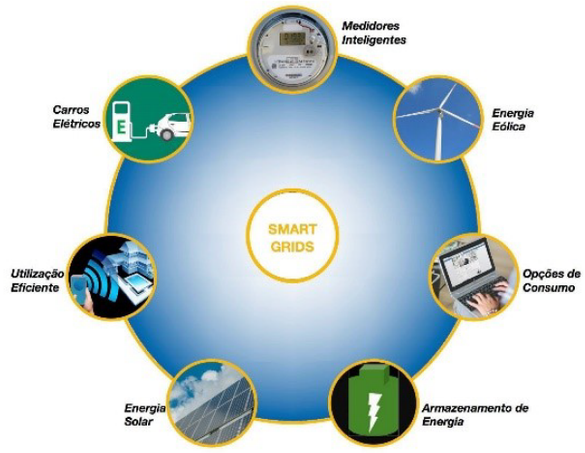
b) Microgeração: disponibilização de geração de pequeno porte e médio porte, através do uso de painéis solares, microgeradores eólicos, células a combustível etc., capazes de produzir energia para subsistência e compensação para a concessionária; e

c) Sistemas Prediais de Gerenciamento de Energia: sistemas para monitoramento e potencialização da demanda de residências e edifícios de forma isolada ou através da Internet.

3.4 DESAFIOS TECNOLÓGICOS

Um dos maiores desafios, para implementação de REI, consiste no envolvimento de várias disciplinas devido ao fato do sistema ter alto teor de complexidade, além de depender do contexto no qual a rede elétrica inteligente será implantada, ou seja, em redes de transmissão, distribuição ou microrredes. (BONALDO et al., 2013).

FIGURA 1 Integração com outros serviços.



Fonte: EESC-USP, 2019.

No caso de microrredes residenciais inteligentes, que representam a evolução da rede de distribuição de baixa tensão, pode-se colocar uma infinidade de recursos energéticos distribuídos (solar, eólica, baterias, células a combustível, microturbinas). Neste contexto, cada fonte de energia está ligada à rede de distribuição por um conversor de eletrônico de potência (CEP). O funcionamento da microrrede pode ser melhorado através de um controle sinérgico de tais processadores de energia.

Dessa forma, é necessário desenvolver uma arquitetura de Tecnologia da Informaçao e Comunicações (TIC) para o controle dos CEP distribuídos. Em uma abordagem *Plug & Play* de controle, cada CEP tem que identificar

a rede ao redor e se comunicar com os consumidores vizinhos para estabelecer uma regra de controle distribuído e próximo do ideal. Com esse procedimento, torna-se possível explorar amplamente todas as fontes de energia existentes, reduzir a perda local de distribuição e estabilizar as tensões da rede. (BONALDO et al., 2013).

3.5 SISTEMAS DE MEDIÇÃO E SENSORIAMENTO DE GRANDEZAS ELÉTRICAS

Os chamados Medidores Inteligentes ou "*Smart Meters"* são equipamentos que podem atuar na operação e no planejamento do sistema de medição. São medidores de energia elétrica que utilizam comunicação bidirecional para atuação remota, para coleta de dados e para fornecimento de informações aos consumidores e distribuidoras são chamados de inteligentes (LAMIN, 2013).

FIGURA 2 Medidor inteligente.

Fonte: NXP Semiconductors Brasil, 2019.

Tais equipamentos possuem muitas aplicações em *Smart Grids*, tais como: tarifação dinâmica; resposta à demanda; conexão e desconexão remotas; gerenciamento de interrupções; e segurança de rede e redução de perdas não técnicas, dentre outras.

Um medidor inteligente deve conter no mínimo as funcionalidades a seguir:

a) Medição de energia ativa e reativa;

b) Capacidade de aplicação de tarifas horárias;

c) Demanda programável;

d) Possibilidade de faturamento em pré-pagamento ou pós-pagamento eletrônico;

e) Inversão de fluxo (geração distribuída);

f) Registro de eventos e apuração de indicadores de continuidade e conformidade;

g) Medição de neutro, sensor de abertura da tampa e alertas antifraude;

h) Corte e religamento remoto;

i) Mostrador LCD parametrizável e display com seis dígitos;

j) Saídas ou entradas de pulsos (ou saída serial) e porta ótica de comunicação local; e

k) Comunicação remota bidirecional.

No quesito comunicação, os medidores inteligentes possuem comunicação bidirecional, podendo receber e enviar dados. Várias tecnologias podem ser usadas para tal, como ZigBee, PLC, rede Mesh, GRPS, etc.

Seguindo uma tendência mundial, não existe no Brasil a previsão de fabricação de medidores eletromecânicos para o futuro. Atualmente, os preços de modelos básicos de medidores eletrônicos são inferiores aos preços dos eletromecânicos, devido ao avanço na eletrônica e à queda de preços de fabricação, além do aumento nos preços de componentes dos medidores eletromecânicos (ferro, alumínio e cobre). Sendo assim, é previsível que não existirão mais plantas fabris de medidores eletromecânicos no país (LAMIN, 2013).

3.5.1 Descarte dos Medidores Eletromecânicos

Segundo a ANEEL, fabricantes e distribuidoras manifestaram soluções simples e viáveis para a questão do descarte de equipamentos, de modo que essa "não seria uma etapa crítica" (Aneel, 2010).

Os fabricantes manifestaram interesse em montar uma logística reversa, com uma empresa especializada em receber os ativos e dar destinação final. A Associação Brasileira da Indústria Elétrica e Eletrônica (ABINEE) pontuou que os descartes são fáceis, já que todas as partes dos medidores eletromecânicos são recicláveis. Segundo a Associação, para o descarte dos medidores eletromecânicos "já

existe uma empresa de logística reversa (recolhimento e destinação final) contatada". Ressaltou ainda que "essa mesma empresa facilmente interessar-se-á pelo recolhimento dos medidores eletrônicos".

Complementarmente, existe a possibilidade de revenda dos equipamentos para países que permanecem utilizando a medição eletromecânica, ou ainda, a opção de que medidores descartados sejam sucateados e suas partes vendidas a uma empresa de reciclagem (ANEEL, 2010). Ou seja, o descarte de medidores eletromecânicos poderia ser considerado até mesmo um benefício, uma vez que poderia ser obtido algum valor monetário com a venda do equipamento retirado de campo. Apesar de terem considerado valor nulo, as análises conduzidas em Portugal (ERSE, 2012) e na Holanda (SENTER NOVEM, 2005) mencionam que pode existir algum valor residual dos medidores convencionais substituídos antes do final da sua vida útil.

3.5.2 Multi-Utility

Por meio da funcionalidade conhecida como AMM+MU (Automated Meter Management + Multi-utility), o medidor eletrônico de energia elétrica permite a interação com outros medidores de serviços públicos, como água e gás. Assim, o medidor está apto a receber dados de outros serviços e comunicá-los remotamente por meio do sistema de telecomunicações e da infraestrutura das empresas de distribuição de energia elétrica (LAMIN, 2013).

3.5.3 Sistemas de Comunicação

Existem basicamente 4 camadas na área de comunicação para Smart Grids: HAN – Home Area Network; LAN – Local Area Network; RAN – Regional Area Network; e WAN – Wide Area Network.

Atualmente a tecnologia ZigBee é mais atrativa para interconectar dispositivos em uma rede privada. Protocolos ZigBee são destinados a aplicações embarcadas que exigem baixas taxas de dados e baixo consumo de energia. Tal tecnologia permite criar uma rede de sensores sem fio, como em uma rede de sensores doméstica (BONALDO et al., 2013). Tal conceito é ilustrado na figura 3.

FIGURA 3 Interconectividade da Smart Grid.

Fonte: SEBRAE, 2019.

Uma possível solução para a transmissão de dados é a tecnologia Power Line Communications (PLC), que é um canal de comunicação natural para redes elétricas. Nesse caso, a topologia de comunicação que corresponde exatamente à topologia da rede, não requer implantação de novos cabos.

Apesar de vários esforços de padronização para apoiar as redes inteligentes, ainda não foi encontrada uma solução definitiva, com as taxas de transmissão de dados necessária às estratégias de controle (BONALDO et al., 2013).

CONCLUSÃO

Diante do exposto, pode-se afirmar que o que caracteriza uma rede elétrica como "inteligente" é a capacidade de integrar as ações de todos agentes a ela conectados, sejam geradores de energia ou consumidores e atuarem de forma autônoma ou ainda remotamente.

Sendo assim, duas características inerentes ao setor elétrico brasileiro podem favorecer e acelerar a implantação das *Smart Grid* no Brasil. A primeira característica refere-se ao crescente aumento da demanda, que causa um risco maior de falta de energia (apagões). A segunda característica diz respeito à necessidade de criação de mecanismos que impossibilitem

o roubo de energia, conhecido popularmente como “gato”. Entretanto, a sua implantação demanda altos investimentos e, no caso do Brasil, ainda falta regulamentação da ANEEL. Ainda assim, as empresas brasileiras apostam na tecnologia, pois é uma tendência mundial.

Tendo em vista as grandes transformações no setor elétrico e o consequente surgimento de inovações que buscam evitar perdas energéticas na distribuição de energia elétrica entre o consumidor final e a concessionária, foram apresentadas, nesse trabalho, as vantagens, desvantagens, viabilidades e dificuldades, para a implantação desse sistema inteligente.

Mediante tal implantação, a extensão do mercado e os incentivos previstos com a implantação das REI podem ser estendidos para outros serviços públicos e privados, caracterizando o conceito de cidades inteligentes (*Smart Cities*). Os medidores inteligentes também podem ser integrados a outros serviços públicos e privados de medição, como por exemplo serviços de gás, água, eletrodomésticos, trânsito entre muitas outras funcionalidades.

No Brasil, a redução de perdas não técnicas, a melhoria da continuidade e da eficiência energética, levam empresas e concessionárias de energia elétrica a realizarem estudos com o objetivo de melhorar a qualidade da prestação de serviço utilizando o conceito de *Smart Grid*. Nesse sentido é possível citar a Companhia Energética de Minas Gerais-CEMIG, que está com projeto piloto na cidade de Sete Lagoas - MG, que fica a 70km de Belo Horizonte - MG, cidade escolhida por ter uma diversidade econômica. A concessionária de energia AES Eletropaulo tem investido nas tecnologias que usam *Smart Grid,* tanto que foi a primeira a ter *Smart Meter* ou medidores inteligentes homologados pelo INMETRO, nas cidades que participam do projeto: Vinhedo – SP, Santos – SP, e Barueri – SP. Além de participarem desse projeto de implantação do Conceito de *Smart Grid*, também caminham para o conceito de Smart City as seguintes cidades: Tubarão – SC, Lajeado – RS, Laguna – CE e Aparecida de Goiânia – GO, que possuem grandes projetos de *Smart City* que, consequentemente, utilizarão *Smart Grid*.

Cabe a observação de que os conceitos apresentados nesse trabalho, causam grandes transformações de conduta à sociedade na qual se insere: melhora-se a educação, mediante a capacitação de novos profissionais especializados; gera-se rendas diretas e indiretas; e há diminuição de perdas técnicas e aumento da eficiência energética. Tudo colaborando para um impacto nacional positivo.

Um fato importante a ser enfatizado quanto à implantação da *Smart Grid* é a necessidade de controle do descarte correto dos medidores eletromecânicos e destinação final dos mesmos, uma vez que, quando começarem a serem substituídos, será gerada uma grande quantidade de lixo. Tal necessidade está alinhada com o pensamento de que toda inovação tecnológica deve ser acompanhada de sustentabilidade, ou seja, de atitudes que mantenham o meio ambiente saudável.

Como sugestão para futuros trabalhos, buscando-se a continuidade desse estudo sugere-se que sejam apresentadas formas eficientes de proteção da rede lógica da *Smart Grid*, uma vez que a tecnologia pode usar sinais de radiofrequência e também a internet das coisas (IOT), visando que nem as concessionárias, nem os consumidores, sejam vítimas de ataques cibernéticos.

SMART GRID DEPLOYMENT IN BRAZIL: POSSIBILITIES AND LIMITATIONS

ABSTRACT: The Brazilian electrical sector is constantly changing and imminent technological transformations on a large scale. This technological transition is characterized by the modernization of the technologies applied to the generation, transmission and distribution of electric energy, aiming at improving the use of the resources of the electric grid itself, with the possibility of providing the final user with greater participation in the planning and operation of the system. This new technological

design is known as Smart Grid or Smart Grid. Even Brazil's renewable energy matrix, with around 90% of the energy generated from renewable and interconnected sources, contemplating generation and transmission with gigantic dimensions, it is observed that much of this energy generated and transmitted is technically lost before reach the destination. With the objective of avoiding these technical losses and achieving a satisfactory energy efficiency, since 2011 the implementation of Smart Grid technology in Brazil has been studied. This motivated electric utilities, public and private companies, to make this technological transformation a reality as fast as possible. This technology involves several technology sectors, such as the Internet of Things and Smart Meters or Smart Meters. The implementation of the Smart Grid can provide facilities for consumer control, identification and resolution of defects remotely, as well as favoring society through benefits such as: more advanced training in energy saving and professionalization on the part of its members. Thus, this work was elaborated through a bibliographic survey about Smart Grid with the objective of presenting the main advantages, disadvantages, feasibility and difficulties for the insertion of intelligent electric grids in the national scenario.

KEY WORDS: Technical losses, smarts grids, energy efficiency, smart meters.

REFERÊNCIAS

AMIN, S. M.; Wollenberg, B. F. Toward a smart grid. IEEE Power and Energy Magazine, v. 3, n. 5, p. 34-38, sep.-oct. 2005.

ANEEL – Agência Nacional de Energia Elétrica. Manual do Programa de Pesquisa e Desenvolvimento Tecnológico do Setor de Energia Elétrica. 2012. Disponível em: <http://www.aneel.gov.br/arquivos/PDF/Manual-PeD_REN-504-2012.pdf>. Acesso em: maio. 2018.

BANDEIRA, F. P. M. Redes de energia elétrica inteligentes (smart grids). Nota técnica. Consultoria Legislativa, 2012. Disponível em: <http://www.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/tema16/2012_7872.pdf>. Acesso em: maio. 2018.

BLOOMBERG. Energy Smart Technologies – Digital Energy – Research Note. New Energy Finance. 2012.

BONALDO J. P., F. N. Braga, J. A. Pomilio, "Single-phase Multifunctional Grid Interface Converter without Grid Sincronization", IEEE 4th International Conference on Clean Electrical Power Renewable Energy Resources Impact, Alghero, Italy, 11-13 June 2013, pp. 330-336.

BRASIL – Ministério de Minas e Energia. Plano Nacional de Eficiência Energética. Premissas e diretrizes básicas na elaboração do plano. 2010. Disponível em: <http://www.mme.gov.br/mme/galerias/arquivos/noticias/2010/PNEf__Premissas_e_Dir._Basicas.pdf>. Acesso em: maio. 2018.

CENTRO SEBRAE DE SUSTENTABILIDADE. Disponível em: <http://sustentabilidade.sebrae.com.br/Sustentabilidade/Para%20sua%20empresa/Estudos%20e%20Pesquisas/Imagens/NIS%20-%20smart%20grid.png>. Acessado em: 28/06/2019.

ERSE (2012). Contadores Inteligentes de Eletricidade e de Gás Natural. Documento de Consulta Pública. Lisboa, Portugal.

FALCÃO, M Djalma, Smart Grids e Microredes: O Futuro já é Presente. VIII Simpase, Simpósio de Automação de Sistemas Elétricos, Programa de Engenharia Elétrica, COPPE, UFRJ, 2013.

LAMIN, HUGO. (2013). Análise de Impacto Regulatório da implantação de redes inteligentes no Brasil. Tese de Doutorado em Engenharia Elétrica, Publicação PPGENE.TD-076/13, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 300p.

NXP Semiconductors Brasil. Disponível em: <https://blog.nxp.com/internet-of-things-2/is-2017-the-year-of-the-smart-meter>. Acessado em: 28/06/2019.

RICHTER GRUPPE EMPREENDIMENTOS E PARTICIPAÇÕES. Disponível em: <http://richtergruppe.com.br/cidades-brasileiras-investindo-em-smart-cities-veja-quais-sao/>. Acessado em: 26/06/2019

RIVERA, Ricardo; Esposito, Alexandre Siciliano; TEIXEIRA, Ingrid. Redes elétricas inteligentes (smart grid): oportunidade para adensamento produtivo e tecnológico local. Revista do BNDES, Rio de Janeiro, n. 40, p. 43-83, dez. 2013

SENTERNOVEM (2005). Implementing smart metering infrastructure at small-scale customers. Recommendation. FAS nº 1-2893 (SenterNovem: 4150). Utrecht, Holanda.

O autor é Graduado em Engenharia Elétrica/ Eletrônica pela Universidade Paulista-UNIP. Pós graduando em Sistema de Energia pela Universidade Paulista-UNIP e pode ser contatado pelo e-mail: andrericardo.santos@eb.mil.br.

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIÊNCIA E TECNOLOGIA

INFLUÊNCIA DA ALTURA ACIMA DO SOLO NOS LÓBULOS DE IRRADIAÇÃO E IMPEDÂNCIA EM UMA ANTENA PARA NVIS

Antonio Anderson Silva Marques

Pós-Graduado em Gestão de Sistemas Táticos de Comando e Controle
Mestrando em Engenharia Elétrica

RESUMO: Antenas próximas ao solo podem ser muito influenciadas por reflexão ou absorção da radiação, especialmente para NVIS (*Near Vertical Incident Skywave*) e quando a altura da antena é menor que 1 comprimento de onda. Para este tipo de antena, o solo será parte componente do sistema, influenciado nos lóbulos de radiação e em sua impedância. Em especial para o território brasileiro, a condutividade do solo em regiões de selva é muito baixa, o que aumenta a necessidade deste tipo de propagação, em detrimento de ondas de superfície ou ondas diretas. Os resultados apontaram que a altura ideal é 0,2λ (5 metros), que apresentou-se como a altura ótima para o diagrama de radiação. A partir deste valor, devido à reflexão no solo, os lóbulos irão se achatar cada vez mais ou formar lóbulos laterais, o que seria não desejável para este tipo de propagação. Abaixo deste valor, há um descasamento muito acentuado de impedância com a linha de transmissão, aumentando a reatância e a perda de radiação para o solo.

Palavras-chave: Antenas HF. Enlaces. NVIS. Ondas Ionosféricas.

INTRODUÇÃO

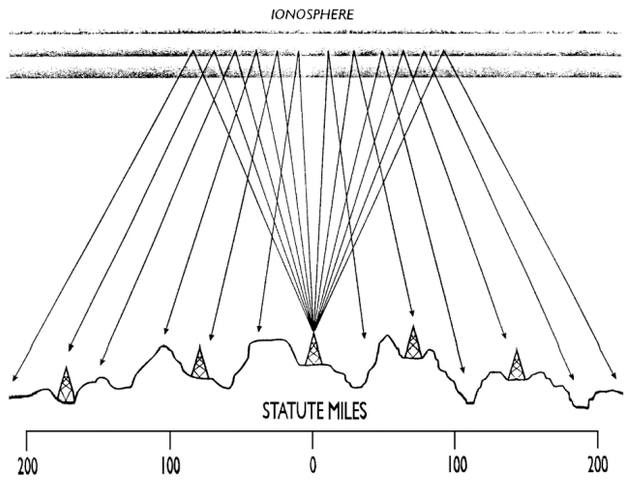
NVIS (*Near Vertical Incident Skywave*) é uma técnica de transmissão em HF (*High Frequency*) que permite alcançar estações receptoras situadas em locais onde a visada direta não é mais possível, devido ao limitado alcance das ondas de superfície.

Em especial para o território brasileiro, a condutividade do solo em regiões de selva é muito baixa. Assis, Filho (2010) em testes de transmissões HF na Amazônia observaram que a condutibilidade do solo (σ_f) é da ordem de 0,2 mSiemens/m e a permissividade (ϵ_f) 1,2, o que representa o menor decil na classificação mundial de condutibilidades de acordo com estudo realizado em escala global (*International Telecommunication Union* - ITU, 1992).

Wallace (1992) cita diversos exemplos bem sucedidos para o uso de NVIS em campo aberto. Sendo relevante a escolha correta da frequência, o tipo de antena que será utilizado e de seu ângulo de partida.

Wivlet et al. (2015) apontam que as propagações ionosféricas em NVIS podem funcionar com eficácia para um raio de até 150 km a partir da fonte emissora. Uma faixa favorável do espectro eletromagnético seria de 3 a 9 MHz, pois esta faixa de frequência é geralmente menor que a frequência crítica da ionosfera. A frequência crítica pode ser observada através de ionogramas, transmissões abaixo deste valor sofrem o fenômeno de refração na ionosfera até sua total reflexão ao solo.

FIGURA 1 Propagação em NVIS.



Fonte: NVIS-TUGA, 2010.

A forma de cobertura do NVIS assemelha-se a um guarda-chuva nas proximidades da antena transmissora, conforme pode ser observado na figura 1. Este tipo de trans-

missão exige ângulos de partida elevados, que possam alcançar a ionosfera e serem refletidos de volta para o solo.

Porém há limitações para este tipo de transmissão que podem ocasionar zonas de silêncio nas proximidades da antena transmissora. Estas limitações estão relacionadas não somente com o ângulo de partida mas também com a frequência que se deseja transmitir em um região específica.

1 METODOLOGIA

Foi realizada uma pesquisa bibliográfica sobre os temas: características da atmosfera, no tocante ao plasma ionosférico; propagações por ondas diretas e ionosféricas e análise das características dos equipamentos disponíveis para tropas brasileiras, como ângulo de partida, sensibilidade para recepção e diretividade das antenas.

Foram utilizados artigos, dissertações, teses e livros disponíveis na literatura especializada. Assim como as recomendações da União Internacional de Telecomunicações (UIT).

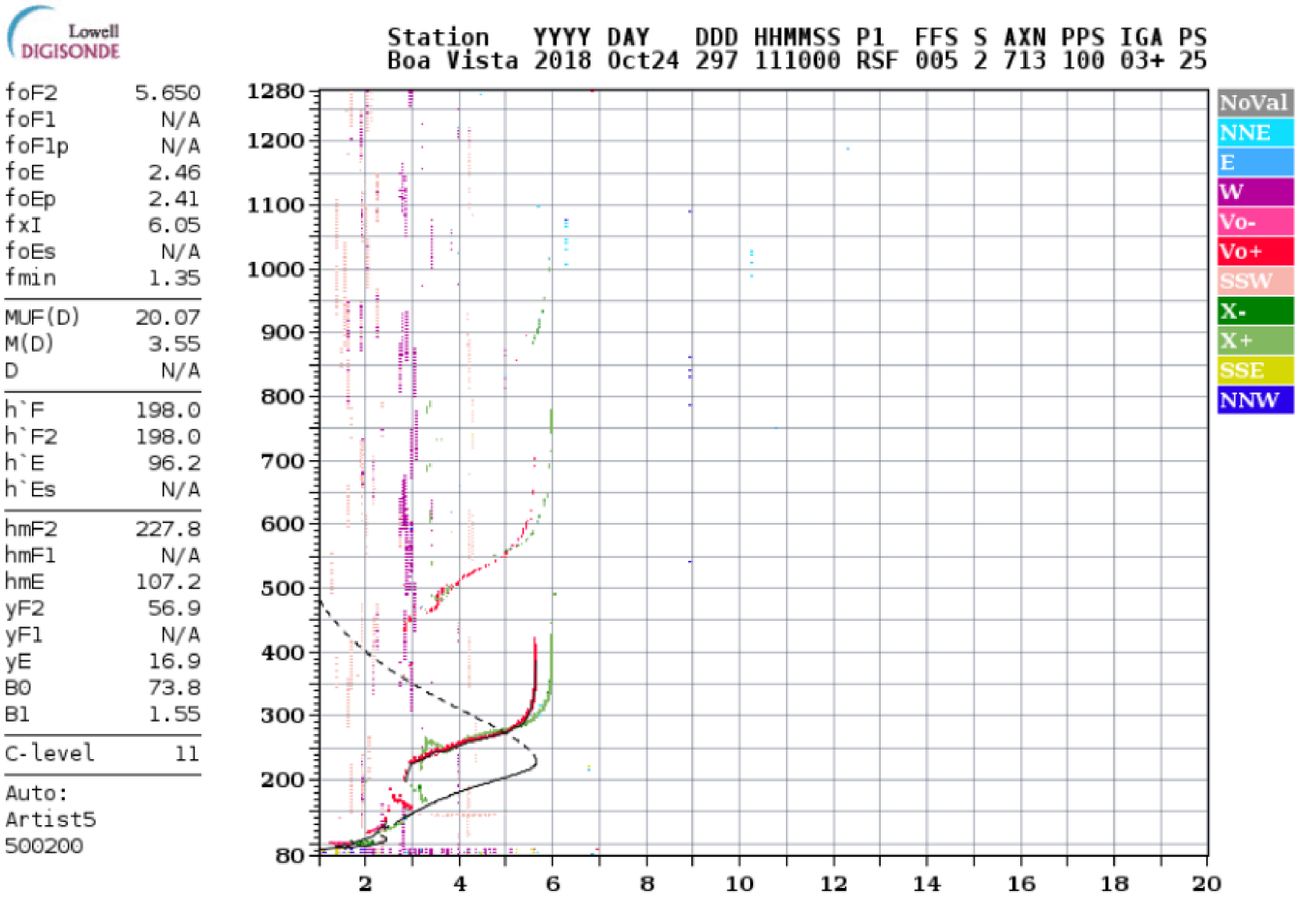
Posteriormente, foram realizados os cálculos de propagação eletromagnética, visando verificar a influência da altura acima do solo nos lóbulos de irradiação e impedância em uma antena para NVIS.

2 IONOSSONDA

Sendo afetadas por diversos fatores naturais, o estudo de propagações ionosféricas é facilitado com o uso das ionossondas. Estes dispositivos estão localizados em diversas cidades ao redor do mundo, medindo a “altura” da ionosfera e sua densidade de elétrons por camada.

Wivlet et al. (2015) afirmam que através das ionossonda é possível determinar a frequência crítica, ou a frequência de plasma,

FIGURA 2 Ionograma



Fonte: GIRO, 2018.

de uma camada, que seria a frequência mais alta de irradiação que retorna para a ionossonda em uma propagação vertical na direção do zênite (ângulo de incidência zero sobre a Normal da Terra). A figura 2 apresenta as informações principais que devem ser lidas em um ionograma.

"Fo" representa a frequência crítica de operação para determinada camada da ionosfera, sendo o parâmetro mais relevante "foF2", pois este aponta o valor de frequência para a camada mais densa, a camada F2. "MUF" representa a Máxima Frequência Utilizável, porém este parâmetro está condicionado ao ângulo de irradiação da antena.

2.1 MUF

Martyn (1935) demonstrou que: MUF = f_c*secθ, sendo f_c a frequência crítica e θ o ângulo de incidência na ionosfera. Esta relação, derivada da lei de Snell, mostra que à medida que o ângulo de incidência é ampliado, a MUF aceitará valores maiores de frequência, pois seu valor é inversamente proporcional ao cosseno (1/secθ) do ângulo.

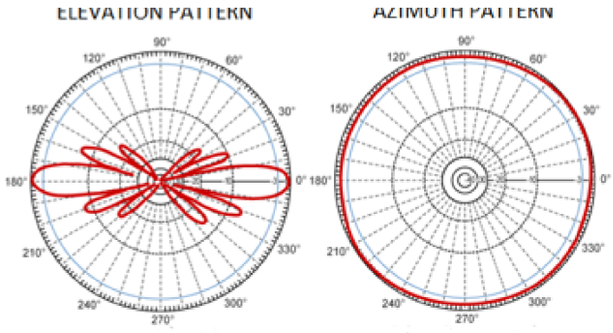
As antenas utilizadas em viaturas por exemplo, do tipo vertical, não terão ângulo de partida suficiente para refração na atmosfera em NVIS. Observando o lóbulo de radiação de antenas verticais, conforme figura 5, é possível verificar que sua maior propagação de radiação será em ângulos de incidência altos (ângulos de partida baixos). Propagações acima de 30º, pelo tamanho reduzido dos lóbulos, terão baixa probabilidade de alcançar uma estação receptora.

A tabela 1 apresenta os diversos ângulos de incidência para a frequência crítica de 5,65 MHz, utilizando como referência a altura virtual da ionosfera de 198 km, conforme obtido no ionograma da figura 2.

Utilizando a relação trigonométrica da secante, os resultados da tabela 1 foram obtidos através de:

$$MUF\ [MHz] = f_c \sqrt{((1+D/2H))} \qquad (1)$$

FIGURA 3 Diagrama de irradiação de antena veicular.



Fonte: Harris, 2017.

Onde D = distância do enlace; H = altura virtual da camada mais densa da ionosfera.

Os dados da tabela 1 indicam, por exemplo, que transmitir em uma frequência acima de 5,89 MHz para cobrir uma distância menor que 25 Km em NVIS levará a perda do sinal (situação a), pois o mesmo não refletirá nas camadas da ionosfera. De forma análoga, uma propagação de 6,03 MHz para uma estação receptora a 100 km deverá ter seu ângulo de incidência limitado a 12,8° (situação b), ou seu ângulo de partida deverá ser no máximo 77,2° (90° - 12,8° = 77,2°), caso esta frequência assuma ângulos de partidas maiores, a onda ultrapassará a atmosfera e não retornará para a Terra.

TABELA 1 Ângulos de incidência na ionosfera

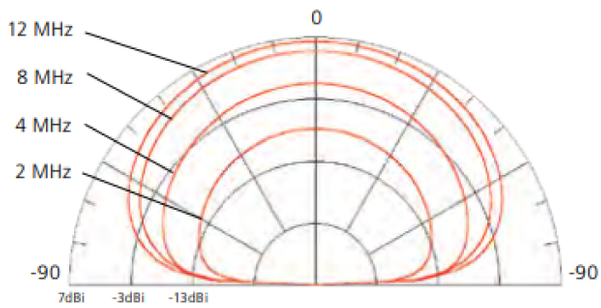
θ (graus)	fc (Hz)	MUF (Hz)	D (km)
0,3	5,65	5,88	2
0,7	5,65	5,88	5
1,0	5,65	5,88	8
1,8	5,65	5,88	14
3,3	5,65	5,89	25
6,5	5,65	5,92	50
9,7	5,65	5,96	75
12,8	5,65	6,03	100
15,9	5,65	6,11	125
21,7	5,65	6,33	175
32,0	5,65	6,46	200
34,3	5,65	6,60	225
32,0	5,65	6,93	275

θ (graus)	fc (Hz)	MUF (Hz)	D (km)
34,3	5,65	7,12	300
36,5	5,65	7,31	325
40,4	5,65	9,04	375
42,3	5,65	10,65	400
69,9	5,65	17,08	1200

Fonte: o autor, 2019.

Aplicando a equação 1 para um enlace de 1200 km obtemos como resultado uma MUF de 17,08 MHz e ângulo de incidência de 69,9°, ou ângulo de partida de 20,1°. Porém observando o diagrama de irradiação de uma antena tática típica para NVIS, a RF-1936 (dipolo cruzada), da empresa Harris, na figura 4, é possível observar que este ângulo possui baixa energia irradiada, o que levará a falha no enlace.

FIGURA 4 Diagrama de irradiação da antena RF-1936 (dipolo cruzada).



Fonte: Harris, 2017.

1.2 A ANTENA RF-1936

Esta antena faz parte de um conjunto de equipamentos táticos voltados para NVIS. A antena RF-1936 possui um mastro e quatro elementos de radiação com alimentação central. É de rápida instalação e possui baixo peso para transporte individual.

Deve ser instalada nos rádios táticos RF-5800H, que operam entre 2 a 30 MHz com uma potência máxima de transmissão de 400 W. Seu diagrama de radiação horizontal é omnidirecional e o diagrama vertical será detalhado nas seções a seguir.

Utilizando o software 4Nec2 é possível visualizar com maior qualidade o diagrama de radiação da RF-1936, conforme a figura 5. Este diagrama representa a radiação de uma antena RF-1936 a 12 MHz, onde cada elemento da antena possui 0,25λ (6,25 metros).

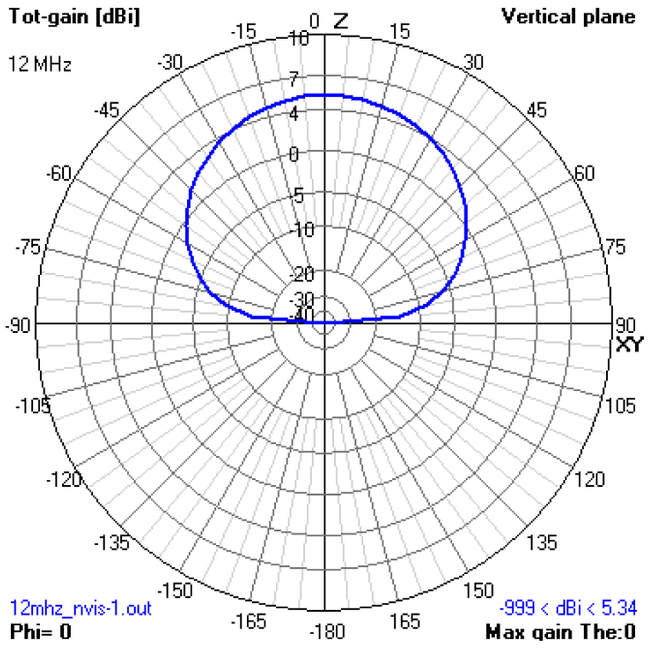
A figura 6 apresenta o perfil geométrico da antena, com seus 4 elementos. A figura 7 é uma foto da antena real.

2 PARÂMETROS

2.1 ALTURA EM RELAÇÃO AO SOLO

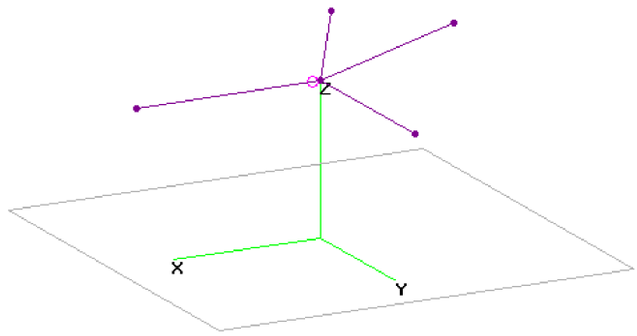
Johnson (1992) cita que antenas próximas ao solo podem ser muito influenciadas por reflexão ou absorção da radiação, especialmente para HF e quando a altura da antena é menor que 1 comprimento de onda. Para este tipo de antena, o solo será parte componente do sistema, influenciado nos lóbulos de radiação e em sua impedância.

FIGURA 5 Diagrama de irradiação da antena RF-1936 no software 4nec2 para 12 MHz.



Fonte: o autor, 2019.

FIGURA 6 Perfil geométrico da antena RF-1936



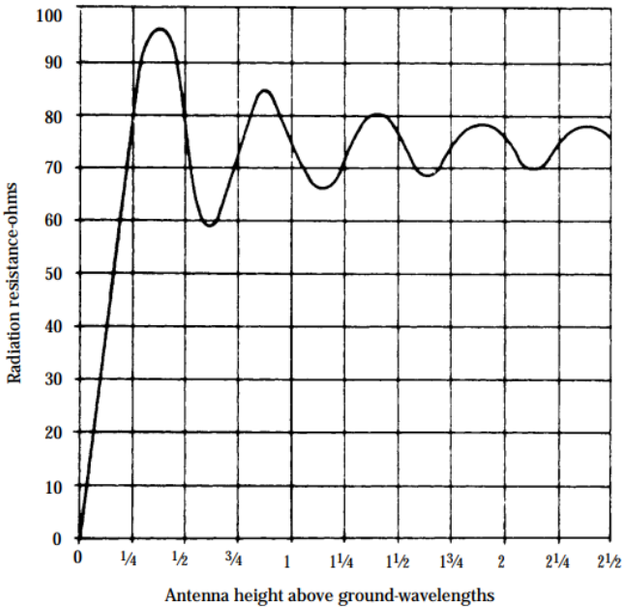
Fonte: o autor, 2019.

FIGURA 7 Antena RF-1936

Fonte: Harris (2017)

A impedância típica de uma antena dipolo é 73 ohms (Laster, 2001). No caso da antena RF-1936, este valor é 50 ohms (HARRIS, 2005) e poderá ser modificado de acordo com a altura em relação ao solo, variando desde 95 ohms até valores próximos de zero, conforme figura 8.

FIGURA 8 Impedância de antena dipolo de acordo com a altura em relação ao solo.



Fonte: Laster, 2001.

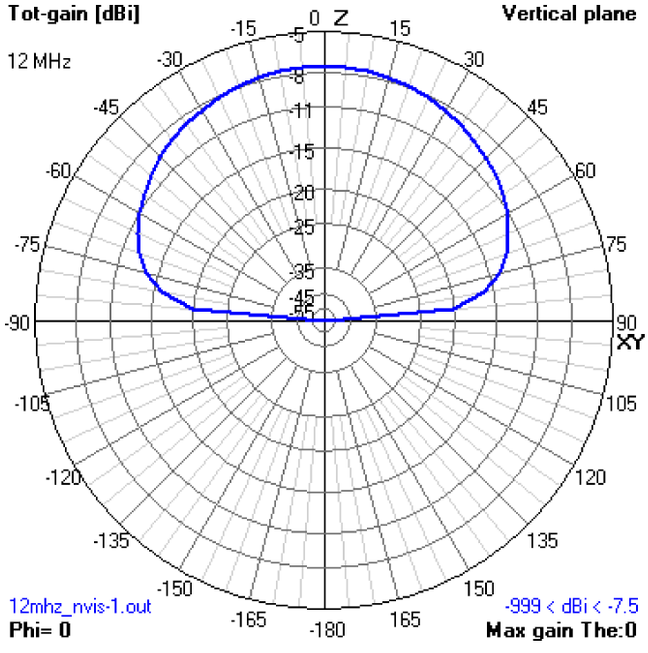
As simulações de altura em relação ao solo foram realizadas no software 4nec2, utilizando o modelo de solo Sommerfeld-Norton (ϵ_f = 13, σ_f = 5 mS/m), que representa uma simulação realista de perdas e reflexão (Burke, 1981). O raio dos fios foi considerado 10 mm. A figura 9 apresenta o diagrama para a altura de 0,02λ, que apresenta alta diretividade, porém com baixo ganho (menos de -7 dBi).

A figura 10 apresenta o diagrama de radiação para 0,06λ, onde já é possível observar que uma distância maior do solo implica em um ganho maior.

A figura 11 apresenta 4 comprimentos de onda, 0,02λ, 0,06λ (já citados), 0,2λ e 0,4λ. À altura de 0,4λ do solo a antena perde diretividade, formando dois lóbulos laterais acentuados, reduzindo esta altura, a 0,2λ (em azul no gráfico), o diagrama volta a ser mais eficiente para NVIS.

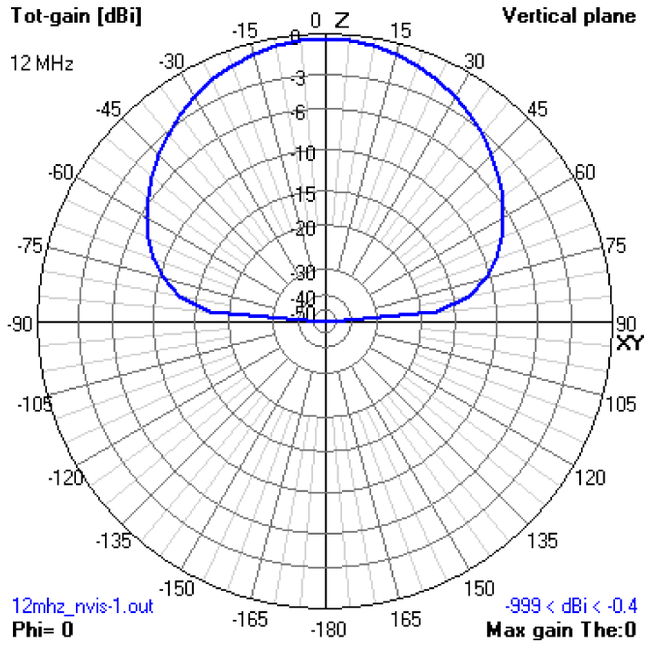
0,2λ (5 metros) apresentou-se como a altura ótima para o diagrama, a partir deste valor, os lóbulos irão se achatar cada vez mais ou formar lóbulos laterais, o que seria um desperdício para o NVIS, conforme figura 12.

FIGURA 9 Antena RF-1936 a 0,02λ do solo.



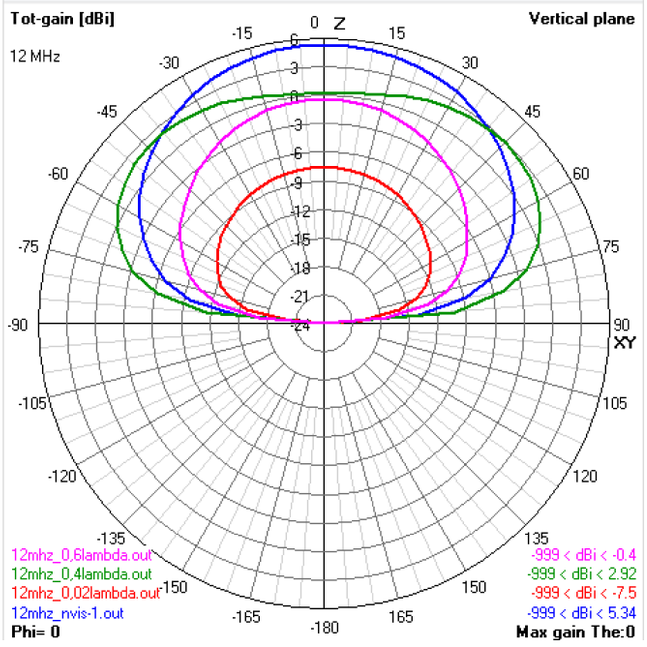
Fonte: o autor, 2019.

FIGURA 10 Antena RF-1936 a 0,06λ do solo.



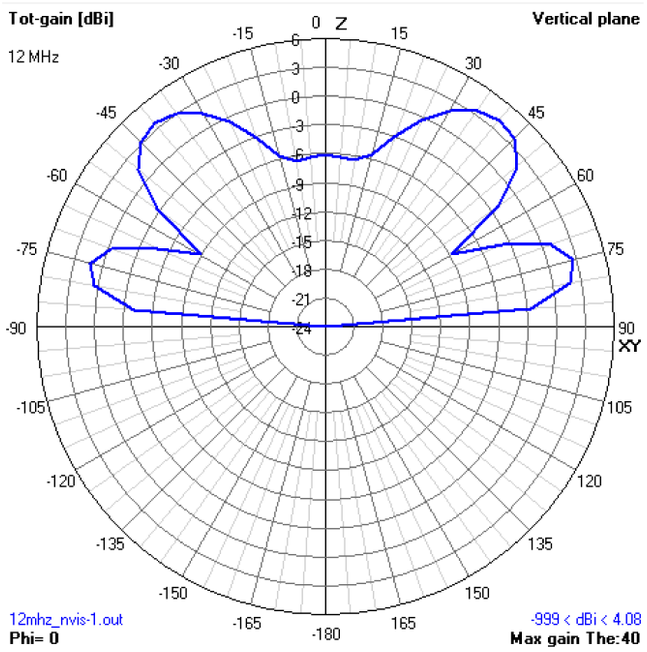
Fonte: o autor, 2019.

FIGURA 11 Antena RF-1936 a 0,02λ (vermelho), 0,06λ (rosa), 0,2λ (azul) e 0,4λ (verde) do solo.



Fonte: o autor, 2019.

FIGURA 12 Antena RF-1936 a 1λ do solo.



Fonte: o autor, 2019.

2.1 ANÁLISE DE RADIAÇÃO

2.1.1 Eficiência da Radiação

A Relação de Ondas Estacionárias (em inglês VSWR) obteve como resultado 1,98:1, figura 13. Utilizando a equação 2.2 é possível obter o coeficiente de reflexão:

VSWR: 1+|Γ|/1- |Γ|; (2.1)

|Γ| = VSWR-1/ VSWR+1; (2.2)

Potência refletida (%) = 100*|Γ|^2 (2.3)

Potência refletida (dB) = 10log(|Γ|^2). (2.4)

Para 1,98:1, o coeficiente de reflexão é 0,33, o percentual de potência refletida é 10,8% ou -9,66 dB, o que se encontra em um valor aceitável para o sistema.

FIGURA 13 VSWR da antena RF-1936.

Filename	12mhz_nvis-1.out		Frequency	12	Mhz
			Wavelength	24.98	mtr
Voltage	73.6 + j 0 V		Current	1.36 - j 0.98 A	
Impedance	35.7 + j 25.7		Series comp.	516.2	pF
Parallel form	54.2 // j 75.3		Parallel comp.	176.1	pF
S.W.R.50	1.98		Input power	100	W
Efficiency	100	%	Structure loss	0	uW
Radiat-eff.		%	Network loss	0	uW
RDF [dB]	7.33		Radiat-power	100	W

Fonte: o autor, 2019.

2.1.2 EIRP

O Cálculo da Potência Efetiva de Saída (em inglês EIRP) foi analisado a partir da potência do equipamento mais o ganho da antena menos as perdas por cabos e conectores. Sendo considerado 1 dB de perda para cada metro do cabo coaxial (para 0,2λ) e 0,25 dB para cada conector.

$$EIRP = Pt - Lc + Ga \quad (3)$$

O que resultou 48.34 dB.

CONCLUSÃO

Visando a propagação em NVIS, o melhor resultado obtido foi 0,2λ (5 metros) que apresentou-se como a altura ótima para o diagrama. A partir deste valor, devido à reflexão no solo, os lóbulos irão se achatar cada vez mais ou formar lóbulos laterais, o que seria não desejável para este tipo de propagação.

Para o resultado de 0,2λ, a impedância obtida apresentou o valor complexo de 35,7 + j25,7, o que aponta a presença de uma reatância indutiva (X>0) e indutância de 0,34 ohms. Porém ao se verificar a VSWR, encontra-se o valor de 1,98:1, o que implica numa potência refletida menor que 12%.

INFLUENCE OF HEIGHT ABOVE THE GROUND ON RADIATION LOBBLES AND IMPEDANCE IN A NVIS ANTENNA

ABSTRACT: Antennas close to the ground can be greatly influenced by reflection or radiation absorption, especially for NVIS (Near Vertical Incident Skywave) and when the antenna height is less than 1 wavelength. For this type of antenna, the soil will be a component part of the system, influenced by the radiation lobes and their impedance. Particularly for the Brazilian territory, the soil conductivity in jungle regions is very low, which increases the need for this type of propagation, to the detriment of surface waves or direct waves. The results indicated that the ideal height is 0.2λ (5 meters), which presented as the optimal height for the radiation diagram. From this value, due to the reflection in the soil, the lobes will flatten or form lateral lobes, which would be undesirable for this type of propagation. Below this value, there is a very marked mismatch of impedance with the transmission line, increasing the reactance and loss of radiation to the ground.

Keywords: HF antennas ionospheric waves. NVIS. Links.

REFERÊNCIAS

Advisory Group for Aerospace Research and Develpment (AGARD). AGARD-AG-326 - Radio Wave Propagation Modeling, Prediction and Assessment. NORTH ATLANTIC TREATY ORGANIZATION. 1990.

ASSIS, Mauro S., FILHO, Rafael C. Pinto. Measurements of the electrical characteristics of vegetation in a dense jungle. Publicado em Proceedings of the Fourth European Conference on Antennas and Propagation. 12 a 16 julho 2010.

BURKE, G. J. et al., Computer modeling of antennas near the ground. Electromagnetics, vol. 1, no. 1, pp. 29–49, Jan. 1981.

HARRIS. Harris Falcon II RF-5800H-MP. NEW YORK, 2005.

HARRIS. Harris Falcon III RF-7800V-HH. NEW YORK, 2017.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). World Atlas of Ground Conductivities. Recommendation 832. 1992.

JOHNSON, Richard C. Antenna Engineering Handbook. 3rd ed. McGraw-Hill. NEW YORK, 1993.

LASTER, Clay. The Beginner´s Handbook of Amateur Radio. 4th ed. McGraw-Hill. NEW YORK, 2001.

NVIS-TUGA. NVIS Tático. 2010. Acesso em 24/10/2018. Disponível em http://nvis-tuga.blogspot.com/2010/11/nvis-tactico.html.

Optimum Antenna Height for Horizontal Dipole Antennas. 2015. IEEE Antennas and Propagation Magazine, Vol. 57, No. 1, February 2015.

WIVLET, B. A. et al. Near Vertical Incidence Skywave Propagation: Elevation Angles and Optimum Antenna Height for Horizontal Dipole Antennas. 2015. IEEE Antennas and Propagation Magazine, Vol. 57, No. 1, February 2015.

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras. Pós-Graduado em Gestão de Sistemas Táticos de Comando e Controle pela Escola de Comunicações. Mestrando em Engenharia Elétrica pela Universidade de Brasília. Possui cursos na área de Rádios definidos por software, Sistemas Satelitais e Comando e Controle. Foi instrutor na Academia Militar das Agulhas Negras. Atualmente serve na Escola de Comunicações. Pode ser contactado através do e-mail: silvamarques.anderson@eb.mil.br.

Itens de notícias relevantes

INFORMATIVO TÉCNICO

DOUTRINA

SISTEMA DE COMUNICAÇÕES DO *COMBAT-TEAM* DO EXÉRCITO DA ÁFRICA DO SUL EM UM AVANÇO OU UM ATAQUE

Daniel Moura Félix Cardoso
Pós-graduado em Operações Militares

RESUMO: Este trabalho apresenta um estudo realizado com base em um curso realizado no Exército da África do Sul *(SAArmy)* de comandante de subunidade integrada, aonde as instruções teóricas e práticas puderam dar uma noção da organização em termos de Comando e Controle por parte daquele Exército. Foi observado o sistema de comunicações de uma Força-Tarefa Mecanizada nível Companhia *(Combat-Team)* empregado na prática em um avanço e em um ataque. Os elementos reunidos nessa Força-Tarefa possuem viaturas distintas, para finalidades diversas em uma operação militar. Dessa forma, foi estudado o sistema de comunicações de um Avanço e um Ataque, sendo possível verificar as possibilidades disponíveis tanto pela flexibilidade disponibilizada como pela integração das viaturas.

Palavras-chave: *Combat-Team*. Força-Tarefa Mecanizada. *SAArmy*. Sistema de Comunicações. África do Sul

INTRODUÇÃO

Com a evolução do combate para a de Guerra de 4ª geração, onde um exército representando uma nação combate uma força irregular, insurgente, normalmente que se utiliza de atividades terroristas, e que não é reconhecida pela nação onde se situa geograficamente aquela força, houve a necessidade de incremento dos armamentos e equipamentos militares, buscando um menor dano colateral à população que circunda o ambiente da Guerra.

Até o ano de 1994, a Força de Defesa da África do Sul (até então conhecida como *SADF*), composta pelo Exército (*SAArmy*), Marinha *(SANavy)* e Força Aérea *(SAAF)* não possuía muitos parceiros para confecção/aquisição de produtos de defesa, fazendo com que a indústria bélica nacional fosse fortalecida. Dessa forma, vários dos equipamentos, armamentos, carros de combate, carros mecanizados, artilharia e até antiaérea foram construídos dentro da República da África do Sul *(RSA)*.

Por mais que diversos produtos de outros exércitos tenham sido tomados por base para a confecção do seu próprio Material de Emprego Militar (MEM), a confecção era interna, garantindo assim uma autossustentação em caso de necessidade. Da mesma forma, os equipamentos intermediários que compõem esses carros de combate e outros sistemas necessários ao Comando e Controle (C^2) foram também produzidos na *RSA*. Sendo assim, foram desenvolvidos os equipamentos rádio e os sistemas integradores destes rádios, facilitando assim o Sistema C^2.

Dessa forma, estudar o que já foi experimentado em conflitos é de extrema importância para que possa existir uma forma de afastar o que já foi comprovado que não é uma boa prática e tentar aperfeiçoar o que já funciona para outras Forças de países irmãos.

1 CARACTERIZAÇÃO DO *SAARMY*

O *SAArmy* é uma Força Armada referência do continente Africano. Em diversos pontos da história, estiveram em combate com países e somaram assim bastante conhecimento, experiência e puderam aprimorar assim os seus equipamentos e formas de combate.

Hoje em dia, o *SAArmy* tem trabalha-

do na pacificação de diversos países da África como o Congo (DRC) pela Missão das Nações Unidas no Congo (MONUSCO), locais onde contribuem para o bem-estar social.

A modularidade de um exército, preparando-se especificamente para a determinada missão, pode garantir que sua tropa tenha êxito ou não. Busca-se não empregar o soldado sem o equipamento necessário ou, ainda, sem o conhecimento da cultura local, tudo visando não ferir preceitos básicos à população e evitando que seja gerado o efeito contrário ao desejado.

Nesse sentido, o emprego dos armamentos, equipamentos e carros deve ser específico para determinada missão, levando-se em conta o cenário do conflito/pacificação e o terreno em que será empregada a respectiva Força.

Os veículos empregados em conflitos devem ser carros preparados para atender então às demandas apresentadas. Veículos blindados, com canhões pesados, sob lagartas ou carros que transportam apenas armamentos de artilharia antiaérea são largamente empregados em conflitos regulares, como guerras contra outros exércitos ou contra Forças insurgentes. Entretanto, carros blindados, mecanizados para transporte de pessoal ou antiminas terrestres, bem como viaturas motorizadas podem ser utilizados tanto para as Operações de Guerra como de Não-Guerra (no caso, Pacificação).

Sendo assim, observando-se a variedade de veículos que podem compor uma frota de uma Força Terrestre, existem algumas linhas de ação que pode ser vislumbradas no que tange ao Sistema C²:

a) todos os veículos (independente da natureza do veículo ou construtora) possuírem o mesmo sistema integrador, favorecendo as comunicações;

b) cada tipo diferente de veículo possuir o seu sistema singular de comunicações, o que implicaria às unidades de comunicações terem mais dificuldade no manejamento dos diversos sistemas e dificultar as comunicações; ou

c) não serem utilizados sistemas de integração no veículo, fazendo com que os sistemas de comunicações devam ser operados de forma independente aos veículos. Nesse caso, por exemplo, o Radio Operador (ROp) deverá colocar a antena do rádio para fora da escotilha durante o emprego do equipamento rádio e, consequentemente, a segurança física da tropa será desfavorecida.

Dessa forma, torna-se desejável que a primeira opção seja adotada, pois facilita todo o trabalho de comunicações, conferindo à tropa mais celeridade nas suas ações e favorecendo o sucesso da operação.

Nesse contexto, o *SAArmy* conseguiu manter esse sistema integrador pois a produção dos seus veículos foi realizada na própria RSA.

O sistema utilizado para integrar os rádios veiculares no *SAArmy* é bastante simples e intuitivo. A seguir, serão apresentadas as principais características do referido sistema integrador, bem como as viaturas que o utilizam e os equipamentos rádios que o compõem.

2 VIATURAS EMPREGADAS NO *SAARMY*

A Família RATEL compõe uma linha de carros mecanizados com a mesma plataforma de 3 eixos diferenciando apenas o armamento que carrega, podendo ser 12,7mm (cal 0.50), canhão 30mm ou então com torre para canhão anticarro 105mm, ou ainda escotilha larga para morteiro 81mm de tiro embarcado. Todos esses veículos compõem o *Combat-Team*.

O veículo mecanizado ROOIKAT é um carro para a cavalaria de reconhecimento, com canhão 76mm e normalmente os pelotões são compostos por 4 carros desses. É bastante

FIGURA 1 Rattel - Viatura mecanizada empregada pela Infantaria e outras armas. A Familia Rattel possui diversas Torres e propósitos.

Fonte: o autor, 2018.

usual a utilização do pelotão de "*Armoured--Cars*" no *Combat-Team* para fazer reconhecimento do terreno e receber o alerta oportuno do inimigo.

FIGURA 2 Rooikat - Viatura do Regimento de Cavalaria Mec com canhão 76mm

Fonte: o autor, 2018.

O carro de combate OLIFANT nas suas versões Mk1 e Mk2 são utilizados no *Combat-Team* como força de choque para dizimar o inimigo encontrado na posição. O carro de combate que possui um canhão 105mm é bastante preciso e pode atingir uma velocidade de 60km/h.

O obuseiro autopropulsado GV-6 da artilharia do *SAArmy* é um veículo sob lagartas e um canhão montado de 155mm. Normalmente é colocado em apoio direto ao *Combat-Team* que encontra-se no avanço realizando a Marcha para o Combate buscando o contato com o inimigo.

O veículo motorizado KASPIR não possui blindagem semelhante ao mecanizado RATEL, mas possui proteção antiminas e seu desenho é em formato "V", que dispersa o efeito de minas anticarros para os lados do veículo, evitando assim a concentração da explosão no centro do veículo.

Todos esses carros possuem mecânica, proteções, armamentos e finalidades diferentes mas de todas as características distintas que possuem, uma é comum a todos: o Sistema C².

3 EQUIPAMENTOS RÁDIO EMPREGADOS PELO SISTEMA C² DO *COMBAT-TEAM*

Os equipamentos rádio utilizados pelo Exército Sul-africano em uma Força-Tarefa Mecanizada atualmente são os equipamentos C21, B46 e A43. Todos eles possuem características distintas mas foram todos produzidos no próprio país da África do Sul.

O equipamento Rádio C21 é um rádio tático que opera em HF e pode ser utilizado em uma estação fixa ou sobre uma plataforma móvel (viatura) para contato a longa distância. Trabalha na faixa de frequência de 1,6 até 29,999MHz e pode operar em AM e SSB. As potências de saída podem variar de 25W a 100W. Possui a função de salto de frequência e opera com antenas verticais ou horizontais. Utiliza bases de antena para fazer o casamento de impedância e consequente alteração do comprimento elétrico da antena, reduzindo a onda refletida para o rádio.

O equipamento Rádio A43 é um rádio leve, de utilização pela tropa a pé como mochila, tático que opera em VHF a curtas distâncias e normalmente em linha de visada. Sua utilização também pode ser veicular. Trabalha na faixa de frequência de 30 a 87,975 MHz, permitindo a configuração de frequências em até 100 canais e além de operar em FM, pode transmitir dados em tecnologia digital FSK. As potências de saída podem variar de 0,4 W a 4 W. Possui a função de transmissão segura encriptada, transmissão de dados e medidas de proteção eletrônica integradas ao rádio. Opera com antenas verticais e horizontais, bem como faz o mesmo casamento de impedância com bases de antena.

O equipamento Rádio B46 é um rádio VHF próprio para operações em base veicular e é compatível com o rádio A43. Opera na faixa de frequência de 30 a 87.975 MHz e possui também configuração de frequência em 100 canais pré-estabelecidos. Trabalha em FM e envia dados digitais em PSK, mas a grande diferença em relação ao A43 é sua saída de potência nominal que varia de 5 W a 50 W, podendo garantir assim um maior alcance. Da mesma forma que o A43, possui a função de transmissão segura encriptada, transmissão de dados e medidas de proteção eletrônica integradas e opera com antenas verticais e horizontais, além de possuir bases de antena para acoplamento elétrico com o rádio.

FIGURA 3 Equipamento Rádio VHF

Fonte: o autor (2018)

2.3 SISTEMA DE INTEGRAÇÃO DOS VEÍCULOS DO *COMBAT-TEAM*

Os equipamentos auxiliares, de comutação e de gerenciamento do rádio é que são o grande diferencial para o sistema C² do *Combat-Team* Mecanizado. Essa integração entre os componentes do sistema e a rápida operação podem garantir valiosos segundos em um campo de batalha.

O capacete com fone de ouvido e microfone (headset) é bastante similar ao utilizado pelo Exército Brasileiro, porém, os fones do tipo extra-auriculares separam uma recepção de rádio por ouvido, fazendo assim com que o militar consiga escutar a conversação de dois rádios distintos de forma simultânea. O normal durante um avanço ou um ataque, é que o rádio cuja conversação seja escutada no falante do ouvido esquerdo seja o do escalão subordinado e o do lado direito o do escalão superior.

A caixa de peito é pendurada com uma cinta que abraça o pescoço do militar e o seu peitoral, conectando o headset com a caixa de controle que será descrita a seguir. Esta cai-

xa de peito facilita o manuseio do sistema com a facilidade de selecionar se o militar irá falar com o rádio que está na frequência do escalão subordinado ou do escalão superior, possuindo também um botão PTT - "*Push to Talk*"ou "Aperte para Falar". Se o militar deseja falar no intercomunicador da própria viatura, não precisa apertar o botão, a transmissão é livre para os outros militares dentro da viatura pelos headsets ou pelos alto-falantes.

A caixa de controle é a que liga a caixa de peito com os equipamentos rádio propriamente ditos. É ela que faz a gerência dos rádios, oferecendo assim a interface com até seis rádios que podem ser dispostos na viatura. Assim sendo, o operador pode selecionar na caixa os equipamentos rádio que quiser utilizar, integrando por exemplo a rede de comando, de logística, de pedidos aéreos, com o escalão subordinado, de inteligência, de apoio de fogo ou outras. A seleção de quais equipamentos rádio comporão determinada viatura será baseada na função do comandante do carro, ou seja, se aquela viatura precisa de contato com determinada rede ou não.

FIGURA 4 Capacete com fone de ouvido e caixa de controle das viaturas.

Fonte: o autor, 2018.

Como acessórios existem, ainda, os alto-falantes do carro, caixas de controle adicionais para elementos de comunicações que por ventura façam parte daquela viatura, antenas com suas respectivas bases de antena que facilitam a fixação à viatura, os cabos de radiofrequência que ligam o rádio às antenas e os cabeamentos para a rede elétrica que liga os rádios à alimentação (baterias da própria viatura).

CONCLUSÃO

O Sistema de Comando e Controle do *Combat-Team* no Exército da África do Sul é bastante eficiente do ponto de vista de operacionalidade, pois facilita assim a transmissão de comandos rápidos, provendo assim uma entrega rápida de pedidos de apoio aéreo, de fogo, coordenação no assalto ou outros aspectos que necessitam ser coordenados.

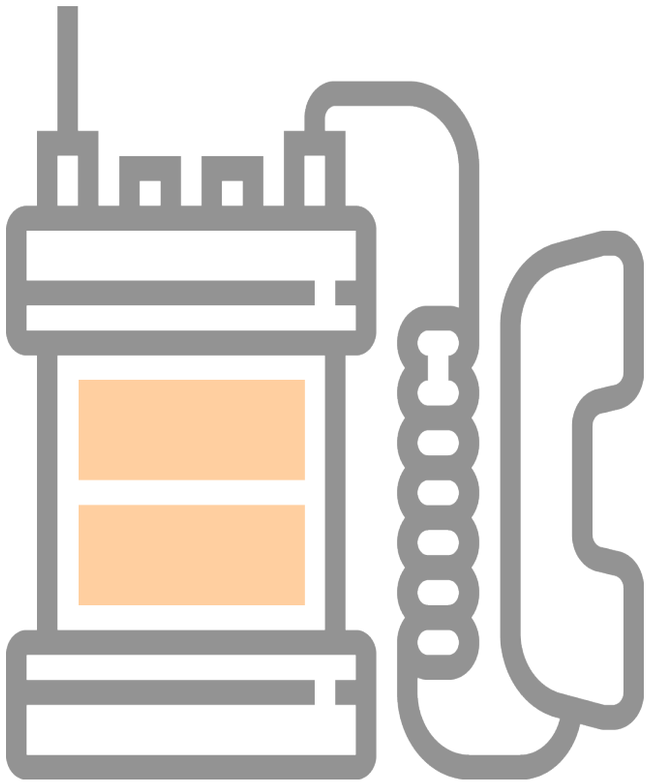
Em uma era de mecanização da Força Terrestre, aspectos relativos às comunicações são tão relevantes quanto o tipo de armamento ou de blindagem que o veículo irá possuir. Garantir o Comando e Controle de uma tropa é posicionar corretamente uma fração no terreno em um ataque, providenciar apoio de artilharia no momento exato e transportar o seu fogo quando necessário e cerrar os meios de reserva no local necessário de emprego, embarcando tecnologia de ponta como georreferenciamento, encriptação de fonia automática ou proteção eletrônica contra possíveis ataques.

Observar um Exército que experimentou na prática esse tipo de comunicações em guerras contra Lesotho em 1998 e contra a Angola (apoiada por Cuba) no período de 1966 a 1989, faz acreditar que essa sistemática funcionou para o combate naquele período, terreno e contra aquele determinado inimigo. Ainda hoje é ensinado e aplicado esse tipo de sistema de Comando e Controle nos bancos escolares do *SAArmy* (Exército da África do Sul) e de suas tropas.

THE SOUTH AFRICAN ARMY COMBAT-TEAM SIGNALS SYSTEM IN AN ADVANCE OR AN ATTACK

ABSTRACT: This paper presents a data set based on a course conducted in the South African Army (SAArmy) of an integrated subunit system. The communications system of the Mechanized Task Force Level (Combat-Team) was presented with the objective of advancing and in an attack. The elements gathered in the Task Force have different infrastructures, for different purposes in a military operation. In this way, the communication system of an Advance and an Attack in practice was studied, being able to verify how the options can be made available through the interface of these vehicles

Keywords: Combat-Team. Mechanized Task-Force. SAArmy. Signals System. South Africa.



REFERÊNCIAS

ÁFRICA DO SUL. South African Army. Volume 8: Infantry Battle Handling. Book 2: Infantry Operations. Pamphlet 4: Command And Control.1996.

ÁFRICA DO SUL. South African Army. Volume 8: Infantry Battle Handling. Book 2: Infantry Operations. Pamphlet 6: Offensive Operations.1996.

ÁFRICA DO SUL. South African Army. Volume 8: Infantry Battle Handling. Book 2: Infantry Operations. Pamphlet 9: Cooperation with other Arms.1996.

Nota de Aula do Integrated Subunit Commander's Course - ISUC, disponibilizada pelo Combat Training Centre – Lohatla, SAArmy, SANDF, República da África do Sul.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Infantaria do Exército Brasileiro, Comandante de Subunidade Integrada pelo Exército da África do Sul. É pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficais. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email: felix.daniel@eb.mil.br.

Itens de notícias relevantes

INFORMATIVO TÉCNICO

CIÊNCIA E TECNOLOGIA

MINIATURIZAÇÃO DE ANTENAS ATRAVÉS DO USO DA GEOMETRIA FRACTAL DA CURVA DE KOCH

Rafael Costa Barros
Pós-graduado em Gestão de Sistemas Táticos de Comando e Controle

RESUMO: A geometria fractal para o desenvolvimento de antenas tem recebido grande atenção do campo da engenharia de antenas. As antenas fractais apresentam características que tornam o seu emprego vantajoso em relação ao modelo convencional de desenvolvimento de antenas. A Ilha Fractal de Von Koch é uma forma originada a partir de iterações do tipo Curva de Koch, que são feitas em cada um dos lados de um triângulo equilátero. Essa geometria tem como uma das principais vantagens o aumento do perímetro de uma determinada antena, sem aumento de sua área.

Palavras-chave: Antena Fractal. Curva de Koch, Miniaturização

INTRODUÇÃO

A geometria fractal para o desenvolvimento de antenas tem recebido grande atenção do campo da engenharia de antenas, devido ao crescimento acelerado das comunicações sem fio. As antenas fractais apresentam características que tornam o seu emprego vantajoso em relação ao modelo convencional de desenvolvimento de antenas. Segundo (R. Jothi Chitra and V. Nagarajan, 2016) as principais vantagens das antenas fractais são o tamanho reduzido da antena, o baixo custo, a operação em multibanda e a operação em banda larga com um excelente desempenho da antena.

Conforme (Waqas, M., Ahmed, Z., & Ihsan, M. B., 2009) as principais vantagens do uso de antenas fractais são: a miniaturização, uma ótima eficiência de radiação e a operação em banda larga. Nas últimas décadas foram empregadas diversas técnicas que utilizam a geometria fractal: Curva de Koch, Triângulo de Sierpinski e a Árvore Fractal.

As antenas fractais empregam o conceito do fractal existente na natureza, pela forma de desenvolvimento desse tipo de antena levar em consideração o formato dos fractais existentes na natureza, como por exemplo: floco de neve, constituição da linha costeira do continente, vaso sanguíneo, vegetal e o curso de um rio.

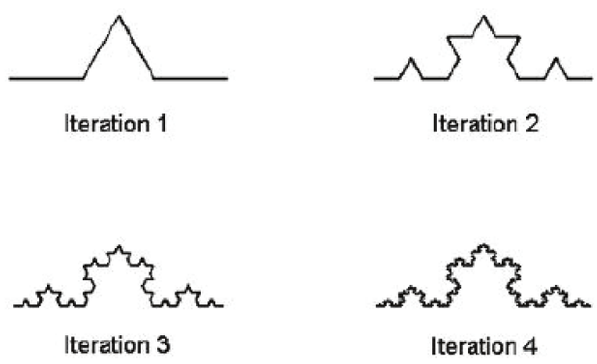
A seguir serão identificados as atuais contribuições da geometria fractal da Curva de Koch na engenharia de antenas.

1 CURVA DE KOCH

Benoit Mandelbrot (Mandelbrot, 1982) definiu como fractais as formas que exibem o mesmo padrão em escalas múltiplas e com dimensões geométricas, que são valores não inteiros. Essas formas foram estudadas exaustivamente durante todo o século XX, com o objetivo de resolver problemas em que apenas com a geometria euclidiana não foi suficiente.

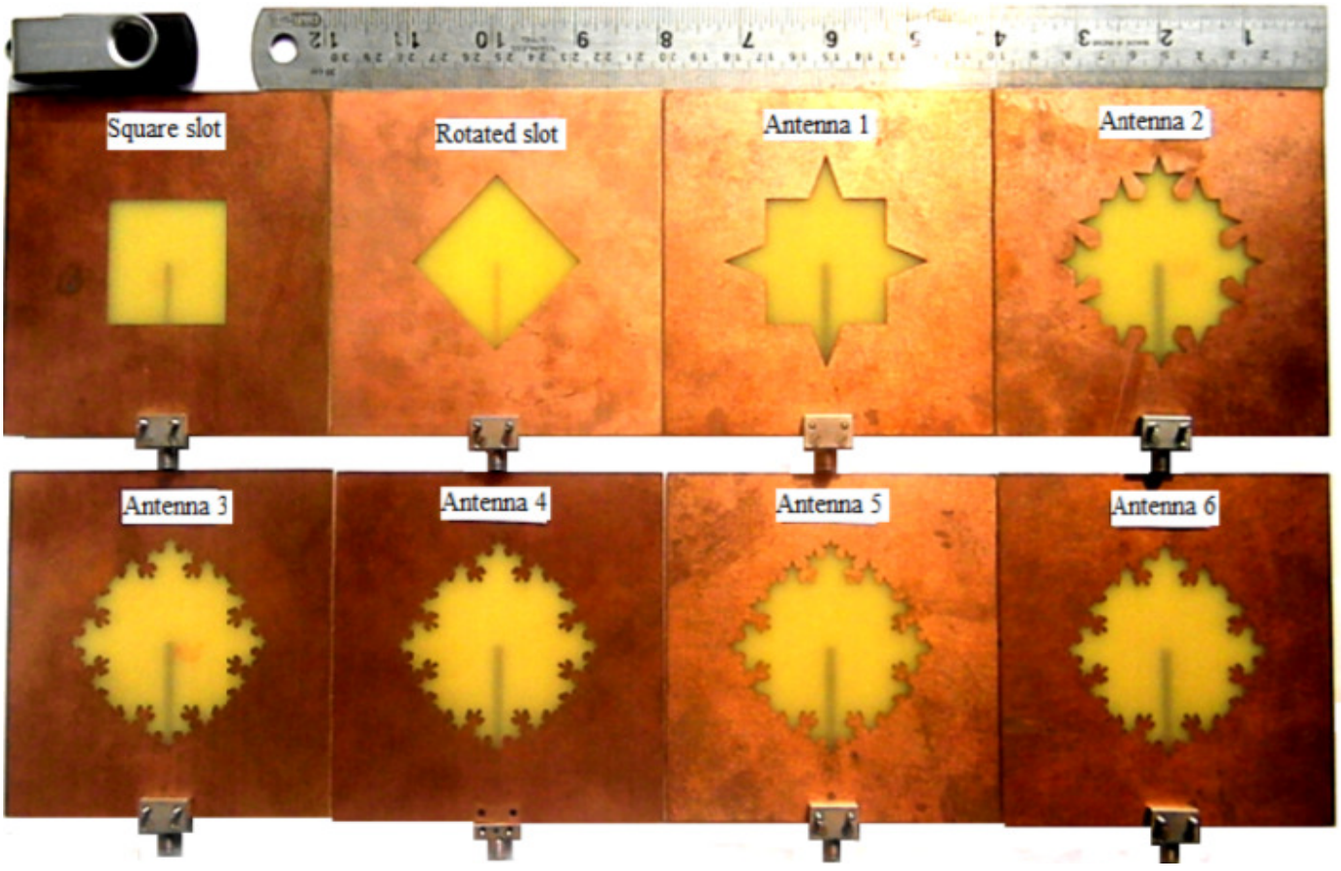
Conforme (H. O. Peitgen, H. Jurgens & D. Saupe, 1992), a Curva de Koch trata-se de uma construção geométrica que é formada a partir de um iniciador, uma linha reta. Esse iniciador é divido em 03 (três) partes iguais, em seguida é suprimido o segmento central que será substituído por 02 (dois) segmentos de mesmo tamanho que o segmento suprimido. Na figura abaixo podemos observar o processo descrito acima.

FIGURA 1 Iterações a partir de um segmento com o uso da geometria fractal da Curva de Koch.



Fonte: RAMADAN, A. & AL-HUSSEINI, M. & KABALN, K. Y. & EL-HAJJ, A., 2011

FIGURA 2 Exemplos de antenas que fazem uso da geometria fractal da Curva de Koch



Fonte: REDDY, V. V., 2018

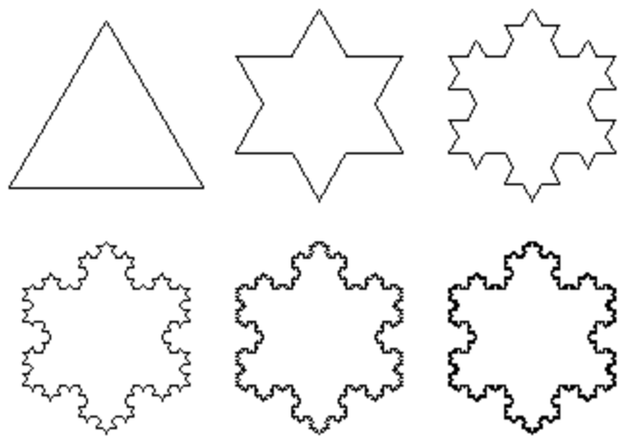
2 ILHA FRACTAL DE KOCH

A Ilha Fractal de Von Koch é uma forma originada a partir de iterações do tipo Curva de Koch, que são feitas em cada um dos lados de um triângulo equilátero. Esse tipo de geometria tem sido utilizado de diversas formas para o desenvolvimento de antenas. Essa geometria tem como uma das principais vantagens o aumento do perímetro de uma determinada antena, sem aumento de sua área.

A Ilha Fractal de Koch também conhecida como Koch Snowflake é um tipo de especial de small loop antena. Esse tipo de antena tem como característica a capacidade de estabelecer frequências de ressonância com uma ótima resistência de radiação a partir de um loop com o comprimento de 01 (um) comprimento de onda. Conforme (W. L. Stutzman & G. A. Thiele, 2013), as antenas de loop pequenas possuem várias aplicações, especialmente como antena receptora.

Conforme (Kathiriya H. J., Dalsania P. C. & Neha S., 2014) a frequência de ressonância aumenta com o aumento do número de iterações. O comportamento multibanda é obtido conforme o número de iterações aumenta. As perdas de retorno aumentam conforme o número de iterações aumenta. A largura de banda da antena também aumenta com o aumento do número de iterações. A melhoria no VSWR também é observada com o aumento de iterações.

FIGURA 3 Exemplos de antenas que fazem uso da geometria fractal da Curva de Koch



Fonte: http://www.oxfordmathcenter.com/drupal7/node/417, 2019

Segundo (Y.K. Choukiker & S. K. Behera, 2017) com a forma Koch Snowflake podemos obter um excelente padrão de radiação omnidirecional em uma larga banda de frequências .

CONCLUSÃO

Conforme pudemos observar, a geometria fractal do tipo Curva de Koch tem sido utilizada amplamente devido aos benefícios gerados: miniaturização, aumento da largura de banda, diminuição da VSWR e aumento da eficiência de radiação.

Dessa forma, devido à grande demanda atual na área das comunicações sem fio, a geometria fractal se apresenta como uma excelente opção para o desenvolvimento de antenas.

MINIATURIZATION OF ANTENNAS WITH THE USE OF FRACTAL GEOMETRY OF THE KOCH CURVE

ABSTRACT: The fractal geometry for the development of antennas has received great attention from the field of antenna engineering. The fractal antennas present characteristics that make their use advantageous in relation to the conventional model of antenna development. The Von Koch Fractal Island a form originated from Koch Curve type iterations, which are made on each side of equilateral triangle. This geometry has as one of the main advantages the increase of the perimeter of a certain antenna, without increasing its area.

Keywords: Fractal Antenna. Koch Curve. Miniaturization

REFERÊNCIAS

GUPTA, M. & MATHUR, V. Koch fractal-based hexagonal patch antenna for circular polarization. Department of Physics, JECRC University, Jaipur, India & Department of Electronics and Communication, JECRC University, Jaipur, India, 2017.

MANDELBROT, B.B. The Fractal Geometry of Nature. W.H. Freeman and Company: San Francisco, 1982.

PEITGEN, H. O., JURGENS, H. & SAUPE, D. Chaos and Fractals, New Frontiers in Science. New York: Springer-Verlag, 1992.

RAMADAN, A. & AL-HUSSEINI, M. & KABALN, K. Y. & EL-HAJJ, A. Fractal-Shaped Reconfigurable Antennas. American University of Beirut, Lebanon, 2011.

REDDY, V. V. Broadband Koch Fractal Boundary Printed Slot Antenna for ISM Band Applications. Electronics and Communication Engineering Department, KITS, Warangal, India, 2018.

R. J. CHITRA & V. NAGARAJAN. Design and Development of Koch Fractal Antenna. International Conference on Communication and Signal Processing, 2016.

KATHIRIYA H. J. , DALSANIA P. C. & NEHA S. Analysis of Koch Snowflake Fractal Antenna for Multiband Application. UniversityRajkot, India, 2014.

WAQAS, M., AHMED, Z. & IHSAN, M. B. Multiband Sierpinski Fractal Antenna. National University of Sciences and Technology, 2009.

W. L. STUTZMAN & G. A. THIELE. Antenna Theory and Design, 3ª Ed., 2013.

Y.K. CHOUKIKER & S. K. BEHERA. Wideband Frequency Reconfigurable Koch Snowflake Fractal Antenna. National Institute of Technology, Rourkela, Odisha, India, 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Pós-graduado em Gestão de Sistemas Táticos de Comando e Controle, pela Escola de Comunicações. Mestrando em Engenharia Elétrica pela Universidade de Brasília. Atualmente, exerce a função de instrutor na Escola de comunicações e pode ser contactado pelo email: barros.rafael@eb.mil.br.

ES COM

Endereço

Estrada Parque do Contorno, Rodovia DF - 001, KM 5
Setor Habitacional Taquari - Lago Norte - Brasília - DF
CEP: 71559-902
Telefone: (0xx61) 3415-3532
(PABX) 3415-3502 (Voz/Fax)
Sitio: www.escom.eb.mil.br