

JEAM-V

V JORNADAS DAS ENGENHARIAS DA ACADEMIA MILITAR

INVESTIGAÇÃO, INOVAÇÃO E PRODUÇÃO: PARTINDO DA IDEIA ATÉ AO PRODUTO

LIVRO DE ARTIGOS

Academia Militar

Amadora

5ª EDIÇÃO DAS JORNADAS DAS ENGENHARIAS

DA ACADEMIA MILITAR

Aquartelamento da Academia Militar da Amadora

02 de junho de 2021

Apoio:

GC-Gabinete do Comandante da Academia Militar

DSA - Departamento Serviços Académicos da Academia Militar

CCSI - Centro de Comunicações e Sistemas de Informação da Academia Militar

CINAMIL - Centro de Investigação, Desenvolvimento e Inovação da Academia Militar

Organizado pelo DCEE - AM - IUM

Índice

COMISSÃO EXECUTIVA 5

COMISSÃO CIENTÍFICA 6

EDITORIAL 7

TRABALHOS:

- Estudo do Comportamento Estrutural da Ponte Militar Mabey & Johnson - Soluções para aumentar a capacidade de carga e de vão. 10
  Eduardo Osório, José Pedro, Pedro Matias

- Avaliação de Segurança de Pontes em Betão Armado da Rede Viária Nacional Sujeitas ao Carregamento de Veículos Militares 14
  Eduardo Filipe, António Costa, Pedro Matias

- Reforço de Pontes Modulares do Tipo Bailey com recurso a sistemas de pré-esforço 18
  Tiago Ramos, João Almeida, António André

- Fundações Indiretas de Pontes Modulares – Soluções de execução acelerada 22
  Manuel Passos, Alexandre Pinto, António André

- CryingJackpot: Fluxos de Rede e Indicadores de Desempenho contra o Crypto-jacking 26
  Gilberto Gomes, Luis Dias, Miguel Correia

- Antena Dual-Band para UAV 32
  Ricardo Oliveira, António Baptista, Maria João Martins

- Reconhecimento Facial Através de Aprendizagem Profunda em Imagens Multi-espectrais 37
Luís Chambino, José Silva, Alexandre Bernardino

- Plataforma de gestão de Energia para Edifícios do Exército 43
Jóni Bernardo, Énio Chambel, Carlos Silva

- Conversor Totalmente Integrado em Tecnologia CMOS de 130nm 47
Sérgio Moreira, Pedro Santos, Maria Beatriz Borges

- Comportamento de Fachadas Envidraçadas sob a Ação de Explosões – Desenvolvimento de uma Solução de Proteção 52
Rui Rita, José Pedro, Pedro Matias

- Deteção de Intrusões por Monitorização do Comportamento através de Mudanças de Clusters 57
Tiago Fernandes, Luís Dias, Miguel Correia

- Aplicação da metodologia "Reliability Centered Maintenance 3" ao sistema de Refrigeração do sistema de armas Pandur II 8x8 63
Filipe Silva, Énio Chambel, Virgínia Infante

ÍNDICE DE AUTORES 68

Comissão Executiva:

Élio Teixeira dos Santos (Cor Art), *Coordenador*

Ana Sofia Oliveira Henriques Moita (Doutora)

Énio Rodrigo Pereira Chambel (TCor Mat)

Henrique Martins dos Santos Cunha (TCor Tm)

João Filipe Melro da Conceição (Cap Eng)

Jorge Paulo Alves Torres (Doutor)

José Alberto de Jesus Borges (Doutor)

José Silvestre Serra da Silva (Doutor)

Nuno Miguel Cirne Serrano Mira (TCor Art)

Nuno Miguel Pinto Jordão (TCor Art)

Paula Cristina Pires Simões (Doutora)

Pedro José da Silva Gonçalves Matias (TCor Eng)

Comissão Científica

Ana Luísa Rodrigues Branco Correia

Ana Sofia Oliveira Henriques Moita

António Carlos Rainha Perry da Câmara

António Joaquim dos Santos Romão Serralheiro

Eduardo Manuel Batista Ribeiro Pereira

Helena Isabel Abrantes de Gouveia da Mota Veiga

João Paulo Neto Torres

Jorge Paulo Alves Torres

José Alberto de Jesus Borges

José Silvestre Serra da Silva

Manuel António Coelho do Carmo

Nuno Manuel Mendes Maia

Paula Cristina Pires Simões

Paula Manuela dos Santos Lopes do Rego Figueiredo

Pedro Nuno Mendonça dos Santos

Sandra Cristina Amador Pinelas Ferreira da Silva

Thomas Peter Gasche

Editorial

A quinta edição das Jornadas das Engenharias da Academia Militar, por força das medidas preventivas profiláticas associadas à pandemia causada pelo vírus Covid-19, teve lugar no dia 02Jun21 e centrou-se na temática "Investigação, Inovação e Produção: partindo da ideia até ao produto", transversal a todos os cursos das Engenharias, do Exército e da Guarda Nacional Republicana, ministrados neste estabelecimento de ensino superior público universitário militar.

Seguindo a metodologia adotada em eventos anteriores, que deu provas de sucesso, as Jornadas das Engenharias foram articuladas em duas partes distintas, envolvendo docentes e discentes dos Ciclos de Estudos de Engenharia Militar, Engenharia Eletrotécnica Militar e Engenharia Mecânica Militar.

A primeira parte dedicada a três apresentações subordinadas à Investigação e Desenvolvimento, esteve a cargo de docentes do Departamento de Ciências Exatas e Engenharias e compreendeu os seguintes tópicos:

- Inovação nas áreas da balística e gestão de materiais energéticos - novos conceitos, apresentação de capacidades e ligações à indústria;
- (Micro)sistemas de conversão de energia para aplicações militares;
- Investigação, inovação e desenvolvimento na AM e no Exército.

Na segunda parte, foram apresentados os trabalhos de investigação efetuados pelos alunos finalistas dos cursos das engenharias, do Exército e da GNR, que se enquadram no desenvolvimento e divulgação do conhecimento académico e científico produzido na Academia Militar.

Releva-se neste evento a atividade de investigação, desenvolvimento e inovação da Academia Militar, em linha com a sua agenda da investigação, que decorre da responsabilidade que lhe está cometida de formar alunos que

contribuam para a criação de saber, promovendo a sua participação em projetos de investigação, em colaboração com outras instituições da comunidade científica, nos domínios nacional e internacional, sendo reconhecido o excelente trabalho desenvolvido e os bons resultados atingidos.

É assim justo manifestar o meu apreço a todos os que contribuíram, direta ou indiretamente, para a concretização destas Jornadas, nomeadamente às suas Comissões Executiva e Científica, bem como aos moderadores dos dois paineis e a todos os participantes, que através o debate dos temas propostos muito contribuiram para o resultado atingido.

Para finalizar, deixo uma mensagem final de incentivo aos jovens engenheiros e futuros Oficiais do Quadro Permanente, para que continuem a investigar, a inovar e a desenvolver os seus projetos, dando o seu valioso contributo para a criação de saber, prestigiando a Academia Militar, o Exército e a GNR.

O Comandante da Academia Militar

Luís António Morgado Baptista

Major General

TRABALHOS APRESENTADOS



Os trabalhos publicados são da exclusiva responsabilidade dos seus autores.

Estudo do Comportamento Estrutural da Ponte Militar Mabey&Johnson – Soluções para Aumentar a Capacidade de Carga e Comprimento de Montagem

Eduardo Miguel da Silva Osório
Escola da Guarda
Academia Militar
Vila Real, Portugal
osorio.ems@gnr.pt

José Oliveira Pedro
Dep. Engenharia Civil, Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal
jose.oliveira.pedro@tecnico.ulisboa.pt

Pedro Matias
Centro de Competências para a Proteção de Infraestruturas, Academia Militar
Exército Português
Lisboa, Portugal
matias.pjsg@exercito.pt

Resumo — **As pontes logísticas militares são, desde a década 30 do século XX, indispensáveis em vários teatros de operações possibilitando transpor obstáculos com elevada rapidez, tais como cursos de água. Procurando aumentar o comprimento de vão bem como a capacidade de carga da mais recente ponte logística militar em Portugal, Ponte Mabey, elaboraram-se vários modelos numéricos de elementos finitos, aferidos com outros estudos, os quais pretenderam avaliar a capacidade de carga da ponte para uma configuração de montagem de um tabuleiro contínuo com dois vãos longos de 57.91 m. Tendo em consideração as limitações de capacidade de carga encontradas para a configuração estudada, tanto para tráfego de natureza militar como civil, avaliaram-se várias possíveis soluções de reforço, desde a alteração geométrica da ponte a alterações de secção e adição de novos elementos. Uma vez definida uma solução possível de ser utilizada, realizou-se o estudo da montagem da ponte por lançamento incremental, a partir da solução proposta pelo fornecedor e um lançamento que foi possível acompanhar e estudar, na Companhia de Pontes do Regimento de Engenharia n.º 1, que serviu como referência no estudo do lançamento da ponte.**

I. INTRODUÇÃO

A Ponte Mabey & Johnson é principalmente utilizada pelo Exército Português em operações militares e, quando solicitada ou em casos de emergência, no apoio à população. As múltiplas configurações possíveis associadas à sua velocidade de montagem/desmontagem têm levado a um aumento da sua utilização, quer em cenários de desastres naturais, quer como substituição temporária de pontes. De acordo com o manual técnico do fabricante, a utilização da ponte é restrita às configurações predefinidas, dependendo do vão pretendido e da carga a ser superada. Porém, com os diversos usos da ponte, há interesse em estudar mais detalhadamente o funcionamento e os seus condicionantes, para que novas configurações possam ser definidas para alcançar vãos mais longos e maior capacidade de carga. Para o estudo da Ponte Mabey & Johnson, normalmente chamada de "Mabey", foram utilizados modelos numéricos computacionais, os quais foram desenvolvidos para simular o máximo possível a realidade. A validação do modelo numérico foi feita por meio de testes experimentais. Os principais objetivos deste estudo são avaliar o comportamento estrutural da ponte Mabey, tanto em condições de serviço como para os estados limites últimos, para diferentes cenários. Para o efeito, foi desenvolvido um modelo numérico, devidamente calibrado, com base nas propriedades catalogadas dos componentes da ponte e com base em modelos previamente executados, de forma a desenvolver um modelo consistente para os vários cenários com os quais a ponte irá ser operada.

II. DESCRIÇÃO DA PONTE MABEY

Possui uma conceção baseada na ponte militar Bailey, porém, com altura longitudinal mais reduzida e perfis mais leves, devido à melhoria da qualidade do aço. A sua configuração consiste, basicamente, em 2 planos verticais de treliças ligados por um plano horizontal perpendicular de carlingas. Os planos de treliças podem ser constituídos desde 1 a 3 treliças dispostas em paralelo, denominando-se de configuração simples, dupla e tripla sucessivamente. Tanto nas cordas superiores como inferiores podem ser adicionadas barras suplementares de forma a aumentar a capacidade resistente da ponte (Figura 1).

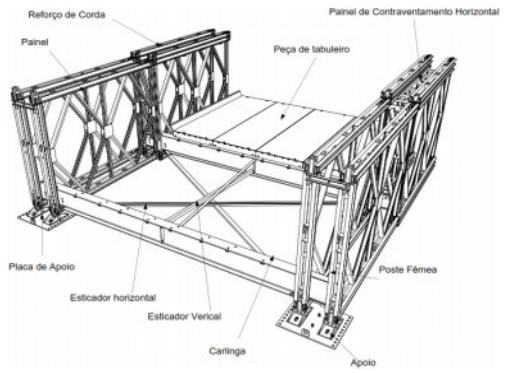


Figura 1. Esquema-Tipo da Ponte Mabey

O seu lançamento pode ser realizado através de 2 formas: recorrendo a uma grua que iça a ponte de forma a colocar na posição final ou através de lançamento incremental, no qual, se lança a ponte de uma das margens, adicionando painéis sucessivamente na retaguarda, até esta chegar à margem oposta.

III. AÇÕES CONSIDERADAS

A. *Sobrecargas Civis*

Tendo em conta a natureza temporária da estrutura e a sua grande flexibilidade, considera-se apenas a ação das sobrecargas de tráfego. No EC1 – Parte 2 (CEN, 2003) definem-se larguras convencionais de via de tráfego correspondentes a 3 m. No caso de faixas de rodagem inferiores a 5.4 metros deve-se adotar-se uma largura de via para "Via 1" de 3 m, sendo o restante considerado como "resto". Neste caso, tendo o tabuleiro uma largura útil de 4.2 m considera-se: 3 m de "Via 1", sujeito ao carregamento uniforme de 9.0 kN/m2 e o restante 1.2 m sujeito a 2.5 kN/m2 (Figura 2).

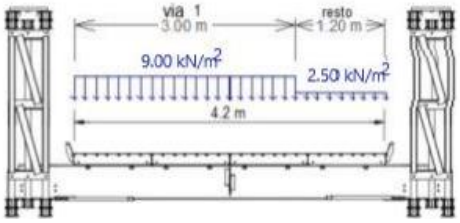


Figura 2. Sobrecarga Civil (Pereira, 2014)

B. *Sobrecargas Miligares*

Relativamente às sobrecargas militares procurou-se utilizar a viatura mais pesada dos Exércitos da NATO. Segundo o STANAG 2021 (2017) a viatura de lagartas com a mais elevada MLC (Military Load Classification) é a Viatura Blindada de Lagartas LEOPARD 2, com aproximadamente 60 toneladas correspondente a uma classificação MLC70 (Figura 3).

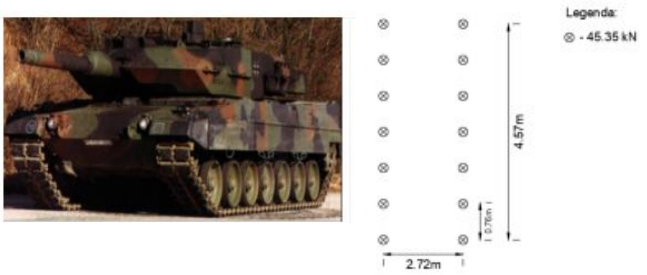


Figura 3. Da esquerda para a direita: Leopard 2 e Modelo de cálculo utilizado

IV. VERIFICAÇÃO ESTRUTURAL DA PONTE EXISTENTE

De forma a ser possível aumentar o comprimento de montagem da ponte Mabey optou-se por utilizar um apoio intermédio de continuidade, conenctando 2 vãos de 57.91 m de comprimento cada. Seguidamente, procedeu-se à verificação da capacidade de carga real desta configuração da ponte.

A. *Sobrecargas Civis*

Verifica-se apenas se for considerada a passagem de viaturas ligeiras simultaneamente, isto é, 2.5 kN/m^2. Caso sejam viaturas isoladas estas não deve ultrapassar as 60 toneladas.

B. *Sobrecargas Militares*

Verifica-se considerando a passagem de uma viatura, isoladamente, com peso não superior a c60 toneladas correspondente a um MLC70.

V. VERIFICAÇÃO ESTRUTURAL COM ALTERAÇÕES À PONTE EXISTENTE

A. *Aumento da Distância entre cordas*

A configuração inicial da ponte Mabey possuía painéis com altura variável. De igual forma, tendo atualmente o painel "standard" uma altura de 2.13 m, respeitando a relação do painel final ser 1.5 vezes maior, criou-se um painel que fez a transição de 2.13 m para 3.2 m (Figura 4).

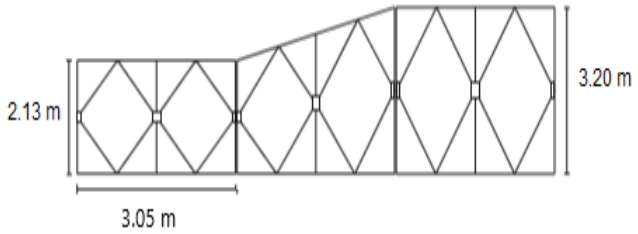


Figura 4 - Configuração adaptada ao modelo em estudo

As verificações de segurança foram realizadas com sucesso para as sobrecargas militares, no entanto, para as sobrecargas civis as diagonais foram ainda mais condicionantes uma vez que o comprimento de encurvadura aumentou nos painéis de maior altura, sem o correspondente aumento da sua secção resistente. Assim sendo, esta solução foi excluída.

B. *Sobreposição de Páineis*

À semelhança de outros tipos de pontes militares, mais especificamente a ponte Bailey, a ponte Mabey permite a montagem com sobreposição de painéis em altura como forma alternativa de aumentar a sua capacidade resistente (Figura 5).



Figura 5- Utilização de painéis sobrepostos no Reino Unido, adaptado de Mabey Bridge 2020

A verificação do ELU de resistência foi assegurado para as sobrecargas militares com bastante margem em todas as secções. No entanto, para as sobrecargas civis que correspondem a um valor bastante superior de sobrecarga no apoio intermédio a segurança das diagonais não é assegurada. De facto, ao se acoplar dois painéis em altura aumenta-se muito a capacidade das cordas, mas não se altera o caminho de carga pelas diagonais comprimidas para o apoio intermédio, mantendo-as condicionantes no dimensionamento. Assim sendo, esta solução foi rejeitada.

C. Alterações das secções das diagonais e cordas

Uma solução alternativa às anteriores corresponde ao reforço dos elementos que constituem os módulos da estrutura, com a adição de chapas de aço soldadas ou aparafusadas aos perfis nas secções condicionantes do dimensionamento (Figura 6).



(a) (b)

Figura 6 - a) Reforço das cordas e b) Reforço das diagonais

Esta solução permitiria verificar a segurança dos elementos tanto para sobrecargas civis e sobrecargas militares, mas mantinha-se a dificuldade de verificação da ligação entre elementos, dado que não era alterada a forma de ligação entre eles. Nomeadamente, seria necessário alterar os parafusos M24 cl. 8.8 para M27 cl. 10.9 na ligação entre as cordas e os reforços das cordas. Todas estas intervenções não constituem uma boa solução, uma vez que configuram uma intervenção profunda nos elementos da estrutura e das ligações, a realizar em oficina para assegurar o necessário controlo de qualidade.

D. Duplicação do Reforço-Corda

Tendo-se testado várias possíveis soluções de reforço, de forma a verificar as sobrecargas tanto civis como militares, chegou-se a uma solução final que consiste em:

- Duplicar os reforços das cordas, tanto na corda superior como na corda inferior (a vermelho na Figura 7);
- Colocar chapas metálicas de 10 mm nas diagonais dos módulos de extremidade e nos cinco módulos para ambos os lados relativamente ao apoio intermédio (a verde na Figura 7);
- As ligações devem ser alteradas de parafusos M24 cl 8.8 para M24 cl 10.9 entre a corda e o reforço da corda (círculos a preto da Figura 7).



Figura 7. Reforços/alterações representadas num painel-tipo

VI. PROCESSO DE MONTAGEM

O processo de montagem das pontes militares é, na maior parte das vezes, realizado através do lançamento incremental (Figura 5), no qual vários painéis vão sendo acoplados e lançados através de apoios rolantes até chegar à margem contrária ao lançamento. Sendo esta fase considerada como uma das fases mais críticas realizaram-se verificações de segurança, no lançamento da solução encontrada, tendo-se aferido que, para verificar a segurança ao ELU, é necessário ter pelo menos dois apoios em cada plano vertical de treliças.



Figura 8. Lançamento incremental da solução no modelo SAP

Outra grande preocupação a ter no processo de montagem por lançamento incremental é verificação de apoios, que leva a que tabuleiro “descole” dos apoios. De facto, este fenómeno pode ocorrer dado que a estrutura se apoia unicamente nos apoios por ação do seu peso, não havendo um mecanismo que a obrigue a estar apoiada nos roletes. Consequentemente, é impossível ocorrer tração nos apoios pelo que na prática tal significa que a ponte estará nesse caso descolada desse mesmo apoio e com um vão livre maior. Contudo, no tipo de análise elástica linear realizada assume-se que o apoio pode ter compressões ou trações. Assim, houve necessidade de aferir de forma iterativa que apoios se encontravam efetivamente à compressão, sendo consequentemente retirados do modelo de análise, tendo-se verificado que para a posição condicionante de lançamento, apenas 3 apoios das 6 iniciais se encontram efetivamente a desempenhar funções estruturais conforme se pode observer na Figura 9.



Figura 9. Apoios à compressão na fase de lançamento mais condicionante

VII. CONCLUSÕES

O estudo realizado conduz às seguintes conclusões:

- A configuração de dois vãos contínuos com 19 módulos (57.91 m cada um) não verifica a segurança regulamentar para as sobrecargas civis, e apenas permite a passagem de uma viatura militar MLC70, caso se utilizem os fatores de majoração conforme a BS 5400-2, utilizada no dimensionamento da estrutura;
- É possível verificar a segurança para o ELU de resistência caso se considerem apenas passagem de viaturas ligeiras e, caso se pretenda o atravessamento pontual de uma viatura de maior tonelagem, esta não deve ultrapassar as 60 toneladas;
- Para o reforço da estrutura, o aumento localizado da distância entre cordas utilizando sobre o apoio intermédio módulos de 1.5 x altura dos módulos correntes não é uma solução aconselhável, uma vez que não resolve a falta de capacidade de carga das diagonais comprimidas próximas do apoio intermédio, que se mantêm condicionantes na verificação de segurança;
- A sobreposição de painéis, ainda que tenha conduzido a um aumento da resistência bastante considerável das cordas, continua a ter as diagonais comprimidas que encaminham as cargas para o apoio intermédio como condicionantes no dimensionamento;
- A alteração das secções transversais dos módulos das treliças, através da adição de chapas de aço verifica a segurança das secções, no entanto, as ligações entre módulos teriam de ser também reforçadas, o que consiste no conjunto a uma intervenção profunda na estrutura existente;
- A melhor solução de reforço para assegurar o ELU de resistência para a passagem das sobrecargas civis e militares consiste na duplicação do reforço corda, e a adição de chapas de aço de 10 mm nas diagonais de 12 dos 38 módulos e o aumento da classe dos parafusos de ligação das cordas aos reforços-cordas para M24 cl. 10.9;
- Ao longo do processo de montagem da estrutura, na posição mais condicionante de lançamento, há três apoios intermédios à tração que não desempenham qualquer função estrutural não devendo ser considerados efetivos;
- Apesar de no catálogo ser utilizado apenas um apoio por cada plano triplo de treliças, a verificação da segurança para o ELS caraterístico requer a utilização de dois apoios e para assegurar o ELU de resistência regulamentar são necessários três apoios em paralelo.

AGRADECIMENTOS

Esta dissertação não teria sido possível sem a ajuda direta das seguintes pessoas e entidades:

- Professor Doutor José Oliveira Pedro, orientador da tese, pela disponibilidade e entusiasmo que demonstrou durante toda a tese;

- Tenente-Coronel Pedro Matias, coorientador da tese, pela disponibilidade, preocupação e sugestões que foram muito importantes para tese;

- Companhia de Pontes do Regimento de Engenharia n.º 1 de Tancos pela abertura que tiveram para poder participar euma montagem da ponte Mabey;

- À minha família e namorada pelo apoio durante a realização da tese e também em todo o meu percurso académico.

REFERÊNCIAS BIBLIOGRÁFICA

[1] BSI. (2000). Steel, concrete and composite bridges - Part 2: Specification for loads. doi:ISBN 0 580 09939 3.

[2] CEN. (2005). Eurocódigo 1 - Ações em estruturas; Parte 2: Ações de tráfego em pontes.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] CEN. (2010). Eurocódigo 3 - Projeto de Estruturas de Aço. Portugal.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] Diário da República. (30 de julho de 1983). REBAP . 7.º Suplemento. Obtido de https://dre.pt/application/conteudo/435595

[5] North Atlantic Treaty Organization. (setembro de 2017). NATO Standard. Military Load Classification of Bridges, Ferries, Rafts and Vehicles(1).

[6] Pereira, R. M. (2015). Comportamento Estrutural de Pontes Logísticas do tipo Mabey do Exército Português. Instituto Superior Técnico, Universidade de Lisboa.

Avaliação de Segurança de Pontes em Betão da Rede Viária Nacional Sujeitas ao Carregamento de Veículos Militares

Eduardo Miguel Antunes Filipe
Academia Militar
Exército Português
Lisboa, Portugal

António José da Silva Costa
Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal

Pedro José da Silva G. Matias
Academia Militar
Exército Português
Lisboa, Portugal

Resumo — **As atividades militares realizadas por parte do Exército Português exigem, frequentemente, a utilização de estruturas existentes na rede viária nacional, designadamente pontes e viadutos, para satisfazer as necessidades de deslocação das viaturas militares. Estas estruturas encontram-se dimensionadas de acordo com a regulamentação de ações associada à época na qual se realizou o respetivo projeto, pelo que importa avaliar se as normas regulamentares utilizadas no dimensionamento garantem a segurança da estrutura para uma utilização militar.**

Para tal, estudaram-se os diferentes regulamentos de ações utilizados nas últimas décadas, designadamente as sobrecargas rodoviárias correspondentes, por forma a compreender a evolução das ações consideradas no projeto e dimensionamento de estruturas de pontes. Deste modo, pretende-se obter a relação existente entre as sobrecargas regulamentares e a sobrecarga militar relativa a uma utilização mista, nomeadamente de tráfego normal e circulação de viaturas militares.

No que diz respeito ao carregamento militar considerou-se a atuação de uma viatura de lagartas e de rodas, cuja classificação de carga militar corresponde à regulamentação aprovada pela NATO e prevista nas normas STANAG. Realizou-se a verificação de segurança da estrutura do tabuleiro de três obras inseridas na autoestrada A1, com soluções estruturais diferentes e projetadas de acordo com regulamentos de ações distintos.

I. INTRODUÇÃO

A regulamentação NATO relativa ao sistema MLC considera 32 veículos hipotéticos, sendo estes igualmente repartidos entre viaturas de rodas e de lagartas, nos quais se salienta as diversas configurações dos primeiros relativamente ao número de rodas e respetivos eixos. Deste modo, os veículos militares encontram-se caraterizados por 32 classes, designadamente entre a MLC 4 e MLC 150. Relativamente à classificação de pontes, são definidas caraterísticas adicionais como a altura do centro de gravidade, área do vento lateral e altura do centro de pressão. Salienta-se o facto de a classificação atribuída pelo sistema MLC ser apenas uma forma de classificação associada a veículos militares, não correspondendo este valor à massa dos mesmos no que diz respeito a veículos de rodas, pois nesta situação são considerados aspetos como a carga máxima por eixo, largura de contato do pneu e espaçamento entre eixos. [1]

II. ANÁLISE GLOBAL – ABORDAGEM PRELIMINAR

Por forma a ter em consideração a evolução da regulamentação relativa às sobrecargas rodoviárias, realizou-se uma análise simplificada dos efeitos produzidos pelas diferentes ações associadas aos regulamentos utilizados em projetos de estruturas de pontes ao longo das últimas décadas. Uma vez que os vários regulamentos consideram diferentes sobrecargas rodoviárias, a análise comparativa realiza-se para uma determinada largura da faixa de rodagem.

Assim, considera-se uma faixa de rodagem composta por duas vias de 3,5 metros e duas bermas de 1,0 metros, traduzindo-se numa largura total correspondente a 9,0 metros. A comparação será realizada em termos de esforço global atuante em tramos de tabuleiro com diferentes vãos, sendo que o esforço global considerado diz respeito ao momento fletor total. Esta abordagem simples permite, numa primeira análise, verificar se existem deficiências em termos da resistência do tabuleiro de obras dimensionadas de acordo com os diferentes regulamentos, tratando-se assim dos designados efeitos gerais das sobrecargas.

Nesta análise não se encontram considerados os efeitos locais em que a sobrecarga condicionante corresponde ao efeito do veículo tipo. Relativamente à circulação de viaturas militares, considera-se o carregamento associado a veículos de lagartas da classe 70 (63,5 t) e veículos de rodas da classe 100 (104,3 t), de acordo com a classificação de carga militar prevista na regulamentação NATO.

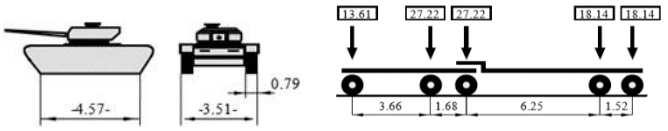


Figura 1. Caraterísticas dos veículos tipo de lagartas e de rodas [STANAG]

Define-se uma via reservada para circulação exclusiva de viaturas militares, sendo que as restantes vias se encontram sujeitas ao carregamento dos veículos tipo previstos no Eurocódigo 1, nomeadamente o veículo tipo 2 e o veículo tipo 3, bem como a atuação da respetiva sobrecarga uniforme. A situação de carga em questão encontra-se definida no quadro abaixo:

TABELA 1. SITUAÇÃO DE CARGA PARA A CIRCULAÇÃO DE UMA COLUNA MILITAR COM VIA RESERVADA

	Carga por eixo [KN]	Sobrecarga uniforme [KN/m^2]
Via 1 (tráfego militar)	Fig. 1	0
Via 2 (tráfego normal)	200	2,5
Via 3 (tráfego normal)	100	2,5

Admitindo que uma situação corrente de circulação militar apresenta condições de travessia normais, o índice de fiabilidade β associado a este cenário corresponde a 3,3, tal como previsto pelo STANAG. Deste modo, obtém-se um coeficiente parcial γ_Q de valor 1,35.

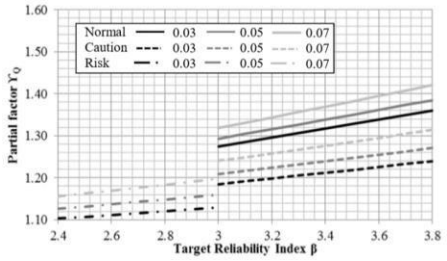


Figura 2. Coeficiente de segurança para ações variáveis segundo diferentes condições de travessia e uma incerteza do modelo entre 3% e 7%

Afetando a sobrecarga militar e as sobrecargas regulamentares dos coeficientes de segurança correspondentes a 1,35 e 1,5 respetivamente, obtém-se o momento fletor total associado aos carregamentos.

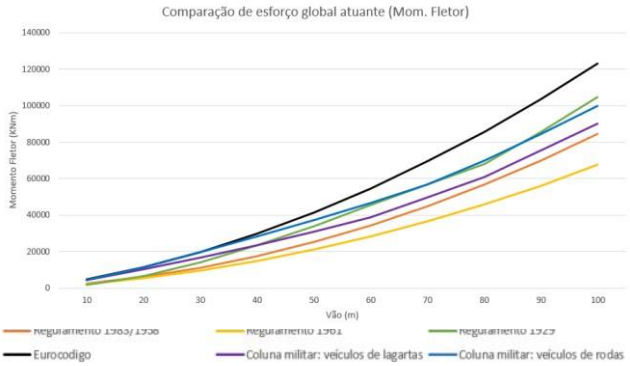


Figura 3. Comparação de esforço global atuante afetado de coeficiente de segurança segundo vários regulamentos

III. ESTUDOS DE CASO – VERIFICAÇÃO DA SEGURANÇA DO TABULEIRO

Neste capítulo efetua-se a verificação da segurança do tabuleiro de três obras com soluções estruturais diferentes, projetadas de acordo com a regulamentação antiga.

A. Viaduto de Alhandra

De acordo com a regulamentação aprovada pela NATO, os coeficientes parciais relativamente a verificações de segurança que envolvam a circulação de veículos militares correspondem a 1,2 e 1,35 para ações permanentes e variáveis, respetivamente.

TABELA 2. ESFORÇOS ATUANTES MÁXIMOS NAS VIGAS LONGITUDINAIS PARA A COMBINAÇÃO FUNDAMENTAL DE AÇÕES

	Carregamento militar			
	Momento fletor [KNm]		Esforço transverso [KN]	
	$M_{Sd,\ 1/2\ vão}$	$M_{Sd,\ 1/4\ vão}$	$V_{Sd,\ apoio}$	$V_{Sd,\ 1/4\ vão}$
V1-8	1398,6	1045,2	346,3	211,8
V9	904,4	677,6	209,9	118,7

Deste modo, encontram-se na tabela seguinte os valores dos momentos resistentes relativos às seções de controlo do tabuleiro, sendo que na análise considerou-se apenas a atuação do pré-esforço interior, tendo sido desprezado o efeito do pré-esforço relativo à intervenção de reforço na estrutura.

TABELA 3. MOMENTO RESISTENTE NAS SECÇÕES DE CONTROLO DAS VIGAS LONGITUDINAIS

	Momento resistente [KNm]	
	$M_{Rd,\ 1/2\ vão}$	$M_{Rd,\ 1/4\ vão}$
V1-8	1219	1060
V9	1340	1135

$$M_{PE} = P_{útil} \times e = 500 \times 0{,}72 = 360\ KNm$$
$$=> M_{Rd,total} = 1219 + 360 = 1579\ KNm \quad (1)$$

Constata-se que a verificação da segurança é satisfeita se for considerado o acréscimo de resistência associado ao efeito do pré-esforço exterior.

B. Viaduto sobre o rio Trancão

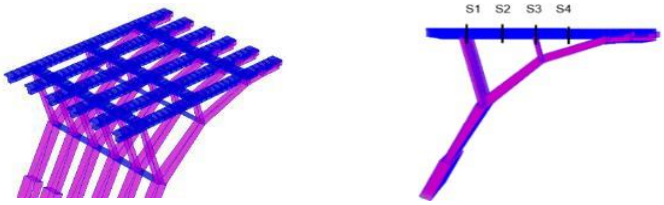


Figura 4. Vista 3D das secções de controlo: apoio das vigas na ligação aos montantes e secções de meio vão correspondente

TABELA 4. DISPOSIÇÃO TRANSVERSAL DA SOBRECARGA RELATIVA AO CARREGAMENTO MILITAR

	Faixa de rodagem 1			Faixa de rodagem 2		
Nº via	**1**	**2**	**3**	**1**	**2**	**3**
VT (carga total) [KN]	635	400	200	400	200	0
SCU [KNm]	0	2,5	2,5	2,5	2,5	2,5

A verificação de segurança foi realizada tendo em consideração as combinações de ações associadas aos diferentes carregamentos e envolvendo as cargas permanentes e as várias sobrecargas.

TABELA 5. ESFORÇO DE FLEXÃO ATUANTE MÁXIMO NAS VIGAS LONGITUDINAIS PARA A COMBINAÇÃO FUNDAMENTAL DE AÇÕES

		Vigas – Momento fletor [KNm]			
Secções de controlo		**1**	**2**	**3**	**4**
Regulamento 1929	**UDL**	-896,8	1610,4	-1087,4	2080,4
	TS	-561,0	1201,2	-779,6	1322,6
Regulamento 1958	**UDL**	-715,4	1516,9	-910,9	1791,6
	TS	-674,9	1771,5	-887,0	1777,5
Sobrecarga militar		-731,3	1943,5	-939,8	2091,5

TABELA 6. CAPACIDADE RESISTENTE À FLEXÃO DOS ELEMENTOS ESTRUTURAIS LINEARES NAS SECÇÕES DE APOIO E A MEIO VÃO

	Momento resistente [KNm]
Secção 1	-2118
Secção 2	2503
Secção 3	-2766
Secção 4	2184

Verifica-se que os elementos analisados verificam a segurança relativamente a esforços de flexão.

C. Viaduto sobre o rio de Mouros

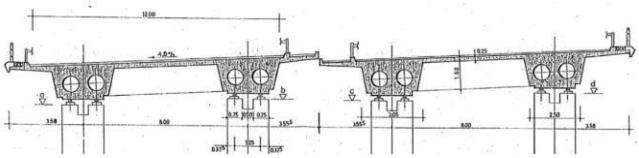


Figura 5. Desenho de projeto da estrutura do tabuleiro em laje nervurada(corte transversal)

TABELA 7. ESFORÇOS DE FLEXÃO NO APOIO E A MEIO VÃO DO TRAMO CENTRAL DO TABULEIRO

		Momento fletor [KNm]		
		1983 (VT)	***1983 (SCU+SCL*)***	***SC militar***
Combinação caraterística	**½ vão**	11692,6	13780,4	19353,2
	Apoio	-13019,1	-16232	-17243,6
Combinação fundamental	**½ vão**	15311,5	18443,1	24241,5
	Apoio	-18395,3	-23214,6	-21803,5

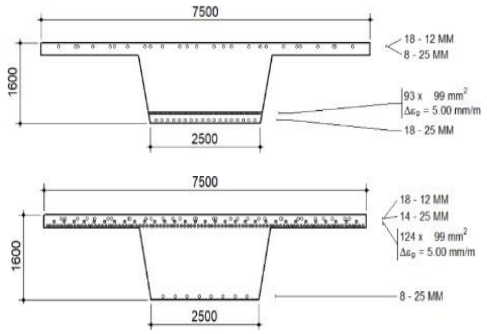


Figura 6. Modelação das secções de ½ vão (cima) e de apoio (baixo)

Deste modo, resultam os seguintes valores relativamente aomomento fletor resistente:

- Secção a meio vão: M_{Rd} = 22772 KNm;
- Secção do apoio: M_{Rd} = -25648 KNm.

Verifica-se que na secção do apoio o momento resistente é superior ao momento atuante e na secção a meio vão o esforçode flexão atuante é superior à respetiva capacidade resistente, pelo que se conclui que a estrutura do tabuleiro não verifica a segurança relativamente ao Estado Limite Último de Flexão.

IV. CONCLUSÕES

Considerando a análise global realizada e tendo por base os resultados obtidos na avaliação de segurança dos casos de estudo abordados, verifica-se que as pontes cujo projeto diz respeito à regulamentação antiga, nomeadamente o Regulamento de Pontes Metálicas (1929), apresentam uma menor tendência paraoriginar problemas de segurança estrutural quando sujeitas a carregamentos militares. Por outro lado, devido à adoção de sobrecargas menos desfavoráveis comparativamente com a regulamentação anterior, as estruturas dimensionadas segundo os regulamentos de ações mais recentes, como o Regulamento de Segurança e Ações (1983), apresentam uma maior tendência para originar problemas de segurança face a uma utilização militar.

No que diz respeito a obras com um comprimento de vão pequeno a intermédio, até cerca de 30 a 40 metros, conclui-se que as várias sobrecargas regulamentares conduzem a esforços relativamente semelhantes, sendo que o carregamento militar induz esforços na estrutura superiores aos anteriores. Para vãos superiores a 40 metros, a sobrecarga associada à circulação dos veículos militares de lagartas e de rodas considerados, nomeadamente da classe 70 e da classe 100, conduz a esforços ligeiramente superiores comparativamente com as sobrecargas rodoviárias dos Regulamentos de 1983 e 1929, respetivamente. Como tal, nas situações para as quais seja previsível que, através de informações relacionadas com a classe dos veículos militares em causa e as caraterísticas da ponte que os mesmos pretendem atravessar, os esforços atuantes relativos ao carregamento militar sejam idênticos ou superiores aos das sobrecargas utilizadas no dimensionamento da estrutura, o tráfego militar deve ser condicionado ou reservado, por forma a evitar o risco de colapso da estrutura ou a ocorrência de danos permanentes na mesma.

Nestas situações, a circulação de viaturas militares deve realizar-se a uma velocidade moderada, no centro da faixa de rodagem, devendo encontrar-se apenas um veículo em cada vão estruturalmente independente, sendo que o restante tráfego rodoviário deve ser temporariamente condicionado.

AGRADECIMENTOS

Agradeço ao Professor Doutor António José da Silva Costa, meu orientador, pela constante disponibilidade e apoio demonstrado ao longo da realização do presente trabalho, assim como pela revisão científica e bibliográfica, na qual o acompanhamento e o conhecimento técnico e científico por parte do docente foram essenciais, tanto na realização do trabalho como no período letivo antecessor. Agradeço igualmente ao Tenente-Coronel Pedro Matias, coorientador deste trabalho de investigação, por toda a ajuda e disponibilidade prestada durante o período correspondente à respetiva elaboração, cuja motivação demonstrada e auxílio na correção erevisão científica, assim como na relação fundamental com a componente militar associada a este trabalho, foram cruciais para o sucesso no cumprimento dos objetivos a que inicialmenteme propus.

Um agradecimento especial à minha família, que me acompanha desde sempre em todas as etapas importantes da minha vida, cuja presença, compreensão e motivação são sempre aspetos fundamentais para o sucesso nos momentos mais difíceis e desafiantes.

Por último, um agradecimento muito especial à minha namorada, companhia de todos os momentos e fonte de força e inspiração, pela total e permanente ajuda e preocupação, pela presença, amizade e amor.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] NATO Standard (2017) AEP-3.12.1.5, Military Load Classification of Bridges, Ferries, Rafts and Vehicles, Edition A, Version 1



E. A. Filipe nasceu a 31 de janeiro de 1996, em Castelo Branco, Portugal. Em 2014, concluiu o Ensino Secundário no Liceu Nuno Álvares e ingressou na Academia Militar, onde se encontra atualmente a terminar o Mestrado Integrado em Engenharia Militar, especialidade de Engenharia Civil - Estruturas.

Reforço de Pontes Modulares do Tipo Bailey com Recurso a Sistemas de Pré-Esforço

Tiago Vieira Ramos
Instituto Superior Técnico
Academia Militar
Lisboa, Portugal
ramos.tv@exército.pt

Prof. João C. de O. F. de Almeida
Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal
jalmeida@civil.ist.utl.pt

Prof. António. C. G. M. André
Berd S.A.
Faro, Portugal
Antonio.andre@protecna.pt

Resumo — **No presente artigo apresenta-se uma possível solução recorrendo a pré-esforço exterior da ponte militar Mabey Compact 200, na sua configuração DSHR2H ++, sujeita a uma sobrecarga militar significativamente mais elevada do que aquela que está documentada, potenciando assim a sua utilização por veículos de classe de carga militar (MLC) superior.**

A análise desta solução foi efetuada com recurso ao software ROBOT, no qual foi modelada a ponte, as cargas e o próprio sistema de pré-esforço. As verificações foram efetuadas também no software depois de tudo estar modelado, visto o programa conseguir fazer essa avaliação sem se proceder a cálculos manuais.

A solução a que se chegou apenas garante uma análise ao ELU da Ponte Mabey, não contemplando verificação em serviço. O principal objetivo deste reforço era tentar instalar o sistema de pré-esforço exterior depois da ponte já estar montada, tentando não alterar qualquer elemento da superestrutura. No entanto verificou-se que haveria um perfil nas extremidades que não iria verificar a segurança para a posição na qual a viatura se encontra a meio vão. No mesmo sentido, analisou-se a posição mais desfavorável para o esforço transverso e também as diagonais não verificaram a segurança, tendo-se reforçado os respetivos perfis. Assim, recorrendo às ancoragens e selas de desvio modeladas no software ROBOT, e à troca dos perfis que não verificaram a segurança, conseguiu-se uma solução de pré-esforço que garante o aumento da capacidade de carga de veículos, para um mesmo vão.

Palavras-chave: Ponte Militares, Reforço Estrutural, Pré-Esforço Exterior.

I. INTRODUÇÃO

As pontes modulares são, nos dias de hoje, soluções viáveis para vencer diversos tipos de obstáculos naturais e/ou artificiais que existam num determinado terreno. O seu fácil transporte, rápido processo de montagem/desmontagem, a sua capacidade de carga e comprimento de vão que atingem, são algumas das caraterísticas que tornam este tipo de pontes muito eficazes em cenários de catástrofes naturais e conflitos armados. Por forma a prestar um apoio incontestável à população e à Proteção Civil em cenários de catástrofes naturais, mas também para solidificar a manobra de Forças Militares, o Exército Português adquiriu o modelo mais recente de pontes modulares da empresa Mabey & Johnson, o modelo Mabey Compact 200. A sua utilização tem sido efetuada com base nos manuais fornecidos pelos fabricantes, nos quais existem várias formas de utilização e montagem da Ponte, dependendo do vão a vencer e da capacidade de carga que se pretende atingir. O interesse em estudar esta Ponte Modular em particular, prende-se com o facto de haver uma necessidade recorrente de aumentar a capacidade de carga de uma forma eficiente, sem comprometer a sua estabilidade e o tempo de vida dos vários elementos que constituem a ponte. Deste modo, vai ser utilizada uma das invenções que mais revolucionou a Engenharia Civil, o Pré-Esforço.

II. PONTES LOGÍSTICAS

Em todas as operações militares, a disciplina, rapidez e organização da manobra das forças é um elemento fulcral, que pode distinguir uma operação bem-sucedida de um completo desastre. Assim, os Exércitos adquirem equipamentos, como pontes de assalto e logísticas, que permitem manter o seu ímpeto, rapidez do movimento e a organização da coluna militar, de modo a conseguir cumprir as missões impostas pelos escalões superiores.

Posto isto, chega-se à conclusão de que as duas grandes Guerras foram os principais motores para a evolução do conhecimento e do fabrico de pontes logísticas, principalmente porque em tempo de Guerra é grande o investimento em equipamento e tecnologias que permitam obter vantagem em relação aos adversários. Na Primeira Guerra Mundial, com o surgimento dos carros de combate de grande envergadura, foi necessário desenvolver pontes que conseguissem suster elevadas cargas nas suas vias, e por isso as pontes que surgiram eram estruturas robustas e pesadas. Com o avanço tecnológico durante o séc. XX e XXI, as pontes tornaram-se cada vez mais leves, rápidas de montar, resistentes e eficientes, sendo nos dias de hoje, soluções viáveis para emergências (Fig. 1).



Fig. 1 – Ponte montada na 2ª Guerra Mundial na Alemanha (esquerda), e Ponte Mabey Compact 200 montada no Reino Unido (direita) [1].

III. REFORÇO DE PONTES MODULARES

Atualmente na Engenharia de pontes, a busca incessante por soluções mais eficientes de reforço de pontes, trouxe uma panóplia de opções cada uma com particularidades diferentes, que nos fazem chegar a uma solução mais viável do que as outras. Ao pensar no assunto, pudemos facilmente concluir que a substituição de certas peças nas pontes por outras mais robustas, é uma solução simples e muitas vezes eficaz, mas existem outras, tais como a adição de novos elementos, adição de área de aço e os sistemas de pré-esforço exterior (Fig. 2).

Desde a sua invenção, o pré-esforço exterior tem vindo a ser desenvolvido e a ganhar cada vez mais importância no plano atual do mundo da construção, principalmente devido à possibilidade de permitir o reforço de estruturas que estão sujeitas a novas solicitações, que se traduzem muitas vezes em incrementos de carga.

A grande particularidade do pré-esforço exterior é o facto de se diferenciar do pré-esforço interno na disposição dos cabos, ou seja, no pré-esforço exterior é maioritariamente utilizado cabos em traçados retos, ao contrário do pré-esforço interno que normalmente, e de modo a ser mais eficaz, tem um traçado parabólico.

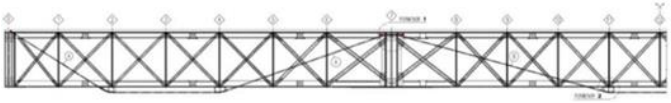


Fig. 2 – Exemplo de aplicação de pré-esforço exterior [2].

Como nenhum sistema é perfeito, o pré-esforço exterior apresenta inúmeras vantagens e desvantagens. As vantagens desta técnica são [3] [4]:

- o Reduzido incremento do peso próprio do elemento reforçado;
- o Intervenção pouco intrusiva e reversível;
- o Possibilidade de monitorização;
- o Facilidade de correção e substituição do pré-esforço;
- o Aumenta a capacidade de resistência aos momentos fletores.

Não obstante, esta técnica ostenta também alguns inconvenientes, tais como [3] [4]:

- o Grande probabilidade de surgir problemas derivados com a deterioração dos elementos em aço face à sua exposição aos agentes atmosféricos;
- o Embora o pré-esforço exterior seja eficaz no aumento da resistência da estrutura à flexão, não confere um reforço ao corte, razão pelo qual é aconselhável uma verificação de segurança ao esforço transverso;
- o Outra das fragilidades é que para ser feita a tensão dos cabos de pré-esforço, torna-se essencial a existência de espaço na zona das ancoragens ativas.

IV. AVALIAÇÃO DO COMPORTAMENTO ESTRUTURAL DA PONTE MABEY COMPACT 200

Para fazer o estudo da ponte, utilizou-se uma situação hipotética na qual se pretende avaliar recorrendo a um sistema de pré-esforço exterior, a viabilidade da ponte instalada em Mafra (vão 45,72m) suportar veículos MLC 100 W, permitindo assim criar uma travessia (não existente nas proximidades) com a capacidade de carga pretendida sobre o Rio Lizandro (Fig. 3). O modelo foi concebido no software ROBOT (Fig. 4 e 5) utilizando a mesma configuração que foi utilizada quando a ponte foi instalada em Mafra, e é objetivo do artigo conceber um sistema de pré-esforço que conseguisse garantir a passagem da viatura de classificação MLC 100 W pela ponte Mabey na configuração DSHR2H ++ [5].

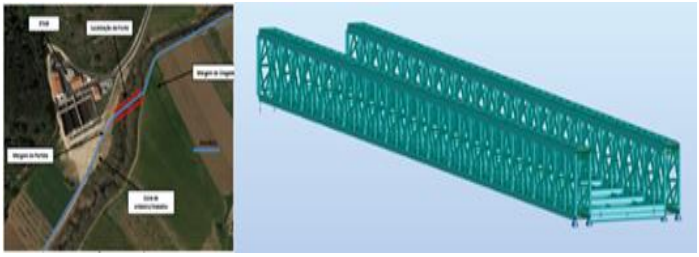


Fig. 3 – Esquema de localização da ponte vista aérea (esquerda), e modelo ROBOT da ponte.

Foi feita uma verificação automática dos perfis da ponte com base no software ROBOT, e verificou-se que muitos perfis não verificavam a segurança. Assim, foi estudada uma solução de pré esforço exterior que conseguisse resistir aos momentos fletores e esforço transverso exercida pela passagem de uma viatura de classificação militar MLC 100 W. Após ser dimensionada e refinada, foram desenvolvidos os elementos de interação, as ancoragens e as selas de desvio, mudaram-se os perfis das diagonais e dos postes macho e fêmea (não verificavam a segurança), e chegou-se a uma solução equilibrada com 2 cabos de 4 cordões de 0,6''N em cada lado da ponte, que cumpria as condições de segurança existentes nos regulamentos. Os valores de "0.00" que aparecem na Figura 6, são referentes a perfis longitudinais que foram adicionados para simular as ligações cavilhadas da ponte, e por isso não apresentam esforços.

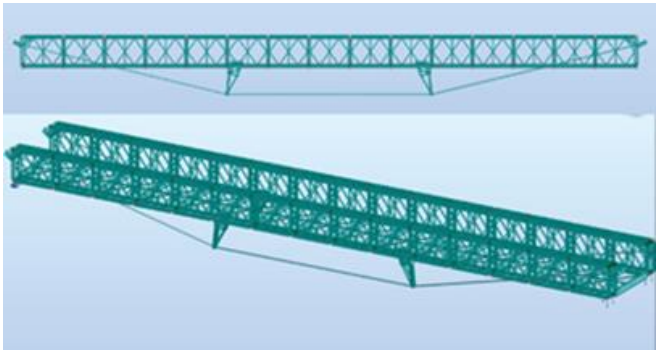


Fig. 4 – Ponte Mabey Compact 200 com sistema de pré-esforço exterior modelada em software ROBOT.

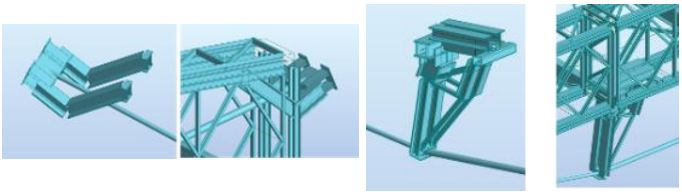


Fig. 5 – Pormenor dos elementos de interação modelado em software ROBOT (Ancoragens e Escoras, respetivamente).

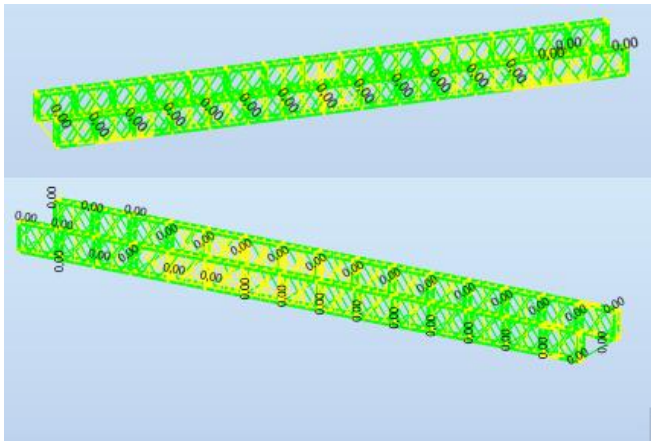


Fig. 6 – Verificação de perfis no sotware da Ponte Mabey Compact 200.

V. CONCLUSÕES

O problema prático apresentado tem por base uma situação real, na qual a ponte Mabey Compact 200 com a configuração DSHR2H++ foi utilizada, mostrando a utilidade que estes tipos de pontes militares podem ter na resolução de problemas em que são necessárias respostas eficientes. No caso em questão, a instalação e desmontagem da ponte apresentou custos na ordem dos 15 000 €, e a manutenção, inspeção e aluguer cerca de 2000 €, ficando notório que os custos associados a uma operação deste tipo são relativamente baixos comparando com os benefícios que a ponte traz ao serviço da população. Durante o tempo em que a ponte esteve montada, decorreram trabalhos de limpeza do itinerário cortado, bem como o reforço das encostas com redes metálicas de alta resistência, de modo a garantir que a estrada mantivesse o seu fluxo normal com a devida segurança.

O objetivo era por isso avaliar um sistema de pré-esforço exterior que garantisse a passagem de um único veículo de classificação MLC 100 W pela ponte. Hipoteticamente, era de extrema importância que essa viatura conseguisse fazer a travessia do Rio Lizandro, não havendo mais opções para a sua passagem. É importante referir que a passagem da viatura com o sistema de pré-esforço exterior e o reforço dos postes macho e fêmea e diagonais foi garantida pela verificação de segurança feita na análise com o software ROBOT, mas o comportamento em serviço não foi avaliado, o que não garante a posteridade desta solução em relação à fadiga e deformação a longo prazo.

Como se pode perceber, era esperado que os perfis aos quais o pré-esforço fosse ligado cedessem, tal como aconteceu no caso dos postes macho e fêmea de cada extremidade visto que as forças inerentes à aplicação do sistema de pré-esforço exterior são altíssimas e estes perfis não foram dimensionadas para aguentar esforços de tal ordem. Pela mesma ordem de ideias, as diagonais cederam, visto não terem sido dimensionadas para cargas de tal forma altas como são as de um MLC 100 W.

Numa forma geral, a implementação deste tipo de reforço nas pontes militares Mabey, poderá ser garantida estudando de uma forma intensiva a forma como é feita a sua montagem, mas é muito difícil de garantir em casos em que a ponte já está montada, tal como é o caso que se apresenta. A troca dos postes macho e fêmea, a troca das diagonais e a acoplamento dos elementos de interação deveria ser feita durante a montagem da ponte, precedida da preparação dos perfis a ser colocados e dos furos para os parafusos que garantem a ligação tanto nos postes em cada extremidade como na corda inferior, ancoragens e selas de desvio.

AGRADECIMENTOS

O presente artigo foi fruto do trabalho e dedicação de muitas pessoas que estiveram a meu lado durante este período, e que por isso merecem o meu agradecimento.

Em primeiro lugar, gostaria de agradecer ao Professor Doutor João Carlos De Oliveira Fernandes de Almeida e ao Professor Doutor António Carlos Guerreiro Morgado André, pela ajuda durante a elaboração do artigo, pois sem o seu empenho, dedicação e parecer em questões técnicas, não teria sido possível resolver os problemas que foram surgindo e que culminaram neste trabalho.

Agradeço também à empresa da BERD, e principalmente ao elemento com quem estive mais em contacto, a Engenheira Inês Ferraz, que muito ajudou durante a modelação da ponte, sempre interessada em ajudar e a dar sempre "inputs" para que tudo corresse da melhor forma.

Não poderia deixar de agradecer também ao meu diretor de curso, Tenente Coronel de Engenharia Matias, pela sua constante preocupação mesmo não fazendo parte da orientação do meu artigo.

Ao Capitão de Engenharia Nuno Alves e ao Tenente de Engenharia Roberto Ladeiras, agradeço a disponibilização de documentos e fotografias da instalação da Ponte Mabey em Mafra, que muito ajudaram para fundamentar o problema prático desenvolvido durante estes meses.

Também tenho de agradecer aos meus camaradas de curso e da Academia Militar que são das pessoas mais importantes que ive até hoje, todos eles foram-se tornando família nesta caminhada de 7 anos que está prestes a concluir. Foram eles que me acompanharam diariamente na minha formação, ajudaram nos momentos difíceis, mas também partilharam comigo momentos dos quais nunca me vou esquecer. Desejo as maiores felicidades e sorte para todos nesta longa caminhada que ainda

está por ser percorrida, pois o final de um capítulo coincide sempre com o início de um novo!

Quero agradecer à minha família e amigos, que representam tudo o que eu sou hoje. São a constante da minha vida, que me ajudaram sempre nas dificuldades que foram surgindo.

Por último, agradeço aos meus avôs, que embora não estejam fisicamente presentes, estiveram e estarão sempre no meu pensamento, garantindo que tenho forças para continuar o meu caminho.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] André, A. C. (2016). Estudo da Aplicação de Pré-Esforço Orgânico em Pontes Provisórias. Porto

[2] Gomes, N. A. (2017). Estudo para Reabilitação e Reforço da estrutura metálica da Ponte sobre a Ribeira de Corges ao PK168+612 da linha de caminho-de-ferro da Beira Baixa. Universidade da Beira Interior, Covilhã.

[3] Neves, S. P. (2012). Pré-Esforço Exterior no Reforço de Estruturas. Lisboa.

[4] Preto, P. D. (2014). Aplicação de Pré-Esforço Exterior como Técnica de Reforço de Estruturas de Betão. Lisboa.

[5] Mabey Bridge. (2014). Logistic Support Bridge - General Manual prepared for the portuguese army - Logistic command material and transportation directorate. Chepstow: Mabey Bridge Limited.

[6] Ladeiras, R. (2017). Ponte Militar Mabey & Johnson - Avaliação da Capacidade para cenários de Acidente. Lisboa.

[7] Pereira, R. M. (2015). Comportamento Estrutural de Pontes Logísticas do tipo Mabey do Exército Português.

[8] NATO. (2006). STANAG 2021. NATO.

Fundações Indiretas de Pontes Modulares – Soluções de Execução Acelerada

Manuel António Correia de Melo Ferreira Passos
Instituto Superior Técnico – Universidade de Lisboa
Academia Militar
Lisboa, Portugal
passos.macmf@exercito.pt

Alexandre da Luz Pinto
Instituto Superior Técnico
Universidade de Lisboa
Departamento de Engenharia Civil, Arquitetura e Georrecursos.
alexandrepinto@tecnico.ulisboa.pt

António Carlos Guerreiro Morgado André
BERD Estruturas
Porto, Portugal
antonio.andre@protecna.pt

Resumo — **O presente artigo pretende-se estudar uma solução de fundação indireta para pontes modulares capaz de satisfazer as exigências dos regulamentos em vigor, nomeadamente os Eurocódigos. Será necessário abordar o campo das pontes modulares e propor uma solução de fundação compatível com as exigências das pontes militares.**

I. INTRODUÇÃO

As pontes modulares são soluções eficientes para unir dois pontos que estão separados por um obstáculo. A montagem das pontes modulares é do "tipo lego", não necessitando de mão-de-obra especializada, e permite configurar a ponte para um determinado vão ou uma determinada carga. Geralmente, estruturas como pontes modulares, são apenas suportadas por encontros superficiais, sempre que possível. Estes encontros são compostos por um bloco de betão assentes diretamente no tereno. Esta forma de montagem poderá provocar assentamentos devido à falta de conhecimentos do solo.

Geralmente, estruturas como pontes modulares, são apenas suportadas por encontros superficiais, sempre que possível. Estes encontros são compostos por um bloco de betão, como explanado ao longo do capítulo 2, assentes diretamente no tereno. Esta forma de montagem poderá provocar assentamentos devido à falta de conhecimentos do solo. Desta forma, é frequente a utilidade das pontes modulares em momentos críticos ou com relativa urgência, posto isto, o local da montagem da ponte é muitas vezes inflexível, o que, por vezes, torna o trabalho do engenheiro mais problemático. Desta forma, será necessário recorrer a uma prospeção rápida do terreno, analisar as características do solo e por fim, ponderar a necessidade de uma solução profunda.

Assim sendo, este artigo prende-se em propor uma solução de fundação profunda eficiente, que seja compatível com as exigências deste tipo de obra e que facilite o dimensionamento e montagem.

II. ESTADO DA ARTE

A. *Introdução Histórica*

Desde o início do seu emprego em ambiente operacional, as pontes modulares eram utilizadas maioritariamente para ambientes de guerra. Estas pontes serviam para apoiar as forças militares e teriam de estar equipadas para resistir às cargas militares, isto é, dimensionadas com critérios mais exigentes.

Estas pontes eram montadas por módulos, facultando a vantagem de serem rápidas de montar. Dependendo das imposições da operação militar, a rapidez de montagem de uma ponte modular era e é um requisito importante. Na segunda guerra mundial os norte-americanos e os ingleses destacaram-se por desenvolver as pontes Bailey. O primeiro avanço na ponte Bailey foi feito pelos militares britânicos com a invenção desta ponte pelo autor Donald Bailey. Esta necessidade de uma ponte mais sustentável para os militares surgiu pelo avanço nos carros de combate. Realce para o veículo Tank Mark IV que pesava cerca de 39 toneladas. (ThinkDefence, 2012)

Durante a Segunda Guerra Mundial, a ponte Bailey foi usada por vários países europeus. Hoje em dia a ponte Bailey continua a ser comercializada e utilizada pelas suas vantagens de ser fácil de transportar, rápida de montar e desmontar, boa capacidade de carga e boa resistência à fadiga.

B. *Tipos de Pontes Modulares*

Foi decidido que seriam analisadas apenas as pontes do tipo apoio/logísticas e de comunicação, pois são estas que abrangem maior interesse para o objetivo final. As pontes logísticas são pontes que também podem ser utilizadas como pontes de assalto, estas pontes, por serem de categoria modular, são flexíveis de gerar diferentes vãos. As pontes logísticas são pontes que poderão conseguir ter uma maior resistência às cargas ou vencer um maior vão, dependendo da sua necessidade.

No que respeita à ponte MB60, utilizada durante o estudo de caso. está avaliada para atingir vãos próximos de 60 metros Em relação aos encontros, a ponte MB36 recorre aos encontros de configuração simples, enquanto que a ponte MB60 recorre a encontros de configuração dupla,. Estes encontros são compostos por blocos de betão, com uma altura que depende das cargas da ponte, que assentam diretamente no solo, caso o solo permita.

III. MICROESTACAS TRM APLICADAS EM PONTES MODULARES

Estruturas como as pontes modulares necessitam de conduzir as cargas do peso próprio e as respetivas sobrecargas de utilização para o terreno, estas cargas são encaminhadas dos montantes de extremidade para o solo. Caso o terreno superficial seja de características mecânicas adequadas, podemos recorrer a fundações superficiais, dispondo apenas de uma camada de betão (grout) e dos apoios de configuração simples, dupla ou tripla, tal como referido anteriormente. Visto estar-se a tratar de pontes modulares, onde se dá primazia à rapidez de construção, torna-se primordial pensar num método de fundação rápido e funcional. Desta maneira, será apresentado uma solução de microestacas tipo TRM, com destaque na composição, comportamento e processos construtivos.

A. Conceitos Gerais das Fundações por Microestacas

No que pertence às fundações indiretas, podemos dividir em estacas moldadas ou cravadas, e dentro das cravadas por estacas de madeira, metálicas, betão armado ou mistas. Para pontes modulares, não se justificaria utilizar estacas moldadas, assim sendo, definiu-se que a solução mais correta seria a de estacas cravadas.

Depois podemos definir como uma estaca de ponta caso seja apoiada num substrato rígido, flutuante caso as cargas sejam resistidas pela resistência lateral da estaca, ou então mista.

B. Microestacas TRM

As microestacas TRM são constituídas por ferro fundido dúctil e posteriormente injetadas com microbetão. O ferro fundido dúctil é utilizado devido à sua elevada resistência química e mecânica e o microbetão para oferecer maior resistência à compressão. O processo construtivo pode ser pelo método de cravação por via seca ou por via húmida, distinguindo-se estes dois pela sequência da injeção do microbetão.

No que respeita à aplicabilidade da solução para diferentes tipos de solos, é importante realçar que esta solução não terá o melhor rendimento para solos duros, rochas ou solos com blocos rochosos dispersos, isto porque a esbelteza da microestaca poderá sofrer encurvadura em situações mais críticas, pelo que, cabe à prospeção geotécnica analisar o terreno e, a partir do perfil geotécnico, retirar conclusões.

Em relação ao tipo de obra provisória, existe a preocupação do reaproveitamento de material de fundação. Este tipo de microestacas permite que sejam parcialmente removidas, no entanto, para este critério, existem outras soluções no mercado que garantem a reutilização do material de fundação, como por exemplo as estacas helicoidais. No que se refere aos equipamentos e maquinas utilizados em obra, estes são fáceis de manobrar e capazes de operar em locais de acesso difícil ou espaços de tamanho reduzido. Tanto as maquinas de construção como os materiais e suas geometrias serão fatores fundamentais para a rapidez de execução do processo construtivo. (Rohre, 2014)

Como destacado, a cravação por via seca está materializada para ambientes em que o terreno é bastante variável e com rigidezes muito desiguais. Em suma, o método viabiliza a realização da microestaca, desde o solo de fraca qualidade até ao substrato rígido, de forma a obter uma microestaca que transmita as cargas da estrutura para o substrato unicamente (comportamento de estaca de ponta). (Tiroler Rohre, 2014)

Realça-se o facto destas microestacas trabalharem como estacas de ponta, ou seja, não resistem aos esforços de tração que poderão surgir por motivos como acidentes ou cheias, assim, deverá haver outro mecanismo no apoio capaz de suportar as cargas anti-gravíticas.

O processo de cravação é feito por um martelo hidráulico, e o controlo da cravação é feita por um operador que vai contabilizando o tempo de cravação por metro de estaca. O processo deverá ser registado num boletim de execução. Para este tipo de estacas será fácil detetar o término deste processo, dado que cravação da microestaca torna-se mais lenta quando atinge o substrato rígido. (Caetano, 2014)

Para atingir o substrato é possível realizar a quantidade necessária de uniões pois não existem limitações quanto ao número de tubos para uma microestaca TRM. (Tiroler Rohre, 2014) Durante a cravação das microestacas é importante estar atento a encurvaduras, pois as pressões aplicadas em secções de elevada esbelteza, como é o caso, poderá provocar encurvaduras que deformem as microestacas, alterando o natural encaminhamento de cargas.

Posteriormente, procede-se à injeção do microbetão no interior do tubo TRM, este material vai otimizar as características da microestaca. Para a selagem interior ser efetuada com sucesso o microbetão terá de atingir toda a profundidade do tubo. Terá ainda de preencher também o topo para assim garantir a boa ligação do tubo TRM à chapa de ligação pois o microbetão será o elemento ligante entre estes dois.

Quanto ao método de cravação por via húmida, e ao contrário do método por via seca, utiliza microbetão durante a sua cravação. O objetivo final deste método é formar um modelo tipo "sandwich" com o tubo TRM e com o microbetão no interior e no exterior do tubo. O microbetão no interior tem a mesma competência que nas microestacas cravadas por via seca, a modificação encontra-se na presença do microbetão entre o tubo TRM e o terreno envolvente, esta alteração garante à microestaca um incremento da resistência lateral provocada pelo atrito do microbetão com o tubo e com o terreno.

Assim, as microestacas cravadas por via húmida destinam-se especialmente a casos em que o terreno não apresenta boas propriedades mecânicas e consequentemente não encontramos solo rígido a uma profundidade próxima. Geralmente são solos granulares com média densidade, ou solos de elevada percentagem de cascalhos e areia. Nestas situações é imprescindível que a microestaca se comporte de modo flutuante. Para confirmar e melhorar o encaminhamento das cargas preenche-se o exterior da microestaca com microbetão de forma a criar uma superfície rugosa, aumentando assim o atrito entre o tubo TRM e a camada exterior. (Caetano, 2014)

Tal como no método por via seca, o primeiro troço a ser cravado é o mais condicionante. Este tubo é dotado de uma sapata de base com aberturas, estas aberturas permitem que o microbetão que está a ser injetado no interior da microestaca (isto durante a cravação) possa fluir para o exterior. A sapata de base terá ainda de ter um diâmetro maior que o diâmetro da estaca, isto para garantir que o microbetão acompanha a cravação.

Durante todo o processo de cravação, existe uma pressão de injeção na sapata de ponta provocada pelo impulso do microbetão, do interior para o exterior, tal como demonstrado na figura 1.

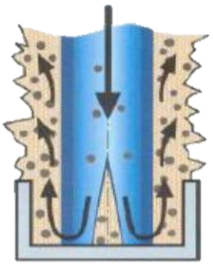


Figura 1. Representação de pressões devido à injeção do microbetão durante a cravação

IV. Critérios de Dimensionamento

Para o dimensionamento das soluções fundações indiretas, devemos partir de prossupostos considerado nos regulamentos de dimensionamento como o EC7. O dimensionamento das fundações profundas prevê o estudo da capacidade resistentes da estaca e a capacidade resistente do solo.

A. Dimensionamento Geotécnico

Para a generalidade do artigo, terá de haver um contraste importante entre o emprego da análise do ELU e do ELS, isto pelo facto de estarmos a lidar com estruturas de carácter temporário e de emergência, como tem sido referido.

B. Dimensionamento Estrutural

Para o cálculo resistente da compressão é necessário considerar os materiais presentes na fundação e as suas diferentes propriedades. Assim, deverá entrar no cálculo a resistência do ferro fundido dúctil e a resistência do microbetão, tal como explanado na tabela 1.

Tabela 1. Áreas transversais de microbetão e de ferro fundido e as respetiva cargas máximas de compressão para cada microestaca TRM

Microestaca (Ø x e) ($mm \times mm$)	**A_b (mm^2)**	**A_s (mm^2)**	**N_d (kN)**
118 x 7,5	2604	8332	897
118 x 9,0	3082	7854	1028
170 x 9,0	4552	18146	1628
170 x 10,6	5308	19557	1835

V. Definição do Modelo de Análise (Plaxis 2D)

No presente capítulo será exposto o estudo de caso e serão apresentados os detalhes executados para obtenção dos resultados pelo software Plaxis 2D.

A. Carcterização Geotécnica do Terreno

Por forma a testar a solução descrita neste artigo, aproveitou-se os dados da campanha de prospeção da empresa ENGGEO em Sarilhos Grandes, Montijo. O estudo geológico-geotécnico da campanha incidiu na identificação das formações geológicas, numa definição de um modelo geológico-geotécnico, e na estimativa das propriedades físicas do maciço e das respetivas características de resistência e deformabilidade

De forma a definir todos os elementos da ponte para posterior análise do peso distribuído para os encontros, é fundamental recorrer aos regulamentos AASHTO, *Trilateral Design and Test Code*, Eurocódigo 1 e STANAG 2021.

Conforme o fornecido pela *BERD*, foram utlizadas as cargas da ponte MB60 e as cargas variáveis Segundo a norma AASHTO.

B. Modelação em Plaxis 2D

A partir do software Plaxis 2D foi possível estimar o comportamento de uma microestaca de 170 mm de diâmetro, em função das cargas da ponte MB60 fornecidas pela BERD.

Para modelar a solução no software proposto, procedeu-se à analise de uma solução profunda de secção circular com carregamento axial no seu eixo. Com isto, iniciou-se o projeto considerando um modelo axissimétrico executado por meio de elementos triangulares de 15 nós (malha de elementos finitos), onde se definiu apenas metade da secção.

Na figura 2 encontra-se o modelo de elementos finitos desenvolvido em software.

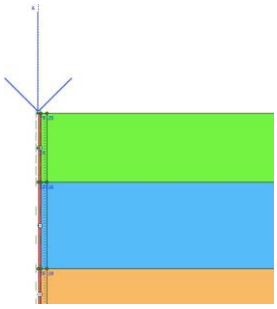


Figura 2. Modelo de Elementos Finitos

De modo a atingir o caso mais desfavorável para avaliar o comportamento da solução, elegeu-se a ponte de 61,6 metros de vão (ponte com maior vão, MB60) de forma a alcançar as cargas mais exigentes.

Assim, a partir do resultado para o ELU, optou-se por definir para este caso a solução microestaca TRM 170x9,0 mm.

Devido à distância entre encontros (mais de 5 metros) é sensato realizar a modelação do caso com apenas uma microestaca, isto porque as microestacas não se influenciarão mutuamente

C. Resultados do estudo

Os resultados obtidos para a solução proposta estão explanados na seguinte ilustração (figura 3), onde se pode analisar os assentamentos da solução no estudo de caso e as verificações impostas pelo EC7 e pela empresa BERD. A partir do EC7, foi calculado o valor para o ELS e para o ELU, resultando os valores de 781 kN e 1128 kN para ELS e ELU, respetivamente.

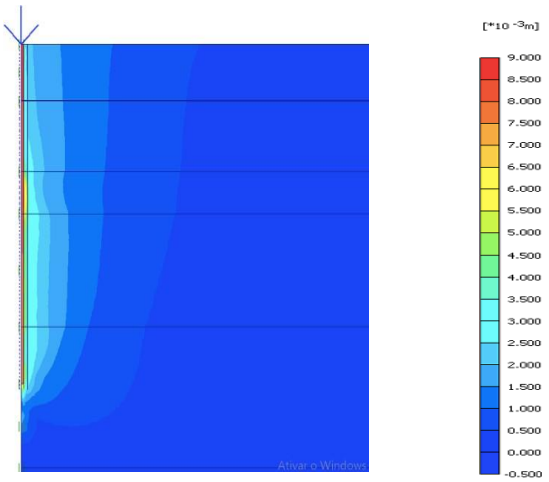


Figura 3. Diagrama de deformações empresa BERD, o valor do assentamento para a carga ELS é admissível.

Na figura 4 está representada em pornemor, a curva carga vs. assentamento para o caso prático.

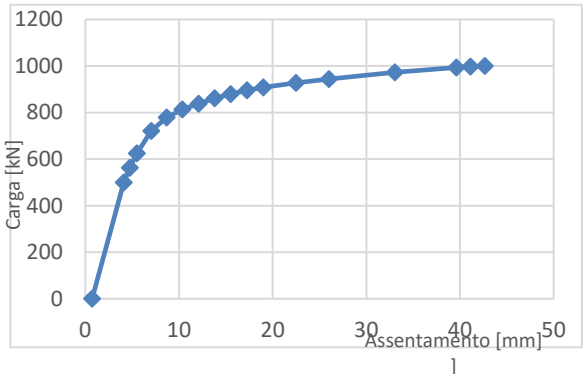


Figura 4. Gráfico curva vs. Assentamento para o ELS.

Assim sendo, verifica-se que o assentamento obtido no software corresponde a um valor expectável (8,8 mm). No que respeita aos valores máximos admitidos pelo EC7 e pela *BERD*.

- Deslocamento vertical máximo (EC7)

$$d_{v,max} = H \times \frac{1}{1000} = 12 \times \frac{1}{1000} = 0{,}012 = 12\ mm > 8{,}8\ mm$$

- Deslocamento vertical máximo (BERD)

$$d_{v,max} = 10\ mm > 8{,}8\ mm$$

VI. CONCLUSÕES

Neste artigo é estudada uma solução de fundação de microestacas cravadas tipo TRM para pontes modulares. Para este feito, o artigo direcionou o foco para três pontos chave: estudar o campo das pontes modulares para entender as suas características base, analisar a adaptabilidade das microestacas TRM em pontes modulares e com isto, o comportamento deste tipo de fundação, e por fim, estudar a solução com base num modelo de elementos finitos e avaliar o seu comportamento, ao nível geotécnico e estrutural.

Outro aspeto específico nas fundações profundas e que precisou de destaque, foram os métodos de prospeção geotécnica expeditos e compatíveis com as exigências deste tipo de estrutura. Por outras palavras, antes da montagem da ponte modular, e dependendo dos conhecimentos que temos do local da obra, será necessário realizar uma prospeção geotécnica.

Definida uma solução que cumprisse os requisitos, foi necessário explorar as características básicas de uma fundação profunda, tal como a que foi escolhida, e ainda aprofundar o processo construtivo da mesma. No que corresponde ao processo construtivo da microestacas TRM, foi importante avaliar a funcionalidade de todo o processo em ambiente urgente, como a facilidade de transporte, matérial, equipamento, aplicabilidade em vários solos e rapidez de execução.

Como conclusão, os objetivos foram alcançados pois, podemos admitir que a solução de fundação profunda por microestaca TRM é uma solução eficiente para uma estrutura como uma ponte modular. O processo construtivo vai ao encontro dos critérios exigidos e a sua capacidade estrutural vai ao encontro do pretendido.

AGRADECIMENTOS

É importante para mim deixar uma palavra de apreço aos meus orientadores, Professor Alexandre Pinto e Engenheiro António André, por toda a dedicação. Por último, aos meus pais, irmã, avó e à Inês o mais profundo obrigado, por todo o apoio, e, acima de tudo, pela confiança que depositaram em mim, sempre crentes no meu sucesso.

REFERÊNCIAS BIBLIOGRÁFICA

[1] André, A. (2016). Estudo da Aplicação de Pré-Esforço Orgânico em Pontes Provisórias. Porto: Faculdade de Engenharia da Universidade do Porto.

[2] BERD. (2019). M1 : Manual Técnico : Instalación, Montaje y Lanzamiento. Porto.

[3] Caetano, M. (2014). Igreja Nossa Senhora dos Navegantes, Parque das Nações : Fundações Indiretas por Microestacas Cravadas. Instituto Superior Técnico. Lisboa.

[4] Eurocodigo 7. (2010). Projeto Geotécnico. Regras Gerais". Eurocódigo 7 - Parte 1. Pré-norma europeia, ENV 1997-1.

[5] ThinkDefence. (30 de dezembro de 2011). UK Military Bridging - Equipment (Pre WWII Equipment Bridging). Obtido em 5 de março de 2020, de https://www.thinkdefence.co.uk/2011/12/ukmilitary-bridging-equipment-pre-wwii-equipment-bridging

[6] Tiroler Rohre. (2014). Piling Systems for Deep Foundations. Obtido em 28 de março de 2020, de http://duroterra.com/

CryingJackpot: Fluxos de Rede e Indicadores de Desempenho contra o Cryptojacking

Gilberto Gomes[1,2] Luis Dias[1,2] Miguel Correia[2]
[1]CINAMIL, Academia Militar, Instituto Universitário Militar – Portugal
[2]INESC-ID, Instituto Superior Técnico, Universidade de Lisboa – Portugal
gomes.g@exercito.pt dias.lfxcm@exercito.pt miguel.p.correia@tecnico.ulisboa.pt

***Resumo*—*Cryptojacking* traduz a apropriação de recursos computacionais alheios sem conhecimento ou consentimento das vítimas para obter moedas criptográficas, um ataque generalizado relativamente fácil de implementar e difícil de detectar. Seja com recurso a um navegador Web ou através de um executável, o *cryptojacking* carece de soluções de detecção robustas e fiáveis.**

O presente artigo descreve o trabalho desenvolvido na prossecução de uma abordagem híbrida para a detecção de *cryptojacking*, onde não é necessário conhecimento prévio sobre os ataques ou dados de treino. A nossa abordagem de deteção, CRYINGJACKPOT, extrai e combina características/atributos baseadas em fluxo de rede e em indicadores de desempenho, agregando utilizadores com comportamentos semelhantes com recurso a algoritmos de aprendizagem automática não supervisionados. Avaliamos experimentalmente o desempenho da nossa abordagem com um conjunto de dados artificial e um conjunto híbrido, obtendo valores para a F-score de até 97%.

***Index Terms*—detecção de intrusões, clustering, cryptojacking, fluxo de rede, indicadores de desempenho, análise de segurança**

I. INTRODUÇÃO

Com o aparecimento da *Bitcoin* em 2009, surgiu uma nova actividade designada como **mineração**, da qual surgiu um novo tipo de ataque, o *cryptojacking*, que por definição traduz a apropriação ilícita do poder computacional dos utilizadores sem o seu conhecimento ou consentimento para a obtenção de moedas criptográficas. Este ataque pode ser executado segundo dois vectores de ataque: *scripts* em navegadores web e *malware* binário (executáveis) [1], [2].

A *Bitcoin*, uma representação digital de um valor, juntamente com a *blockchain*, um registo de transacções acessível para apêndice apenas, veio substituir os intermediários convencionais nas transacções utilizando uma rede descentralizada de nós [3]. Para um novo grupo de transacções, o processamento das mesmas passa por utilizar uma elevada fracção de poder computacional para validar, adicionar, e distribuir um novo bloco com estas transacções através da *blockchain*. O esforço computacional está associado à solução de um problema criptográfico, o qual passa pela solução da designada Prova de Trabalho (PoW). Por sua vez o mineiro (*miner*) que resolve a PoW e consegue anexar o bloco à *blockchain* é recompensado com novas moedas [4], [5].

Embora recente, a extracção ilícita de moedas criptográfica representa uma ameaça tanto imediata como a longo prazo, para organizações e utilizadores. Por exemplo, vários dos domínios mais visitados na internet, incluindo YouTube [6], Showtime, e The Pirate Bay [7], foram criticados por empregar *scripts* de mineração contra os seus utilizadores. A um nível diferente, *malware* para a extracção de Monero (XMR) foi encontrado num sistema aeroportuário europeu [8].

As abordagens mais comuns de detecção de intrusões são: **utilização indevida / detecção de assinaturas**, que utiliza o conhecimento prévio dos ataques para construir assinaturas num processo de correspondência que identifica comportamentos que partilham semelhanças com as assinaturas existentes. Normalmente gera um baixo número de falsos positivos, mas falha na detecção de ataques nunca antes vistos; **detecção de anomalias**, onde a ideia é identificar padrões que se desviam do comportamento normal, uma solução apelativa devido à sua capacidade de detectar ataques nunca vistos. No entanto, conduz frequentemente a elevadas taxas de falsos alarmes. [9], [10].

Ambas abordagens partilham uma desvantagem em comum: a necessidade de conhecimento prévio, quer dos ataques existentes, quer do que é o comportamento normal. Ambos tipos de informação podem ser difíceis de obter [11].

Os Sistemas de Detecção de Intrusões (IDSs) também podem ser classificados segundo a fonte dos dados, como (1) baseados nos utilizadores, (2) baseados em rede, ou (3) híbridos. O primeiro (1) tem em conta as características do utilizador para a detecção, o segundo (2) monitoriza o tráfego da rede, e o terceiro (3) – a nossa abordagem – combina ambas as fontes de dados [12].

As técnicas de Aprendizagem Automática (ML), onde modelos estatísticos são construídos com o conhecimento extraído a partir dos dados, através de um processo computacional, desempenham um papel fundamental em muitos IDSs. Estas técnicas podem ser divididas em duas grandes categorias: métodos supervisionados e não supervisionados. Nos **métodos supervisionados**, dados de treino etiquetados são utilizados por um algoritmo para construir um modelo. Um dos métodos supervisionados mais comuns é a classificação, onde o modelo é utilizado para rotular pontos de dados nunca antes vistos e determinar a que classe pertencem. A maioria dos métodos de ML utilizados nos sistemas de detecção por utilização indevida são supervisionados [10].

Aprendizagem não supervisionada – o conjunto de técnicas que utilizamos – é convincente para a detecção de intrusões porque, por definição, não precisa de dados etiquetados como entrada, nem de assinaturas, ou de treino.

Apresentamos o CRYINGJACKPOT, um nova abordagem para um IDS híbrido baseado em aprendizagem não supervisionada para a detecção de *cryptojacking*. A nossa abordagem combina uma técnica de *ensemble* com diferentes algoritmos de *clustering*, utilizando tanto características baseadas em utilizadores como

em rede. Fazendo uso de indicadores de desempenho de um sistema operativo os quais traduzem o estado ou actividade de um sistema e fluxos de rede, pretendemos desenvolver uma abordagem robusta e fiável que não necessitará de conhecimentos prévios ou dados de treino para a detecção de *cryptojacking* em navegadores web ou em executáveis. Combinando a natureza dual das nossas características, a nossa abordagem é capaz de detectar *cryptojacking*, inclusive com cargas de trabalho intensivas e sob tráfego de rede elevado, sendo resistente a diferentes graus de *throttling* (percentagens de consumo), ocultação de código, e o uso de *proxies*.

Testamos a nossa abordagem primeiro com um conjunto de dados público, (CSE-CIC-IDS 2018 [13]), limitado ao uso de atributos baseados em fluxo de rede, um conjunto de dados que possui outros ataques em adição ao *cryptojacking*. Também criámos um conjunto de dados híbrido para analisar fluxos de rede e indicadores de desempenho em simultâneo. O CRYINGJACKPOT obteve valores para a *F-score* de 82% para o conjunto de dados público e uma *F-score* de 97% para o conjunto de dados híbrido em várias experiências concebidas para cobrir um grande número de cenários do mundo real.

Os resultados parciais do presente trabalho encontram-se publicados como: G. Gomes, L. Dias e M. Correia em "CryingJackpot: Network Flows and Performance Counters against Cryptojacking" no 19th IEEE International Symposium on Network Computing and Applications (NCA), Novembro, 2020.

II. ANTECEDENTES

Esta secção começa por explicar a arquitectura dos ataques de *cryptojacking*, fornecendo alguns antecedentes sobre a utilização de *clustering* para a detecção de intrusões, e explica a nossa abordagem para a avaliação (detecção de *outliers*).

A. Cryptojacking

Para lidar com algumas das questões levantadas pela *blockchain*, tais como o consenso dentro da rede, a irreversibilidade das operações, entre outras, foi introduzida a ideia de PoW. Este algoritmo torna a tarefa de adicionar novos blocos à cadeia altamente dispendiosa em termos de consumo computacional [5]. Esta tarefa – definida como mineração – é feita repetidamente até que um número específico de zeros previamente definido para o valor da *hash* seja obtido. O primeiro mineiro capaz de resolver este problema é recompensado com novas moedas pelo esforço computacional utilizado. O novo bloco é divulgado através dos nós do sistema que o acrescentam à sua instância local da *blockchain* [4], [5].

Resultado da constante evolução tecnológica, não muito depois do aparecimento da *Bitcoin*, a prática da extracção desta moeda criptográfica com as máquinas de utilizadores correntes tornou-se inviável. Este paradigma não iria mudar até 2014 com o aparecimento de uma nova moeda criptográfica, o **Monero (XMR)**. XMR usa o *RandomX*, um algoritmo que torna as tarefas de mineração igualmente eficientes na Unidade de Processamento Central (CPU) e na Unidade de Processamento Gráfico (GPU), ao mesmo tempo que torna a prática menos eficaz em Application-Specific Integrated Circuits (ASICs). Sendo ideal para mineração pelas máquinas dos utilizadores do dia a dia, houve um aumento no desenvolvimento de *scripts* para este fim.

B. Clustering e detecção de intrusões

Clustering é um conjunto de técnicas para encontrar padrões em dados não etiquetados de alta dimensão [9]. A ideia geral é que objectos semelhantes são agrupados através da medição da distância entre os mesmos. Um algoritmo de *clustering* aceita como entrada um conjunto de entidades e devolve um grupo de subconjuntos (ou *clusters*) dessas entidades. No entanto, este processo não nos diz nada sobre a natureza dos subconjuntos/clusters individuais.

Para a detecção de intrusões ou anomalias, muitos trabalhos fazem uso da ideia de que grandes *clusters* representam comportamentos normais e que os *outliers* (e.g, pequenos aglomerados de entidades ou ruído) podem corresponder a um comportamento anómalo [10]. Os *outliers* são os pontos de um conjunto de dados que são altamente improváveis de ocorrer para um determinado modelo desses mesmos dados.

Neste trabalho, perseguimos a ideia de descobrir *outliers* como sendo *clusters* com uma só entidade, para o qual a escolha dos algoritmos traduz um passo fundamental no desenho da nossa abordagem. Devido à falta de literatura para a detecção de *cryptojacking* com métodos não supervisionados, decidimos prover a nossa abordagem de redundância, escolhendo três tipos diferentes de algoritmos e a implementação de uma técnica de *ensemble* influenciada por trabalhos anteriores [14], [15].

Os algoritmos de *clustering* que escolhemos podem ser classificados como baseados em partições, hierárquicos, e baseados em densidade. *K-means* ($O(nkdi)$), é um algoritmo popular baseado em partições que distribui os pontos de dados X em k *clusters*, onde cada ponto de dados é mais semelhante ao centróide que define o seu *cluster* do que aos centróides de *clusters* vizinhos.

Dentro do *clustering hierárquico (HC)*, os algoritmos organizam os dados numa estrutura hierárquica de acordo com uma matriz de proximidade. Os resultados do HC são normalmente representados por uma árvore binária ou dendrograma. Escolhemos o algoritmo *Agglomerative*, uma vez que a utilização de algoritmos divisórios é uma prática invulgar devido ao esforço computacional associado [16].

DBSCAN agrupa os pontos de dados em *clusters* que têm uma densidade mais elevada do que um certo valor limite ($MinPts$). Executa esta tarefa dentro de uma janela com um tamanho especifico definido pela distância até ao ponto de dados (eps)[10].

III. CRYINGJACKPOT, A ABORDAGEM

A nossa abordagem titulada CRYINGJACKPOT (Figura 1), visa identificar automaticamente outliers, i.e, entidades – utilizadores – alvo de *cryptojacking*, extraindo, combinando e processando um conjunto de características/atributos. Estas características são obtidas a partir de indicadores/contadores de desempenho relativos aos utilizadores [17] e fluxo de rede [18]. Em relação aos contadores, neste trabalho consideramos apenas contadores fornecidos pelo sistema operacional Windows, mas a abordagem é genérica.

A. Colecção de dados

Como mencionado anteriormente, o CRYINGJACKPOT obtém os atributos de duas fontes de dados diferentes, indicadores de desempenho e fluxo de rede.

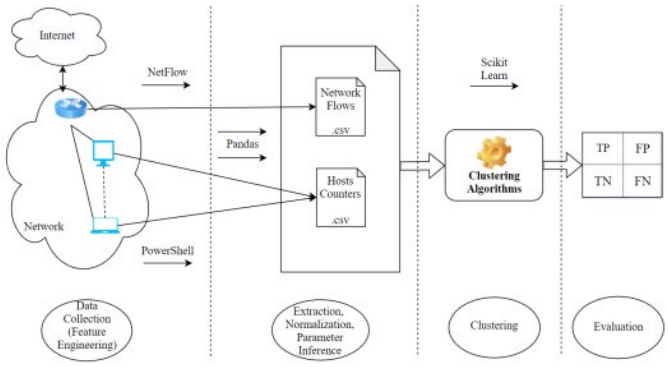


Fig. 1. Perspectiva geral do CRYINGJACKPOT.

Optamos por usar **indicadores de desempenho** para máquinas Windows, para explorar o comportamento do *cryptojacking* como um ataque computacionalmente intensivo. Acabamos com 123 contadores de desempenho, um conjunto de indicadores que descrevem **CPU, memória, utilização da rede, e processos em execução dentro de uma máquina.** Alguns exemplos:

```
\Processor(*)\% Processor Time
\Memory\Available Bytes
\Network Interface(*)\Bytes Sent/sec
```

Em relação às características baseadas no **fluxo de rede** as nossas escolhas foram influenciadas por obras que descrevem o protocolo Stratum e a detecção de *cryptojacking* [19].

Do ponto de vista da fonte, o CRYINGJACKPOT começa por extrair 2 características fixas que exploram os padrões de dados recebidos: (1) `SrcBytesPktBwd`, número de bytes por pacote recebido como SrcIP; (2) `SrcMeanBytesBwd`, número médio de bytes recebidos como SrcIP.

Implementamos também uma técnica que melhorou significativamente os nossos resultados. Extraímos um conjunto de 11 características de fluxos cujos IPs de destino tinham sido, durante uma determinada janela de tempo, contactados apenas por um IP hospedeiro/fonte, i.e., um destino raro. Esta decisão visou explorar as ligações feitas com os domínios exclusivos das piscinas de mineração. Além disso, o CRYINGJACKPOT também define 5 características relacionadas com portas de rede, HTTP/80 e HTTPS/443, utilizando neste caso, as portas de rede de origem como chaves de agregação.À semelhança da avaliação realizada para os contadores de desempenho, também pesámos o nosso conjunto inicial de características, terminado com 37 características baseadas em fluxo de rede.

O CRYINGJACKPOT é semelhante desde do ponto de vista do destinatário, diferindo nas características relacionadas com portas de rede.

B. Extracção, normalização, e parâmetros iniciais

A nossa abordagem pode processar dados em diferentes janelas de tempo pré-definidas, de duração $\mathcal{W} = \{w_1, w_2, ..., w_n\}$, e.g., 10 minutos, 1 hora, 1 dia. Esta abordagem efectua o *clustering* para cada janela de duração $w_i \in \mathcal{W}$, para os períodos de dados disponíveis. Para cada janela de tempo de duração $w_i \in \mathcal{W}$, são extraídas características de todos os fluxos e contadores relativamente à janela de tempo em análise seguindo a lógica da Secção III-A.

Esta etapa resulta em dois vectores de características para cada anfitrião, um contendo as características obtidas dos contadores de desempenho e o segundo com características dos fluxos da rede.

Para cada janela de tempo $w_i \in \mathcal{W}$, os atributos têm de ser normalizados antes da etapa de *clustering*. A normalização é realizada escalonando cada característica a um intervalo comum, e é importante não perder informação durante este processo.

Avançando para a fase de *clustering*, uma decisão crítica está associada aos parâmetros de inicialização dos algoritmos. Estes parâmetros ditam os resultados obtidos no que é conhecido como processo de tentativa e erro, por não existir um conjunto específico de parâmetros pré-definidos que se saiba que gerem resultados ideais.

Em relação aos parâmetros do *K-means* e do *Agglomerative*, ambos distribuem um conjunto de objectos em K *clusters*, pelo que K tem de ser definido. O melhor valor de K pode ser encontrado através de força bruta, um método que é inviável na prática, devido ao esforço computacional necessário. Para tal, utilizamos dois algoritmos, o algoritmo **do cotovelo** e o algoritmo **silhueta**, para encontrar o valor de K.

Em relação ao *DBSCAN*, este requer que a densidade numa vizinhança de um determinado objecto seja suficientemente alta para ter um *cluster* atribuído [16]. Temos de escolher o número de amostras numa vizinhança para que um ponto possa ser considerado como um ponto central ($min_samples$) e a distância máxima entre duas amostras para que uma seja considerada como na vizinhança da outra (eps) [20]. eps pode ser escolhido como a alteração mais pronunciada, quando as distâncias entre cada entidade e os seus vizinhos são calculadas e ordenadas [21]. Os três algoritmos mencionados podem ser implementados utilizando a distância euclidiana.

C. Clustering e avaliação

Após a extracção e normalização das características, os vectores de características são fornecidos como entrada para os algoritmos de *clustering*. A ideia é agrupar máquinas com comportamento semelhante, com base nos valores das características. O CRYINGJACKPOT é capaz de executar esta tarefa utilizando as características relacionadas com a máquina/utilizador independentemente das baseadas em fluxo, sendo o objectivo principal a utilização simultânea de ambos os conjuntos. Este é um passo importante na concepção porque dota a nossa abordagem de flexibilidade para futuras implementações.

O resultado da etapa de *clustering* é um conjunto de *clusters/clusters* com anfitriões para cada janela de tempo de duração $w_i \in \mathcal{W}$. Cada anfitrião aparece num *cluster* para cada janela de tempo.

Vários métodos podem ser utilizados para a classificação. Se necessário, uma inspecção manual pode ser realizada por um analista em segurança, começando com os *clusters* mais pequenos. Contudo, para automatizar a identificação de anomalias, consideramos que **um outlier é uma entidade isolada num cluster**. A desvantagem desta abordagem é que, para várias vítimas em simultâneo, as nossas capacidades de detecção deterioram os resultados, uma vez que as vítimas tendem a partilhar *clusters*.

IV. Conjunto de dados híbrido

Devido à natureza da nossa abordagem, não fomos capazes de descobrir um conjunto de dados que satisfizesse as nossas necessidades de ter fluxos de rede e indicadores de desempenho, combinados com ataques de *cryptojacking*. Por conseguinte, criámos um conjunto de dados híbrido, onde dados do mundo real foram recolhidos e adaptados para serem depois utilizados nos nossos testes.

Tal como foi afirmado por Sharafaldin et al. [22], existe um conjunto de considerações a ter em conta ao utilizar ou criar um conjunto de dados. Tivemos estas observações em consideração pois precisávamos de obter um conjunto de dados específicos para os nossos testes de detecção. Esta tarefa foi conduzida em duas fases: Recolha de dados benignos (perfis-B) e recolha de dados maliciosos (perfis-M).

A nossa abordagem para a criação do conjunto de dados é descrita como se segue. Decidimos obter um pequeno conjunto de dados do mundo real, sem filtragem. Extraímos toda a informação, relativa ao tráfego de rede (pacotes) e indicadores de desempenho, para um conjunto de utilizadores cujas impressões digitais reflectiram as actuais tendências computacionais do mundo real. Este conjunto inicial de dados foi então utilizado para replicar a restante estrutura da rede (Secção IV-B) utilizando uma abordagem que visou assegurar que os dados se aproximassem do que seria um conjunto de dados do mundo real. Os dados do perfil M (Secção IV-A) foram obtidos com uma abordagem semelhante, utilizando amostras reais de malware combinadas com o tráfego real dos utilizadores.

A. Recolha de amostra maliciosas

Encontrar amostras de *cryptojacking* foi uma das tarefas mais importantes, pois queríamos garantir que apenas amostras maliciosas activas eram recolhidas, e que tínhamos coberto o maior número possível de variantes do ataque. O nosso objectivo era encontrar scripts de utilização em navegadores web, bem como malware executável.

Em relação ao *cryptojacking web*, utilizámos um motor de pesquisa de código-fonte (https://publicwww.com/) para procurar etiquetas específicas que identificassem código de scripts de mineração incorporados em diferentes domínios.

Tabela I
Amostras de cryptojacking baseadas em navegador web.

Etiqueta de Busca	Domínio	Script de Mineração
minero.cc	tibumpiscinas.com.br	minero.cc/lib/minero.min.js
minero.cc	naftkala.com	minero.cc/lib/minero.min.js
hostingcloud	serieshdpormega.com	hostingcloud.racing/8vVW.js
hostingcloud	vstars.pl	hostingcloud.racing/BBlJ.js
webminepool	oslafo.com	webminepool.com/lib/base.js

Da nossa pesquisa seleccionámos 5 amostras baseadas em navegador web que verificamos estarem ativas. A Tabela I resume a informação sobre as amostras e a Figura 2 mostra um extracto de código-fonte para um dos domínios maliciosos. Estas amostras também funcionam com diferentes níveis de *throttle*, ou seja, limite para o consumo efectivo de recursos, o que nos permite explorar diferentes cenários durante a detecção. Conseguimos mostrar que mesmo ataques com consumo reduzido de CPU são detectados.

```
<script src="https://www.hostingcloud.racing/Aync.js"></script>
<script>
      var _client = new
  Client.Anonymous('03f0ff94450082fe747c62c0d24b9c90d4d5f06d581643c1ebe2740356f36321',
  {
          throttle: 0 , c: 'w' , ads: 0
      });
       _client.start();
</script>
<div style="display:none">
    </div>
```

Fig. 2. Código-fonte do domínio www.serieshdpormega.com

Também desenvolvemos a nossa abordagem para poder detectar **amostras de *cryptojacking* executável**. Para encontrar estes binários, procurámos através de repositórios de *malware* como https://urlhaus.abuse.ch/ e https://dasmalwerk.eu/. Recolhemos 5 amostras de *malware* executável para *cryptojacking* estes também com diferentes valores de *throttle* (Tabela II).

Tabela II
Amostras de cryptojacking executável.

Amostra
down.gogominer.com/sex_Live1.5.0.1099.exe
14.141.175.107/cryptominerbros/wordpress/
14.141.175.107/cryptominerbros/wordpress/wp-content/Vh/
149.28.24.180/miner/bashd32
ivansupermining.info/bin/minbuild.exe

B. Criação das extracções base

Com as amostras maliciosas necessárias, criámos as extracções de base que mais tarde foram utilizadas para criar o conjunto de dados híbridos pretendido. Os perfis B visam encapsular os comportamentos das entidades dos utilizadores nas suas tarefas normais. Este é um dos grandes desafios dos conjuntos de dados artificiais, o de alcançar o comportamento complexo de um utilizador do mundo real. Para as extracções do nosso conjuntos de dados definimos 3 tipos de perfis de comportamento para os anfitriões: (1) perfil baixo (L); (2) perfil médio (M); (3) perfil alto (H). Perfil baixo representa anfitriões com baixa utilização dos recursos do sistema e tráfego de rede ligeiro. Perfil médio representa anfitriões com um uso intermédio de recursos focados na produtividade (Microsoft Office, trabalho em nuvem). O perfil alto visa reproduzir cargas computacionais intensas (máquinas virtuais, Adobe Photoshop, downloads, múltiplos separadores web). A nossa abordagem visou a criação de um conjunto de dados que simulassem diferentes tipos de redes, i.e., permitir a detecção de *cryptojacking* para diferentes cargas de trabalho, e mais importante, para compreender se as cargas de trabalho de alto perfil escondem o comportamento do ataque.

Tendo a nossa estratégia definida, utilizámos 9 computadores Windows 10 Enterprise com CPU Intel(R) Pentium(R) G3250 @3.20GHz, 3200 Mhz, 2 Core e 8,00 GB de RAM para executar as nossas extracções. Estas máquinas foram divididas pelos três perfis, e cada máquina tinha a ferramenta Wireshark instalada para obter os pacotes de rede, e um script PowerShell por nós desenvolvido para a recolha dos indicadores de desempenho.

Seguindo um calendário para que as expectativas para os perfis fossem satisfeitas, acabamos por ter o equivalente a um dia de extracções relativas a actividade benigna, com 9 ficheiros CSV três para cada perfil e de forma semelhante, 9 ficheiros PCAP com o tráfego da rede. Aos ficheiros PCAPs aplicámos o *CICFlowMeter* disponível em https://github.com/ahlashkari/

CICFlowMeter para obter fluxos de rede partir dos pacotes recolhidos.

Seguindo a mesma abordagem, mas agora utilizando as amostras maliciosas anteriormente mencionadas, utilizámos 10 máquinas. 5 delas foram utilizadas para executar os scripts web seguindo calendarização e as outras 5 para as amostras binárias a executar permanentemente no segundo plano das vítimas. Além disso, também aqui as máquinas foram divididas por perfis. No final da nossa extracção diária, obtivemos ficheiros equivalentes como na extracção benigna.

Como passo final para criar o conjunto final de dados, criámos 10 dias de extracções, um dia para cada uma das vítimas que tínhamos criado. Definimos o número de máquinas que queríamos para cada um dos dias, um número que variou entre 300 e 400 máquinas. O processo para criar estas máquinas a partir das extracções base foi:

- definir o número de máquinas por perfil;
- reproduzir a quantidade de máquinas pretendidas a partir das extracções base com a adição de ruído.

Relativamente a aplicação de ruído, o objectivo era clonar máquinas/anfitriões alterando os valores de base por uma percentagem aleatória (Equação 1).

$$x' = x + random([-1, 1]) \times \frac{x}{random([3, \alpha])}, \alpha \in [15, 30] \quad (1)$$

Os valores predefinidos foram escolhidos para estabelecer um limiar para o qual não alterássemos o tipo de perfil para as réplicas. O nosso conjunto de dados final terminou com 10 dias de dados, contendo os primeiros 6 dias predominantemente máquinas de baixo perfil, um comportamento comum em redes do mundo real, e os outros 4 dias com máquinas predominantemente de alto perfil , sendo a principal razão destas a avaliação da nossa abordagem na detecção de *cryptojacking* entre elevadas cargas de trabalho. Além disso, durante estes 10 dias, metade têm vítimas sob *cryptojacking* web, i.e., o ataque existe para janelas de tempo específicas durante o dia. A outra metade tem *malware* binário estando o *cryptojacking* a correr em segundo plano.

V. Avaliação experimental

Para desenvolver e avaliar o CryingJackpot, utilizámos maioritariamente Python (v3) [23]. Além disso, utilizámos bibliotecas populares tais como *Pandas* [24] para manipulação de dados, e *Scikit-learn* [20] para o processamento de dados e os algoritmos de *clustering*. Todas as experiências foram conduzidas com uma máquina Windows (4-Core Intel Core i7 2.6GHz com 16GB de RAM). O objectivo das experiências é o teste contra diferentes cenários possíveis do mundo real e avaliação de desempenho.

A. Métricas

Tabela III
Indicadores baseados na matriz de confusão.

Indicador	Descrição
Verdadeiros Positivos (TP)	entidades correctamente classificadas como *outliers*
Falsos Positivos (FP)	entidades incorrectamente classificadas como *outliers*
Verdadeiros Negativos (TN)	entidades correctamente classificadas como *inliers*
Falsos Negativos (FN)	entidades incorrectamente classificadas como *inliers*

Considerámos um *outlier* – um positivo – como sendo um anfitrião isolado num *cluster*, identificado por um endereço IP, tendo sido assinalado pelo CryingJackpot. Com base na matriz de confusão da Tabela III, foram utilizadas as seguintes métricas na avaliação:

- Precisão (PREC) – fracção de outliers que são reais (i.e., verdadeiros positivos): $PREC = TP/(TP + FP)$
- Recall (REC) – fracção de outliers corretamente classificados pelo detetor: $REC = TP/(TP + FN)$
- F-score – pontuação global de deteção: $FScore = 2 \times (PREC \times REC)/(PREC + REC)$

Para obter os valores dos indicadores da Tabela III, analisámos os resultados do *clustering* relativos apenas às janelas de ataque (*malware* persistente implica a consideração de todas as janelas de tempo).

B. Caracterização dos conjuntos de dados

Foram utilizados dois conjuntos de dados. O primeiro conjunto de dados, por nós desenvolvido, é descrito na Secção IV.

O segundo, *CIC-IDS 2018* [13], que designámos como o conjunto de dados artificial, foi criado para testar e avaliar IDS em rede. Utilizámos este conjunto de dados combinado com os ataques de *cryptojacking* que criámos para testar a nossa abordagem em diferentes circunstâncias (o conjunto de dados original não continha ataques de *cryptojacking*).

Ao contrário do conjunto de dados híbrido, o conjunto artificial já possuía ataques estando estes limitados a informação relativa a fluxo de rede, sobre os quais adicionamos informações relacionadas com o *cryptojacking*.

C. Resultados com o conjunto híbrido

Os nossos primeiros testes consistiram em combinar características baseadas em fluxo com características baseadas em contadores, para identificar *cryptojacking* utilizando os algoritmos de *clustering* já mencionados. Também realizámos a detecção utilizando ambos os tipos de características de forma independente. Uma primeira observação foi que **a combinação de características baseadas em anfitriões e baseadas em fluxo gerou melhores resultados do que a sua utilização individual**. Estas diferenças traduzem-se em resultados muito mais consistentes para todos os algoritmos implementados e melhorias nos resultados globais (Figura 3). Da utilização individual de atributos baseados em fluxo, obtivemos um aumento de 39% para a melhor F-score, e um aumento de 4,5% para a utilização de contadores, resultado do uso combinado de características.

Relativamente aos resultados gerais do método, **os três algoritmos implementados tiveram um comportamento semelhante, com o DBSCAN a ter um desempenho ligeiramente superior.** Para o K-means e o Agglomerative, a silhueta contribuiu para melhores resultados do que o algoritmo do cotovelo. Contudo, o mesmo não se aplicou ao conjunto de dados artificial (cf. Secção V-D), o que poderá ter estado relacionado com a utilização exclusiva de características baseadas em fluxo de rede.

D. Resultados com o conjunto artificial

O conjunto de dados artificiais tem apenas características baseadas em fluxo de rede, mas inclui mais ataques do que o

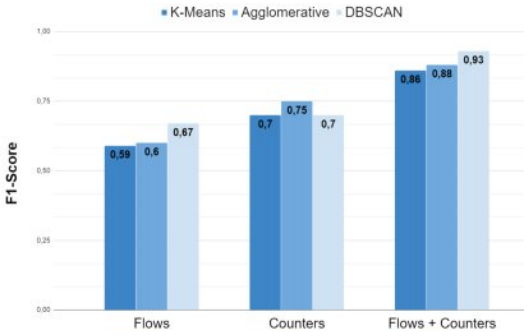


Fig. 3. Comparação de F-scores para a utilização de fluxo de rede, indicadores de desempenho, e o uso simultâneo de ambos tipos de características (conjunto híbrido).

cryptojacking. Por conseguinte, aqui avaliamos o desempenho do CRYINGJACKPOT com essa restrição e perante a presença de outros ataques.

Para os resultados obtidos da deteção de *cryptojacking* para as duas melhores janelas de tempo, observamos que **a nossa abordagem de clustering com *ensemble* melhora os resultados** que são um relativamente inconsistentes para os três algoritmos implementados (e.g., baixa precisão mas alta recall para o Agglomerative). Além disso, o melhor desempenho na detecção de *cryptojacking* foi obtido com o K-means combinado com o método de cotovelo, com uma média de F-score para todas as janelas de tempo de 0,68.

VI. CONCLUSÃO

Apresentamos o CRYINGJACKPOT, uma abordagem híbrida de detecção de *cryptojacking*, baseada em aprendizagem automática não supervisionada, que detecta ataques indefinidos sem assinaturas e dados de treino. A nossa abordagem baseia-se em *clustering*, i.e., na agregação de utilizadores com padrões de dados semelhantes, utilizando para este fim a combinação de características de dados baseados em fluxo de rede e indicadores de desempenho para máquinas Windows. Para a avaliação, foram utilizados dois conjuntos de dados. Em primeiro lugar, desenvolvemos um conjunto de dados híbrido fiável com dados baseados em fluxo e baseados nos utilizadores, onde a detecção de *cryptojacking* foi realizada com excelentes resultados. Depois utilizámos um conjunto de dados público para testar as nossas capacidades quando limitados ao fluxo de rede, estudando a detecção de *cryptojacking* na presença de outros ataques, tendo obtido resultados positivos. O CRYINGJACKPOT provou ser uma solução robusta e flexível para a detecção de *cryptojacking* com valores de precisão, recall, e F-score entre 0,92 e 1.

REFERÊNCIAS

[1] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark, "A first look at browser-based cryptojacking," in *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, Jul. 2018, pp. 58–66.

[2] H. L. J. Bijmans, T. M. Booij, and C. Doerr, "Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale," *Proceedings of the 28th USENIX Security Symposium*, pp. 1627–1644, 2019.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system satoshi nakamoto," Tech. Rep., 2008.

[4] M. E. Peck, "Blockchains: How they work and why they'll change the world," *IEEE Spectrum*, vol. 54, no. 10, pp. 26–35, Oct. 2017.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, Sep. 2017, pp. 557–564.

[6] D. Goodin, *Now even YouTube serves ads with CPU-draining cryptocurrency miners*, 2018. [Online]. Available: https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners (visited on 11/08/2019).

[7] The Guardian, *Ads don't work so websites are using your electricity to pay the bills*, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/sep/27/pirate-bay-showtime-ads-websites-electricity-pay-bills-cryptocurrency-bitcoin (visited on 11/05/2019).

[8] S. Gatlan, *European airport systems infected with monero-mining malware*, 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/european-airport-systems-infected-with-monero-mining-malware (visited on 11/08/2019).

[9] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, Apr. 2016.

[10] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. 2011, vol. 66, pp. 37–39.

[11] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, 2012.

[12] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," *2008 Third International Conference on Systems and Networks Communications*, pp. 23–26, 2008.

[13] *A realistic cyber defense dataset (cse-cic-ids2018) - registry of open data on aws*. [Online]. Available: https://registry.opendata.aws/cse-cic-ids2018 (visited on 08/12/2020).

[14] A. Strehl and J. Ghosh, "Cluster ensembles: A knowledge reuse framework for combining multiple partitions," *Journal of Machine Learning Research*, vol. 3, no. Dec, pp. 583–617, 2002.

[15] L. Dias, S. Valente, and M. Correia, "Go with the flow: Clustering dynamically-defined netflow features for network intrusion detection with DynIDS," 2020, in submission.

[16] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Transactions on Neural Networks*, vol. 16, no. 3, pp. 645–678, 2005.

[17] *Windows performance monitor - Microsoft Docs*. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/perfctrs/about-performance-counters (visited on 08/08/2020).

[18] B. Claise, "Cisco systems netflow services export version 9," RFC 3954, Oct. 2004.

[19] D. Draghicescu, A. Caranica, A. Vulpe, and O. Fratu, "Crypto-mining application fingerprinting method," *2018 International Conference on Communications*, pp. 543–546, 2018.

[20] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[21] N. Rahmah and I. S. Sitanggang, "Determination of optimal epsilon (eps) value on DBSCAN algorithm to clustering data on peatland hotspots in Sumatra," in *IOP Conference Series: Earth and Environmental Science*, vol. 31, Feb. 2016.

[22] I. Sharafaldin, A. Gharib, A. H. Lashkari, and A. A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset," *Software Networking*, vol. 2017, no. 1, pp. 177–200, 2017.

[23] G. van Rossum, "Python tutorial release 3.8.1," Tech. Rep., 2020.

[24] W. McKinney *et al.*, "Data structures for statistical computing in python," in *Proceedings of the 9th Python in Science Conference*, vol. 445, 2010, pp. 51–56.

Antena Dual-Band para UAV

Ricardo Figueiredo Gomes de Oliveira
Academia Militar
Lisboa, Portugal
oliveira.rfg@exercito.pt

António Carlos de Campos Simões Baptista
Instituto Superior Técnico
Lisboa, Portugal
baptista@tecnico.ulisboa.pt

Maria João Marques Martins
Academia Militar
Lisboa, Portugal
mariajoaomartins2@gmail.com

Resumo — **A Força Aérea Portuguesa, através do Programa de Investigação e Tecnologia em Veículos Aéreos Não Tripulados (UAV), desenvolve tecnologia com o objetivo de melhorar as capacidades desta tipologia de veículos. Nesse contexto, surge a necessidade de otimizar o seu sistema de transmissão, atendendo aos requisitos propostos pela Força Aérea. Este artigo apresenta os princípios teóricos considerados no dimensionamento de uma antena microstrip de banda dupla. A operação em banda dupla com um patch retangular pode ser alcançada pela gravação de fendas no plano terra da antena (Defect Ground Structures) ou na superfície do patch metálico. Além disso, são apresentados os resultados da simulação obtidos. Estas foram realizadas para o substrato RT Duroid 5870. O objetivo final é dimensionar uma antena patch de banda dupla (1,33 GHz e 5 GHz) para a transmissão de um canal de vídeo. O melhor resultado de simulação foi obtido para a inserção de ranhuras num patch alimentado por inset-feed. O trabalho de simulação no desenvolvimento da antena foi feito usando o COMSOL Multiphysics.**

I. INTRODUÇÃO (ESTILO: HEADING/TÍTULO 1)

O emprego de Veículos Aéreos Não Tripulados (UAV) em Teatros de Operações tem crescido ao longo do tempo, principalmente pela flexibilidade, alcance operacional e por serem capazes de reunir Informações sem colocar vidas humanas em risco [1].

Para cumprir as suas missões, o Exército Português e a Força Aérea Portuguesa começaram a adquirir e a desenvolver plataformas de UAV. No caso da Força Aérea, isso foi realizado no âmbito do Projeto de Investigação e Tecnologia em Veículos Aéreos Não-Tripulados - PITVANT.

Este trabalho surge no contexto do aprimoramento dos sistemas de UAV das Forças Armadas. O progresso tecnológico impõe novos desafios a esses sistemas, surgindo daí a necessidade de melhorar os seus sistemas de comunicação. O principal desafio associado ao uso de UAV é a necessidade de *links* de dados para controlar o voo, monitorar a aeronave e transmitir os dados recolhidos pelos sensores da mesma.

O objetivo principal deste trabalho é a análise teórica, projeto e simulação de uma antena planar direcional de banda dupla, que opera nas frequências de 1,33 GHz e 5 GHz. Os requisitos operacionais da antena são uma largura de banda de 8 MHz em ambas as bandas de frequência, um ganho maior que 3 dB e um coeficiente de reflexão inferior a -10 dB. Este trabalho surge no seguimento das dissertações realizadas pelo Tenente Pedro Marques, pelo Tenente António Carneiro e pelo Tenente João Pinto [2][3][4].

II. ESTADO DA ARTE

A. *Sistemas de Comunicação*

A comunicação entre um UAV e a sua Estação Terrestre requer dois *links* de dados: o *uplink*, que garante a transmissão dos parâmetros de controlo de voo, e o *downlink*, no qual o UAV transmite a informação recolhida pelos seus sensores de bordo [5].

Existem três formas diferentes de estabelecer a comunicação entre o UAV e a Estação Terrestre, sendo elas as seguintes: por laser, por fibra ótica ou por rádio. Qualquer um destes métodos deve transmitir dados de forma segura e confiável e a uma taxa adequada [5].

A comunicação do laser é limitada pelo seu alcance, enquanto os links de fibra ótica são usados apenas em alguns cenários de voo de baixa altitude. Os *links* de rádio são o principal método implantado em sistemas de comunicação de UAV [5].

B. *Antenas de UAV*

Em relação aos UAV, os requisitos operacionais ditam o dimensionamento das antenas, tendo como fator limitante as características aerodinâmicas da mesma.

As antenas mais comuns neste tipo de aplicação assumem a forma de um chicote, lâmina ou antena planar. As antenas de chicote (normalmente monopólo) tendem a dobrar a altas velocidades e têm ganhos reduzidos. As antenas do tipo lâmina apresentam melhor desempenho aerodinâmico, porém tanto as antenas do tipo chicote como as antenas do tipo lâmina apresentam um nulo de radiação associado ao elemento metálico da antena [6].

As antenas planas permitem maior versatilidade nas suas características de irradiação, mantendo um bom desempenho aerodinâmico e tendo como principal desvantagem uma largura de banda menor quando comparada às antenas monopólo tradicionais [7].

III. ANTENAS PLANARES

As antenas planares são uma solução comum para aplicações em que as dimensões, custo, desempenho e perfil aerodinâmico da antena são fatores limitadores. Estas antenas são bastante versáteis em termos de frequência de ressonância, polarização e impedância, além de terem um custo de fabricação relativamente baixo e de permitirem uma grande adaptabilidade a diversos tipos de superfícies de montagem [7].

O seu peso e tamanho reduzidos permitem uma instalação simples na asa do UAV, com mínima interferência aerodinâmica, o que as torna adequadas para este tipo de aplicação.

A. *Características Básicas*

As antenas planares convencionais consistem num *patch* de metal com espessura $t \ll \lambda_0$ (onde λ_0 representa o comprimento de onda em espaço livre) colocado no topo de um substrato dielétrico, que por sua vez é colocado no topo de um plano metálico (plano terra). O substrato dielétrico tem, tipicamente, uma espessura de $h \ll \lambda_0$ (normalmente $0{,}003\lambda_0 \leq h \leq 0{,}05\lambda_0$). O substrato dielétrico possui uma constante dielétrica (ϵ_r), cujo valor depende do tipo de substrato utilizado, mas geralmente está compreendida no intervalo $2{,}2 \leq \epsilon_r \leq 12$ [7].

B. *Modelo da Linha de Transmissão*

A existência de meios dielétricos não homogéneos e a configuração geométrica dos elementos da antena tornam complexa a análise deste tipo de antenas. Portanto, é necessário recorrer a modelos analíticos para simplificar a compreensão das características de funcionamento da antena [7].

Um *patch* retangular pode ser descrito por uma linha de transmissão *microstrip* que, por sua vez, pode ser descrita por um guia de onda retangular com paredes que são condutores magnéticos perfeitos. Como o comprimento (L) e a largura (W) do *patch* são dimensões finitas, existem radiações espúrias nas extremidades do *patch* [7].

Este efeito faz com que algumas das ondas se propaguem no *patch* e outras no ar, sendo portanto necessário definir uma constante dielétrica efetiva (ϵ_{reff}), que é dada por [7]:

$$\epsilon_{reff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2}\left[1 + 12\frac{h}{W}\right]^{-\frac{1}{2}}, \quad for\ W/h > 1 \quad (1)$$

O comprimento de onda no guia é descrito por [7]:

$$\lambda_g = \frac{\lambda}{\epsilon_{reff}} \quad (2)$$

Esta cavidade é ressonante quando o comprimento do *patch* é aproximadamente igual a $\lambda_g/2$. A existência de radiações espúrias nas extremidades do *patch* provoca um aumento do comprimento elétrico do mesmo. Este aumento (ΔL) deve ser tido em conta no dimensionamento do *patch* [7]:

$$L = L_{eff} - 2\Delta L \quad (3)$$

$$L_{eff} = \frac{c_0}{2f_r\sqrt{\epsilon_{reff}}} \quad (4)$$

$$\Delta L = 0.412h\frac{\left(\epsilon_{reff} + 0.3\right)\left(\frac{W}{h} + 0.264\right)}{\left(\epsilon_{reff} - 0.258\right)\left(\frac{W}{h} + 0.8\right)} \quad (5)$$

onde c_0 representa a velocidade da luz em espaço livre.

A largura do *patch* depende da frequência de ressonância e do valor da constante dielétrica do substrato, sendo descrita por [7]:

$$W = \frac{1}{2f_r\sqrt{\mu_0\varepsilon_0}}\sqrt{\frac{2}{\epsilon_r + 1}} = \frac{c_0}{2f_r}\sqrt{\frac{2}{\epsilon_r + 1}} \quad (6)$$

A frequência de ressonância do modo dominante TM_{010} varia com o comprimento do *patch* e é dada pela seguinte expressão [7]:

$$(f_r)_{010} = \frac{1}{2L\sqrt{\epsilon_r}\sqrt{\mu_0\epsilon_0}} = \frac{c_0}{2L\sqrt{\epsilon_r}} \quad (7)$$

onde μ_0 é a permeabilidade magnética do vácuo e ϵ_0 é a permitividade elétrica do vácuo.

No entanto, como a expressão (7) não tem em conta os efeitos introduzidos pelas radiações espúrias, esta expressão é modificada para [7]:

$$(f_{rc})_{010} = \frac{1}{2L_{eff}\sqrt{\epsilon_{reff}}\sqrt{\mu_0\epsilon_0}} = q\frac{c_0}{2L\sqrt{\epsilon_r}} \quad (8)$$

onde q é o fator de efeito de bordo [7]:

$$q = \frac{(f_{rc})_{010}}{(f_r)_{010}} \quad (9)$$

O aumento do comprimento elétrico da antena é equivalente à introdução de duas ranhuras irradiantes, que podem ser descritas pela sua admitância equivalente. Numerando estas ranhuras como 1 e 2, a admitância de uma ranhura é descrita por [7], (figura 1):

$$Y_1 = G_1 + jB_1 \quad (10)$$

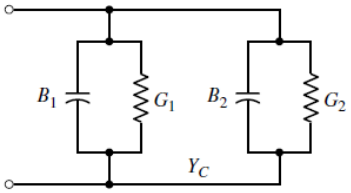


Figura 1: Circuito equivalente da linha de transmissão [7]

A condutância (G) e a susceptância (B) de uma única ranhura de largura finita (W) são dadas por [7]:

$$G_1 = \frac{W}{120\lambda_0}\left[1 - \frac{1}{24}(k_0h)^2\right], \frac{h}{\lambda_0} < \frac{1}{10} \quad (11)$$

$$B_1 = \frac{W}{120\lambda_0}[1 - 0{,}636\ln(k_0h)], \frac{h}{\lambda_0} < \frac{1}{10} \quad (12)$$

Como ambas as ranhuras são idênticas, verifica-se o seguinte [7]:

$$Y_2 = Y_1, G_2 = G_1, B_2 = B_1 \quad (13)$$

A potência irradiada é dada por [7]:

$$P_{rad} = \frac{|V_0|^2}{2\pi\eta_0}\int_0^{\pi}\left[\frac{\sin\left(\frac{k_0 W}{2}\cos\theta\right)}{\cos\theta}\right]^2 \sin^3\theta\, d\theta \quad (14)$$

A condutância de uma ranhura também pode ser descrita por [7]:

$$G_1 = \frac{I_1}{120\pi^2} \quad (15)$$

onde:

$$I_1 = \int_0^{\pi}\left[\frac{\sin\left(\frac{k_0 W}{2}\cos\theta\right)}{\cos\theta}\right]^2 \sin^3\theta\, \mathrm{d}\theta = -2 + \cos(X) + XS_i(X) + \frac{\sin(X)}{X} \quad (16)$$

e:

$$X = k_0 W \quad (17)$$

A admitância de ressonância de entrada é dada por [7]:

$$Y_{in} = 2G_1 \quad (18)$$

Quando a antena está adaptada, a ressonância de entrada tem apenas parte real. Desprezando os efeitos de acoplamento, esta é descrita por [7]:

$$Z_{in} = \frac{1}{Y_{in}} = R_{in} = \frac{1}{2G_1} \quad (19)$$

Considerando os efeitos de acoplamento, modifica-se a expressão anterior para [7]:

$$R_{in} = \frac{1}{2(G_1 \pm G_{12})} \quad (20)$$

onde G_{12} representa a condutância mútua entre as duas ranhuras [7]:

$$G_{12} = \frac{1}{120\pi}\int_0^{\pi}\left[\frac{\sin\left(\frac{k_0 W}{2}\cos\theta\right)}{\cos\theta}\right]^{-2} J_0(k_0 L\sin\theta)\sin^3\theta\, d\theta \quad (21)$$

onde J_0 é a 1ª função de Bessel de 1ª espécie e ordem 0.

Quando a antena é alimentada por uma linha *microstrip*, a impedância característica da linha é descrita por [7]:

$$Z_c = \frac{60}{\sqrt{\epsilon_{reff}}}\ln\left[\frac{8h}{W_0} + \frac{W_0}{4h}\right] \quad (22)$$

quando $W_0/h \leq 1$, e:

$$Z_c = \frac{120\pi}{\sqrt{\epsilon_{reff}}\left[\frac{W_0}{h} + 1{,}393 + 0{,}667\ln\left(\frac{W_0}{h} + 1{,}444\right)\right]} \quad (23)$$

quando $W_0/h > 1$.

Sabendo Z_c, a largura da linha de alimentação pode ser calculada com recurso às expressões (22) ou (23).

A resistência de entrada de um dado ponto da linha de alimentação (y_0) é dada por [7]:

$$R_{in}(y = y_0) = \frac{1}{2(G_1 \pm G_{12})}\cos^2\left(\frac{\pi}{L}y_0\right) = R_{in}(y = 0)\cos\left(\frac{\pi}{L}y_0\right) \quad (24)$$

A resolução da expressão (24) em ordem a y_0 permite encontrar o ponto de alimentação, ou seja, o ponto onde a impedância de entrada da antena está adaptada à impedância da linha de alimentação [7], (figura 2).

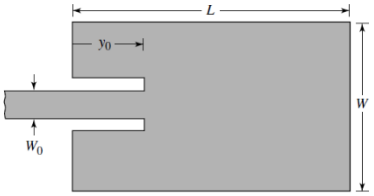


Figura 2: *Patch* rectangular alimentado por *inset-feed* [7]

C. *Funcionamento em Dual-Band*

Uma das principais desvantagens das antenas planares é largura de banda estreita. Nalguns cenários, pode ser necessária uma largura de banda maior para a transmissão simultânea de canais diferentes. Neste caso, o funcionamento em dupla frequência pode ser uma solução para o problema de largura de banda. O principal desafio no processo de projeto de uma antena deste tipo é a obtenção de características de radiação semelhantes nas duas bandas de frequência, principalmente quando o rácio entre frequências é elevado [8].

Neste trabalho, foram analisadas teoricamente e posteriormente simuladas duas técnicas para o funcionamento em dupla frequência, sendo elas a introdução de *slots* no *patch* metálico e a introdução de *slots* no plano terra.

IV. Resultados de Simulação

Nesta secção apresentam-se os resultados da simulação da configuração da antena que permitiu cumprir um maior número dos pré-requisitos definidos. Esta configuração corresponde a um *patch* retangular com ranhuras alimentado por *inset-feed*.

Os resultados de simulação foram obtidos com recurso ao COMSOL Multiphysics. O substrato dielétrico utilizado nas simulações é o RT Duroid 5870, que tem uma constante dielétrica de $\epsilon_r = 2.33$ e uma espessura de $h = 1.575\ [mm]$ [9], (figura 3).

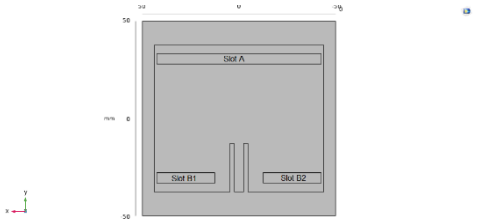


Figura 3: Geometria do *patch*

TABELA I
DIMENSÕES DA ANTENA

PARÂMETRO	Valor [mm]
Comprimento do substrato	100.00
Largura do substrato	100.00
Largura do patch (W)	87.50
Comprimento do patch (L)	75.56
Ponto de Inset Feed (y_0)	24.93
Largura da linha de alimentação (w_0)	4.71
Comprimento do Slot A (L_{SA})	5.40
Largura do Slot A (W_S)	85.00
Comprimento do Slot B (L_{SB})	5.00
Largura do Slot B (W_{SB})	30.00
Distância do Slot A à extremidade do patch (D_{AE})	4.44
Distância do Slot B à extremidade do patch (D_{BE})	4.53
Distância ente o Slot B1 e o Slot B2 (D_{SB})	25.00

A primeira frequência de ressonância ocorre para $f_r = 1.45\ GHz$, com coeficiente de reflexão $S_{11} = -8.89\ dB$ e uma largura de banda de 16 MHz para $S_{11} = -3\ dB$. No processo de otimização não foi possível obter um valor final que permitisse cumprir em simultâneo para ambas as frequências os requisitos operacionais previamente definidos. Na banda de frequência superior ($f_r = 5\ GHz$), a antena tem uma largura de banda de 80.7 MHz para $S_{11} = -10\ dB$ (Figura 4).

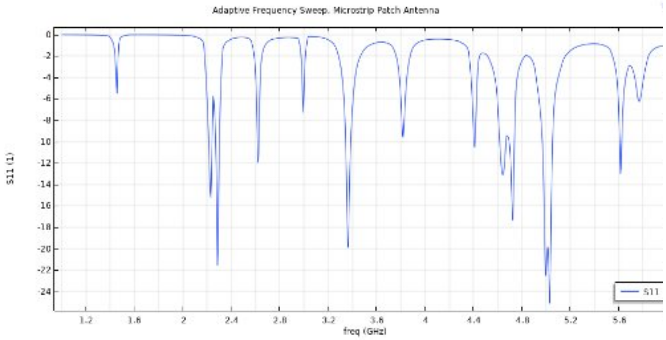


Figura 4: Coeficiente de Reflexão, S11 (dB)

Os resultados que a seguir se apresentam foram obtidos para as frequências de ressonância de $f_r = 1.45\ GHz$ e $f_r = 5\ GHz$. Na banda de frequência inferior, a distribuição do campo elétrico demonstra perturbações mínimas, correspondendo à distribuição esperada para o modo dominante (Figura 5). Na banda de frequência superior, a distribuição do campo elétrico permite verificar a condição de circulação de corrente em torno dos *slots* inseridos na superfície do *patch* (Figura 6).

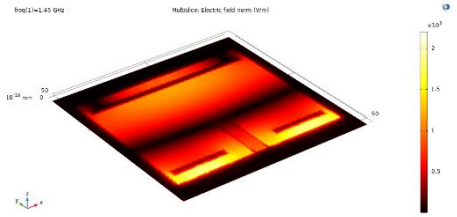


Figura 5: *Distribuição do Campo Elétrico* ($f_r = 1.45\ GHz$)

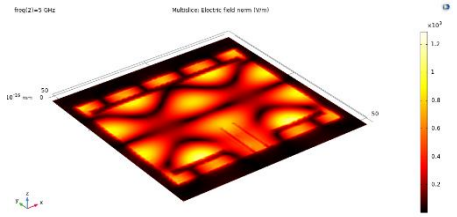


Figura 6: *Distribuição do Campo Elétrico* ($f_r = 5\ GHz$)

A principal vantagem deste tipo de estrutura advém das suas características de irradiação. Como se verifica nos diagramas de radiação (Figura 7, Figura 8, Figura 9 e Figura 10), nas duas bandas de frequência verifica-se a existência de um máximo do diagrama de radiação na direção ortogonal ao plano de colocação do *patch*, tendo um valor de diretividade de 7.16 dB para $f_r = 1.45\ GHz$ e de 11.57 dB para $f_r = 5GHz$.

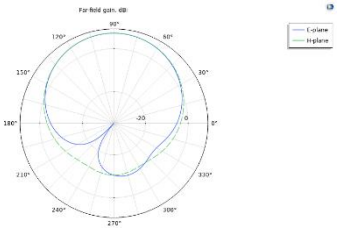


Figura 7: *Diagrama de Radiação* ($f_r = 1.45\ GHz$)

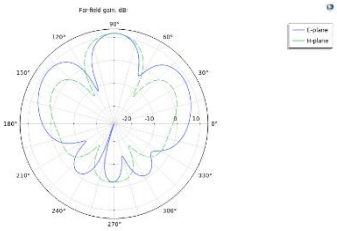


Figura 8: *Diagrama de Radiação* ($f_r = 5\ GHz$)

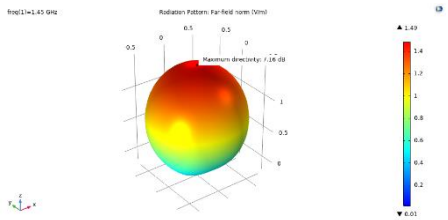


Figura 9: Diagrama de Radiação 3D ($f_r = 1.45\ GHz$)

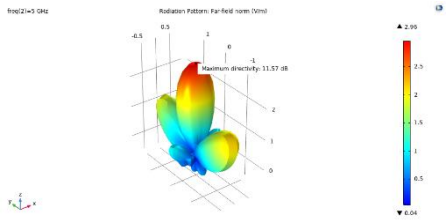


Figura 10: Diagrama de Radiação 3D ($f_r = 5\ GHz$)

V. CONCLUSÕES

Este artigo tinha como objetivo o projeto e simulação de uma antena planar diretiva que operasse em banda dupla e que cumprisse requisitos de largura de banda, ganho e coeficiente de reflexão previamente definidos e utilizando o substrato RT Duroid 5870. Em primeiro lugar, realizou-se uma análise teórica com o objetivo de compreender os princípios de funcionamento das antenas planares e das antenas de banda dupla. Foram testadas várias configurações geométricas para a antena. Destas, aquela que permitiu obter os resultados com melhor aproximação aos resultados esperados foi o *patch* retangular alimentado por *inset-feed* e com inserção de *slots* no mesmo.

O protótipo final, resultante do processo de dimensionamento, simulação e otimização opera nas frequências de 1.45 GHz e 5 GHz (rácio de frequências de 3.44), tendo, para a banda inferior, 16 MHz de largura de banda e 7.16 dB de diretividade e, para a banda superior, 80.7 MHz de largura de banda e 11.57 dB de diretividade.

REFERÊNCIAS BIBLIOGRÁFICA

[1] B. Soares, «UAS e Reconhecimento Terrestre: contributos para um modelo de instrução e treino.», Academia Militar, 2013.

[2] P. M. M. Marques, «Antenas de comunicações para UAV's», Instituto Superior Técnico, 2016.

[3] A. F. A. Carneiro, «"Smart" antena para aplicação em UAV's», Instituto Superior Técnico, 2017.

[4] J. M. N. Pinto, «Otimização do sistema de controlo de antenas para UAV», Academia Militar, 2018.

[5] R. Austin, *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. 2010.

[6] K. P. Valavanis e G. J. Vachtsevanos, *Handbook of unmanned aerial vehicles*. 2015.

[7] C. A. Balanis, *Antenna Theory; Analysis and Design*. Wiley, 2016.

[8] S. Maci e G. Biffi Gentili, «Dual-frequency patch antennas», *IEEE Antennas Propag. Mag.*, 1997, doi: 10.1109/74.646798.

[9] Rogers Corporation, «RT/duroid® 5870 /5880». 2017.

Reconhecimento Facial Através de Aprendizagem Profunda em Imagens Multiespectrais

Luis Lopes Chambino
Academia Militar, Lisboa
Instituto Superior Técnico (IST), Universidade de Lisboa
chambino.lcl@exercito.pt

José Silvestre Silva
Academia Militar, Lisboa
CINAMIL, Lisboa
LIBPhys-UC, Coimbra
jose.silva@academiamilitar.pt

Alexandre Bernardino
Instituto Superior Técnico (IST), Universidade de Lisboa
Instituto de Sistemas e Robótica (ISR), Portugal
alex@isr.tecnico.ulisboa.pt

Resumo – **O reconhecimento facial é um método de identificação ou autenticação da identidade de indivíduos através dos seus rostos. Atualmente, os sistemas de reconhecimento facial que utilizem imagens multiespectrais obtêm melhores resultados, em comparação com aqueles que utilizem apenas imagens da banda espectral do visível. Neste trabalho, é proposto um detetor de pele a ser aplicado num módulo de deteção de falsificação e uma arquitetura que utiliza múltiplas redes neurais convolucionais profundas e imagens multiespectrais para efetuar o reconhecimento facial. É realizado um estudo com o objetivo de avaliar o desempenho da adaptação de diversas camadas da rede neural base. Adicionalmente, foi realizado um segundo estudo para avaliar o desempenho das Máquinas Vetoriais de Suporte (SVM) e dos classificadores k-Nearest Neighbor para classificar os conjuntos de características multidimensionais obtidas através da arquitetura proposta. Os resultados experimentais nas bases de dados multiespectrais Tufts e CASIA NIR-VIS 2.0 indicam um desempenho competitivo no reconhecimento facial obtendo uma pontuação de *rank-1* de 99,7% e 99,8%, respetivamente.**

I. INTRODUÇÃO

Nos dias de hoje, muitos dos sistemas biométricos de reconhecimento facial funcionam na banda espectral do visível. Estes possuem diversos obstáculos, tais como: oclusões, variação de poses, cooperação da pessoa e, o mais problemático, alterações na luminosidade. Como resultado, é necessário complementar os atuais sistemas de reconhecimento facial, com a utilização de outros sensores biométricos (e.g., impressão digital ou íris) ou com outras bandas espectrais, a fim de minimizar estes problemas [1] [2].

Na Tabela 1 estão indicadas as bandas espectrais mais utilizadas e aplicadas em reconhecimento facial multiespectral.

TABELA 1. INTERVALOS ESPECTRAIS UTILIZADOS EM RECONHECIMENTO FACIAL [4].

Nome da Banda Espectral	Comprimento de Onda (μm)
Visível	0,38 – 0,75
Near Infrared (NIR)	0,75 – 1,40
Short Wavelength Infrared (SWIR)	1,40 – 3,00
Mid Wavelength Infrared (MWIR)	3,00 – 8,00
Long Wavelength Infrared (LWIR)	8,00 – 15,00

A utilização do espectro eletromagnético infravermelho, nomeadamente as bandas espectrais *Near Infrared* (NIR), *Short Wavelength Infrared* (SWIR), *Mid Wavelength Infrared* (MWIR) e *Long Wavelength Infrared* (LWIR), têm sido utilizadas com sucesso em sistemas de reconhecimento facial, como complemento do espectro visível [1] [3]. A estes sistemas, que utilizam mais do que uma banda espectral, denominam-se de multiespectrais.

A utilização do espectro eletromagnético infravermelho em sistemas de reconhecimento facial possui diversas vantagens quando comparada com o espectro eletromagnético do visível. O infravermelho é impercetível ao olho humano e, ao mesmo tempo, menos sensível às diferenças de luminosidade. Por exemplo, as câmaras noturnas utilizadas na vigilância por vídeo utilizam *LEDs*, com emissão no espectro infravermelho de forma a iluminar o local, e realizar vigilância noturna sem que as pessoas tenham conhecimento [5].

Dado que as bandas espectrais NIR e SWIR estão próximas da banda espectral do visível, é possível adaptar os métodos de aprendizagem automática treinados com imagens do espectro visível. As bandas espectrais MWIR e LWIR (também conhecida por térmica) permitem a utilização de sistemas de reconhecimento facial à noite, quando a luminosidade é reduzida ou mesmo nula.

Este trabalho está organizado da seguinte forma: na Secção II é efetuado o estudo do estado da arte sobre métodos de reconhecimento facial multiespectral, das métricas mais utilizadas e das bases de dados multiespectrais públicas; na Secção III é definida e proposta a metodologia para a deteção facial multiespectral; na Secção IV são indicadas as bases de dados multiespectrais utilizadas, apresentados os resultados obtidos e a sua respetiva análise e discussão; a Secção V é efetuada a conclusão tendo por base os resultados e discussão apresentados na secção anterior, e ainda sugeridos possíveis trabalhos futuros.

II. ESTADO DA ARTE

Nesta secção é apresentado uma revisão sistemática do reconhecimento facial multiespectral, sendo descritos de forma breve os métodos utilizados.

Para efetuar a revisão sistemática foi utilizado a base de dados *Web of Sciences*. Foram considerados artigos publicados de 2000 até junho de 2020 em revistas

internacionais com fator de impacto; trabalhos publicados em conferências não foram considerados. O produto da pesquisa foram 283 artigos publicados em 132 revistas internacionais científicas com fator de impacto.

Para este estado da arte foi necessário efetuar uma segunda seleção mais refinada. Como tal, foram considerados apenas os artigos que efetuavam reconhecimento facial ou deteção facial com duas ou mais bandas espectrais (e.g., VIS-NIR, VIS-LWIR, VIS-NIR-LWIR, NIR-LWIR, entre outras possíveis combinações), reduzindo assim o número de artigos para 47. Estes artigos foram considerados os mais relevantes para a análise em questão.

Foi realizada uma análise destes artigos tendo em consideração as bases de dados multiespectrais e métricas de avaliação utilizadas, tendo sido concluído que a base de dados mais utilizada é a CASIA NIR-VIS 2.0 [6], a qual foi empregue 15 vezes nos artigos analisados.

A métrica mais utilizada para comparar resultados entre metodologias, quando utilizada a mesma base de dados, foi o *rank-1*.

Através da análise sistemática foi possível destacar cinco métodos principais utilizados no reconhecimento facial multiespectral: reconhecimento por características, subespaço acoplado, síntese, fusão e redes neurais profundas. A metodologia mais utilizada corresponde às redes neurais profundas, tendo sido empregue por 32% dos trabalhos relevantes analisados.

Na Figura 1 está ilustrado a distribuição dos métodos de reconhecimento facial por ano de publicação. Da análise deste gráfico, é possível concluir a predominância dos artigos que utilizam o método de fusão de imagens em reconhecimento facial multiespectral até 2016 inclusive. A partir de 2017, o método de fusão foi superado pelo método de redes neurais profundas, uma vez que este produz resultados superiores.

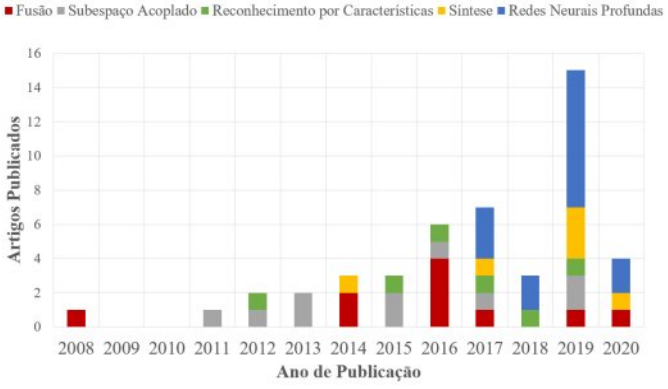


Fig. 1. Distribuição dos métodos por ano de publicação.

A Figura 2 apresenta um gráfico caixa de bigodes que resume o desempenho obtido nos artigos estudados para cada método. Tal estudo permite comparar o nível de desempenho em cada método.

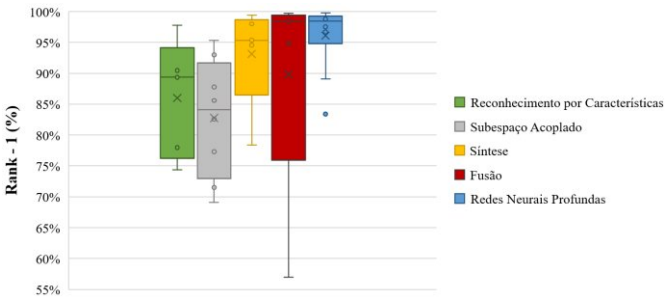


Fig. 2. Desempenho obtido nos métodos descritos nos artigos analisados.

Como é possível observar pela Figura 2 as redes neurais profundas obtêm os melhores resultados, justificando a procura e criação e novas redes neurais profundas, sendo esta área de investigação muito ativa (também corroborado pela Figura 1, na coluna ano 2019).

III. METODOLOGIA

Neste capítulo é apresentada a metodologia adotada para a implementação de um sistema de reconhecimento facial multiespectral. Na Figura 3 está ilustrado o fluxograma da metodologia proposta.

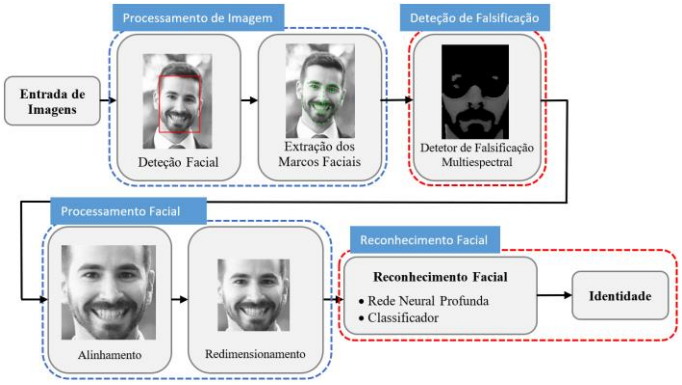


Fig. 3. Fluxograma da metodologia proposta.

A metodologia proposta inicia-se pela obtenção de imagens multiespectrais (i.e., visível e infravermelho).

O passo seguinte é a conversão das imagens para a gama de cores do cinzento, deteção das faces humanas e a extração dos marcos faciais (e.g. olhos, nariz, boca) na imagem. O módulo encarregue por efetuar esta tarefa é o módulo de processamento de imagem.

O sistema de reconhecimento facial proposto inclui um módulo para detetar e avisar potenciais ataques de falsificação, denominado de módulo de deteção de falsificação. Este módulo tira partido de todas as imagens multiespectrais disponíveis para efetuar a deteção da pele, prevenindo assim o sistema de reconhecimento facial de possíveis ataques.

No módulo seguinte é realizado o processamento facial, onde são utilizados os marcos faciais, obtidos no primeiro módulo (i.e., processamento de imagem), de forma a alinhar a face. Este módulo tem como principal objetivo a

normalização da imagem a inserir na rede neural convolucional profunda (DCNN).

O módulo de reconhecimento facial, extrai um conjunto de características da pessoa a identificar. De seguida, é feita uma classificação da identidade mediante o conjunto de características obtidos anteriormente de forma a obter a identificação da pessoa nas imagens multiespectrais processadas inicialmente no primeiro módulo.

A principal vantagem da arquitetura proposta é permitir a utilização de diversos canais, alocando para cada canal uma banda espectral, ou intervalo espectral (caso se esteja a utilizar vários intervalos espectrais na mesma banda).

A DCNN base utilizada em cada canal é a LightCNN [7]. A rede base possui como entrada imagens na gama de cores do cinzento, com tamanho de 128x128 pixéis, e como saída, um conjunto de características, representativo da identidade da pessoa, de 256 dimensões. São adaptadas camadas distintas da LightCNN [7] de forma a adequar o modelo utilizado a uma banda espectral diferente do visível.

Tendo como ponto de partida a LightCNN, foi adicionada no fim da rede uma nova camada, denominada de última camada ligada (UCL), tendo como entrada um conjunto de características com dimensões de *N* x *256*, que através de uma transformação linear produz um conjunto de características de 256-dimensões.

Na Figura 4 está ilustrado um caso genérico de utilização da rede proposta que utiliza *N* canais, estando assinalado a verde as camadas que são adaptadas, e a azul as camadas que não são adaptadas. O *Canal 0*, atribuído à banda espectral do visível, não é adaptado. Ao reutilizar-se os pesos de uma DCNN já pré treinada para reconhecimento facial numa base de dados com um número elevado de imagens faciais, é evitado um possível sobre ajuste, dado o número limitado de imagens multiespectrais utilizadas na fase de treino [8].

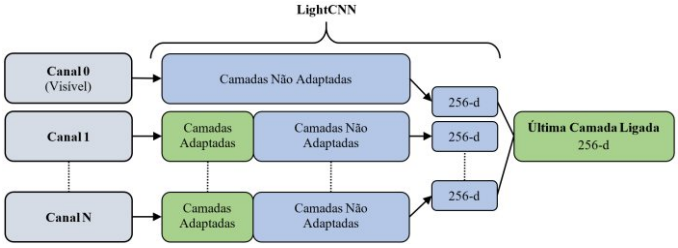


Fig. 4. Esquema da arquitetura da DCNN proposta.

IV. Resultados e Discussão

Nesta secção serão descritas as bases de dados multiespectrais utilizadas, os testes efetuados com a finalidade de aferir qual as camadas a serem adaptadas e quais os classificadores que devem ser utilizados.

A. *Bases de Dados Multiespectrais*

De forma a avaliar corretamente os algoritmos incluídos na metodologia proposta foram utilizados três bases de dados multiespectrais: a Tufts [9], a CASIA NIR-VIS 2.0 [6] e um conjunto de imagens adquiridas na Academia Militar (AM).

A base de dados Tufts [9] é composta por três bandas espectrais, VIS NIR e LWIR. Após a sua limpeza esta ficou com um total de 7 675 imagens faciais de 109 pessoas, tendo sido excluído 53 imagens faciais e 4 pessoas.

A CASIA NIR-VIS 2.0 [6] é composta por duas bandas espectrais, VIS e NIR, constituída por 17 489 imagens faciais de 715 pessoas.

A base de dados elaborada na AM é composta por três bandas espectrais, VIS, SWIR e LWIR. Esta base de dados foi contruída para ser utilizada durante a fase de experimentação do módulo de deteção de falsificação. Durante a construção da base de dados foram utilizadas diversas máscaras, com o intuito de simbolizar diferentes ataques de falsificação. Na Figura 5 estão ilustradas algumas das imagens presentes na base de dados multiespectral elaborada na AM.



Fig. 5. Exemplo de imagens da base de dados multiespectral construída na Academia Militar.

B. *Deteção de Falsificação*

No módulo de deteção de falsificação foi empregue um classificador de pele que tira proveito de todas as bandas espectrais disponíveis de forma a efetuar uma correta classificação de pele.

O classificador efetua uma classificação ao nível do pixel. Numa primeira etapa é determinada a diferença normalizada, $d[g_a, g_b]$, para todas as combinações possíveis de imagens faciais, tendo em conta os canais disponíveis, usando a expressão:

$$d[g_a, g_b] = \left(\frac{g_a - g_b}{g_a + g_b}\right) \quad (1)$$

em que g corresponde ao valor da intensidade do pixel para o canal *a* e *b*, com $1 \leq a \leq n$ e $a \leq b \leq n$, onde *n* corresponde ao número de canais disponíveis no módulo de deteção de falsificação. A diferença normalizada resulta em valores de $-1 \leq d[g_a, g_b] \leq +1$.

Obtida a diferença normalizada é possível agora aplicar o classificador de pele que utiliza os valores da diferença normalizada de forma a classificar os pixéis como pele ou não pele.

A gama de valores escolhida para classificar como pele ou não pele, foi definida empiricamente. Os valores para pele estão compreendidos entre:

$$(76, 51, 65) < (d[g_1, g_2], d[g_1, g_3], d[g_2, g_3]) < (131, 140, 127)$$

Na Figura 6 está ilustrado o "antes" (imagem à esquerda) e o "produto final" após a aplicação do classificador proposto (imagem à direita) durante a utilização de uma máscara na zona ocular. Nesta figura, a região a preto corresponde ao que foi classificado como não sendo não pele.



Fig. 6. O resultado final após aplicação do classificador proposto. Imagem original (esquerda) e imagem após classificador (direita).

Para validar a nossa proposta, foram utilizados outros dois classificadores, o YCbCr e HSV. Na avaliação foi tido em consideração o número de marcos faciais, obtidos no módulo de processamento de imagem, que foram incorretamente classificados como pele. Após analise dos resultados experimentais, é possível afirmar que os classificadores de pele que utilizam a banda espectral do visível tem dificuldades em diferenciar a pele real (i.e., pele humana) de pele falsificada, proveniente das máscaras de falsificação utilizadas.

Quando utilizados estes classificadores de pele, do visível, como método de deteção de falsificação, a taxa de deteção de falsificação (i.e., quando este consegue detetar corretamente um ataque de falsificação) foi de 13%. Resultado justificado pelo facto de os classificadores utilizados não serem capazes de efetuar uma correta diferenciação da pele humana de a máscara.

Quando comparados com o classificador que utiliza as três bandas espectrais, este obtém melhores resultados. A taxa de deteção de falsificação para este foi de 83%. Comparativamente com os classificadores anteriores, este consegue efetuar uma correta diferenciação da máscara, como é possível observar na Figura 6.

C. Reconhecimento Facial

Depois de efetuado o processamento das imagens faciais das bases de dados (i.e., deteção e alinhamento facial), é necessário extrair o conjunto de características dessas mesmas imagens, a fim de classificar a identidade da pessoa presente nas imagens.

Foram efetuados diversos testes para averiguar quais as camadas mais adequadas para o treino da rede neuronal; que valores devem ser tomados nos hiperparâmetros dos classificadores; e, após escolha dos melhores hiperparâmetros, determinar o melhor classificador para classificar o conjunto de características.

As imagens de cada base de dados foram divididas em três conjuntos: treino, validação e teste. A percentagem de imagens para o conjunto de treino foi de 64%, para o conjunto de validação 16%, e por fim, 20% para o conjunto de teste. Esta partição de cada base de dados foi uma divisão estratificada de forma a que cada pessoa tem um número equitativo de imagens faciais suas em cada subconjunto.

1. Procedimento de Treino

Foi utilizado o alargamento de dados para obter um modelo mais generalizado. Nas imagens presentes no conjunto de dados de treino foi utilizado espelhagem aleatória horizontal e um recorte aleatório para redimensionar a imagem numa resolução de 128x128 pixéis (as imagens no início do treino da rede possuem uma resolução de 144x144 pixéis). Para o conjunto de validação foi apenas aplicado um recorte ao centro, para cumprir o requerimento de resolução da LightCNN [7].

2. Camadas Adaptadas

Foi efetuado um teste para estimar quais as camadas adequadas a adaptar na arquitetura da LightCNN [7]. Inicialmente é adaptado apenas a UCL. Esta camada inicialmente não existia na inicial da DCNN, tendo sido implementada posteriormente para que a saída da arquitetura continuasse a ser o conjunto de características de 256-dimensões.

De seguida, as camadas inicias da DCNN são adaptadas (inclusive a UCL) até que todas as camadas da DCNN sejam adaptadas. Em todas as experiências os pesos foram inicializados a partir do modelo inicial da LightCNN [7].

A nomenclatura dos grupos adaptados segue a nomenclatura inicial dos autores da LightCNN [7]. As notações utilizadas na combinação das camadas adaptadas são as seguintes: (i) UCL – apenas a UCL é adaptada, (ii) Conv1-N-UCL ({1-N}+UCL) – adapta as camadas de 1 a N em conjunto com a UCL, e (iii) Todas as Camadas – todas as camadas da LightCNN e a UCL são adaptadas.

O número de épocas durante o procedimento de treino foi de 10 e 30 para as bases de dados Tufts [9] e CASIA NIR-VIS 2.0 [6], respetivamente. Após o treino foram extraídos os conjuntos de características de 256-dimensões das imagens de cada base de dados multiespectral.

Efetuado o treino da DCNN com a adaptação de diversas camadas é possível afirmar que, independentemente da base de dados utilizada, para a métrica *rank-1* obtiveram-se os valores de 99,7% e de 99,8% para as bases de dados Tufts [9] e CASIA NIR-VIS 2.0 [6], respetivamente, para o conjunto das camadas ({1-3}+UCL).

3. Estudo dos Hiperparâmetros

Com o melhor modelo, obtido na secção anterior, foi efetuada a extração dos conjuntos de características de 256-dimensões. Para classificar estes conjuntos foram utilizados os classificadores SVM (com *kernel* linear e RBF) e kNN.

Foi aplicada a validação cruzada estratificada, efetuada 5 vezes para a base de dados Tufts [9] e 4 vezes para a base de dados CASIA NIR-VIS 2.0 [6].

O hiperparâmetro afinado para o classificador SVM-Linear foi o parâmetro de regularização (C) de $10^{-10} \leq C \leq 10^{+5}$ com incrementos de uma década.

Para o classificador SVM-RBF foram afinados os seguintes hiperparâmetros: o parâmetro de regularização (C), de $10^{-4} \leq C \leq 10^{+7}$, e o coeficiente de *kernel* (Υ) de $10^{-10} \leq \Upsilon \leq 10^{+2}$, tendo sido utilizados incrementos de uma década para ambos.

Por último, para o classificador kNN, o hiperparâmetro a afinar foi o número de vizinhos próximos (k). A gama de valores analisada para o hiperparâmetro k foi de $1 \leq k \leq 25$, com incrementos de uma unidade.

Após o estudo observa-se que os classificadores SVM, independentemente do *kernel* utilizado, obtêm a pontuação em *rank-1* superior, obtendo uma pontuação em *rank-1* de 99,89% e 99,86% para as bases de dados Tufts [9] e CASIA NIR-VIS 2.0 [6], respetivamente. É também observável que, o melhor valor para o número de vizinhos, hiperparâmetro da kNN, é igual, independentemente da base de dados multiespectral utilizada.

4. Comparação com o Estado da Arte

Efetuado o estudo dos hiperparâmetros mais adequados para cada classificador, é necessário avaliar o desempenho de cada classificador para o conjunto de teste de cada base de dados multiespectral. Simultaneamente, é efetuado um estudo para diferentes classificações através da utilização de uma curva características de correspondência cumulativa (CMC) para auxiliar na decisão do classificador. Nesta curva são traçados a taxa de identificação no eixo das ordenadas e a *rank-N* no eixo das abcissas.

A partir da utilização dos valores em *rank-1* e dos valores obtidos para diferentes classificações (i.e., curva CMC) é possível aferir qual o melhor classificador para cada base de dados multiespectral.

A metodologia proposta utiliza a DCNN LightCNN [7] como base, adaptando as camadas ({1-3} + UCL), para produzir um conjunto de características de 256-dimensões, que são classificadas posteriormente pelo classificador SVM-Linear.

Resultados usando a Base de Dados Tufts

Após avaliação do conjunto de teste, da base de dados Tufts, com os classificadores (i) SVM-Linear, (ii) SVM-RBF e (iii) kNN, foram obtidos os seguintes valores em *rank-1*: (i) 99,7%, (ii) 99,2% e (iii) 99,2%.

Na Figura 7 está ilustrado a curva CMC, para os três classificadores, para as primeiras dez classificações (i.e., rank-10) para a base de dados Tufts [9].

Realizando uma análise comparativa entre os três classificadores através dos valores em *rank-1*, o classificador SVM-Linear é aquele que obtém os melhores resultados, com uma pontuação em *rank-1* de 99,7%. Comparativamente, os classificadores SVM-RBF e kNN obtiveram ambos o resultado de 99,2%, para o mesmo conjunto de imagens.

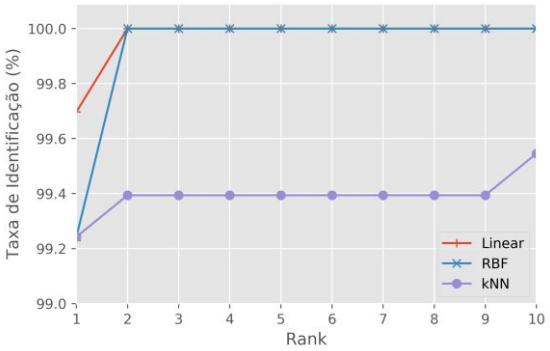


Fig. 7. Curva CMC para os classificadores SVM-Linear, SVM-RBF e kNN, para o conjunto de teste da base de dados multiespectral Tufts.

Na Figura 7 é possível constatar que, para o *rank-2* e independentemente do *kernel* utilizado no classificador SVM, este obtém uma taxa de identificação de 100%. Ou seja, a totalidade das imagens faciais do conjunto de teste foram corretamente identificadas. Comparativamente, o classificador kNN apenas consegue obter uma taxa de identificação de 100% no *rank-102*.

Na Tabela 2 apresenta-se os resultados obtidos pela metodologia proposta e por outras metodologias descritas na literatura. A negrito está salientado o método que obteve melhor pontuação em rank-1.

TABELA 2. RESULTADOS OBTIDOS ATRAVÉS DA METODOLOGIA PROPOSTA QUANDO COMPARADOS COM O ESTADO DA ARTE PARA A BASE DE DADOS TUFTS.

Método	***Rank-1***
TR-GAN [10]	88,7 %
Circular HOG [11]	94,5 %
Metodologia Proposta	**99,7 %**

A Tabela 2 mostra que a metodologia proposta produz um resultado bastante competitivo em comparação com os resultados obtidos por outras metodologias. De realçar que, sendo a base de dados recente, disponibilizada ao público para investigação em 2020, o número de autores que a utilizam ainda é reduzido.

Resultados usando a Base de Dados CASIA NIR-VIS 2.0

Depois de processado o conjunto de teste da base de dados CASIA NIR-VIS 2.0, com os classificadores (i) SVM-Linear, (ii) SVM-RBF e (iii) kNN, foram obtidos os seguintes valores em *rank-1* de (i) 99,8%, (ii) 99,8% e (iii) 99,7%.

Na Figura 8 está ilustrado a curva CMC, para os três classificadores, as primeiras dez classificações para a base de dados CASIA NIR-VIS 2.0.

Numa análise comparativa entre os três classificadores através dos valores de *rank-1*, ambos os classificadores SVM, independentemente do *kernel* utilizado, obtém uma pontuação de 99,8%. Em comparação, o classificador kNN obtém uma pontuação em *rank-1* de 99,7%.

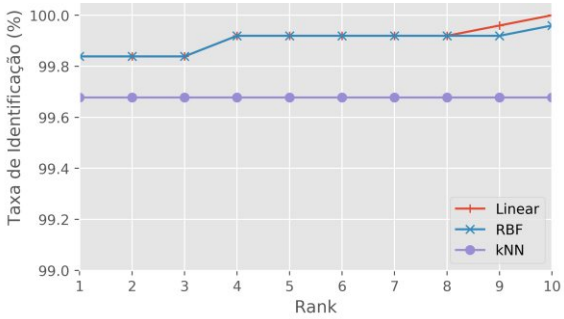


Fig. 8. Curva CMC para os classificadores SVM-Linear, SVM-RBF e kNN, para o conjunto de teste da base de dados CASIA NIR-VIS 2.0.

A Figura 8 mostra que a partir *rank-8* o classificador SVM-Linear obtém uma taxa de identificação superior, quando comparado com o SVM-RBF. Os classificadores SVM-Linear e SVM-RBF obtém uma taxa de identificação de 100% para os *rank-10* e *rank-12*, respetivamente.

Na Tabela 3 encontram-se indicados os resultados obtidos da metodologia proposta e de outras metodologias descritas no estado arte.

TABELA 3. RESULTADOS OBTIDOS ATRAVÉS DA METODOLOGIA PROPOSTA QUANDO COMPARADOS COM O ESTADO DA ARTE PARA A BASE DE DADOS CASIA NIR-VIS 2.0.

Método	***Rank-1***
LightCNN [7]	96,7 %
DSU [8]	96,3 %
CycleGAN [12]	99,4 %
Metodologia Proposta	**99,8 %**

Observando a Tabela 3 verifica-se que a metodologia proposta obtém resultados superiores em *rank-1* quando comparado com os valores de outros métodos descritos no estado da arte. O trabalho mais recente que utiliza a base de dados CASIA NIR-VIS 2.0 é o artigo de Bae *et al.* [12] que obteve uma pontuação em *rank-1* de 99,4%, inferior ao resultado obtido pela metodologia proposta, de 99,8%.

Após uma análise detalhada da Tabela 3, é possível observar que a metodologia base da LightCNN [7] obteve uma pontuação em *rank-1* de 96,7%. Através da metodologia proposta foi possível melhorar significativamente a pontuação em *rank-1* de +3,1%.

V. CONCLUSÕES

Neste trabalho, é proposta uma nova arquitetura para o reconhecimento facial utilizando imagens multiespectrais. A arquitetura produz conjuntos de características de 256-dimensões que representam a identidade de uma pessoa baseada em imagens multiespectral.

Adicionalmente, neste estudo é proposto um detetor de personificação com o objetivo de detetar a utilização de máscaras. O classificador multiespectral obtém melhores resultados quando comparado com o YCbCr ou o HSV.

Foram realizados diversos testes com o intuito de identificar quais as melhores camadas a adaptar da LightCNN e concluiu-se que o melhor resultado corresponde ao conjunto das camadas ({1-3}+UCL). Este estudo permitiu concluir que quanto maior for o número de camadas adaptadas, pior é o resultado final. Os melhores resultados ocorrem da adaptação das camadas iniciais da rede neural.

Para classificar os conjuntos de características de 256-dimensões o classificador SVM com *kernel* linear obteve os melhores valores em *rank-1* quando comparado com os restantes classificadores, para as duas bases de dados multiespectrais utilizadas.

Estudos extensivos nas bases de dados multiespectrais demonstraram a superioridade da metodologia proposta, tendo sido obtidos valores em *rank-1* de 99,7% e 99,8% para as bases de dados multiespectrais Tufts e CASIA NIR-VIS 2.0.

AGRADECIMENTOS

Este trabalho foi apoiado, em parte, pelo Centro de Investigação, Desenvolvimento e Inovação da Academia Militar (CINAMIL) no âmbito do projeto Reconhecimento Facial Multi-Espectral, e pela FCT com o projeto LARSyS - FCT Project UIDB/50009/2020.

REFERÊNCIAS

[1] Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics. Springer, 2011.

[2] R. Munir and R. Khan, "An Extensive Review on Spectral Imaging in Biometric Systems: Challenges and Advancements," Journal of Visual Communication and Image Representation, vol. 65, no. 1, p. 14–26, 2019.

[3] W. Zhang, X. Zhao, J. Morvan, and L. Chen, "Improving Shadow Suppression for Illumination Robust Face Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 3, pp. 611–624, 2019.

[4] A. D'Amico, C. Natale, F. Castro, S. Iarossi, A. Catini, and E. Martinelli, "Volatile Compounds Detection by IR Acousto-Optic Detectors," in Unexploded Ordnance Detection and Mitigation.Springer Netherlands, 2009, pp. 21–59.

[5] S. Hu, N. Short, B. Riggan, M. Chasse, and M. Sarfraz, "Heterogeneous Face Recognition: Recent Advances in Infrared-to-Visible Matching," in International Conference on Automatic Face Gesture Recognition. Washington DC, USA: IEEE, 2017, pp. 883–890.

[6] S. Li, D. Yi, Z. Lei, and S. Liao, "The CASIA NIR-VIS 2.0 Face Database," in IEEE Conference on Computer Vision and Pattern Recognition Workshops. Portland, United States of America: IEEE, 2013, p. 348–353.

[7] X. Wu, R. He, Z. Sun, and T. Tan, "A Light CNN for Deep Face Representation with Noisy Labels," IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2884–2896, 2018.

[8] T. D. Pereira, A. Anjos, and S. Marcel, "Heterogeneous Face Recognition Using Domain Specific Units," IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1803–1816, 2019.

[9] K. Panetta, et al., "A Comprehensive Database for Benchmarking Imaging Systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 3, pp.509–520, 2020.

[10] L. Kezebou, V. Oludare, K. Panetta, and S. Agaian, "TR-GAN: Thermal to RGB Face Synthesis with Generative Adversarial Network for Cross-Modal Face Recognition," in Mobile Multimedia/Image Processing, vol. 11399. SPIE, 2020.

[11] S. Rajeev, K. Shreyas, Q. Wan, K. Panetta, and S. Agaian, "Illumination Invariant NIR Face Recognition Using Directional Visibility," Electronic Imaging, Image Processing: Algorithms and Systems, pp. 273–1–273–7, 2019.

[12] H. Bae, T. Jeon, Y. Lee, S. Jang, and S. Lee, "Non-Visual to Visual Translation for Cross-Domain Face Recognition," IEEE Access, vol. 8, no. 7, pp. 50 452–50 464, 2020.

Plataforma de gestão de Energia para Edifícios do Exército

Jóni André Santo Bernardo
Academia Militar,
Exército Português
Lisboa, Portugal
bernardo.jas@exercito.pt

Énio Rodrigo Pereira Chambel
Direção Ensino, Academia Militar,
Exército Português
Lisboa, Portugal
chambel.erp@exercito.pt

Carlos Augusto Santos Silva
Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal
carlos.santos.silva@tecnico.ulisboa.pt

Resumo — **Este trabalho consiste num estudo-projeto para gerir os consumos e aumentar a eficiência energética dos edifícios do Exército Português, tendo como objeto de estudo o campus da Academia Militar-Amadora. Este estudo está dividido em 2 fases, sendo que a primeira consiste na construção de um modelo energético urbano no City Energy Analyst do campus, e efetuar uma simulação dinâmica de forma a verificar os consumos do mesmo e verificar medidas para aumentar a eficiência energética do campus. A segunda fase consiste na construção de um modelo energético no DesignBuilder, utilizando como simulador dinâmico o EnergyPlus, do edifício que aloja os alunos, de forma a analisar os consumos de eletricidade, propor medidas de eficiência energética e simular o potencial de redução de custos elétricos e térmicos de um edifício que representa cerca de 12,5% das necessidades do campus. Com o objetivo de melhorar a eficiência energética do edifício foi realizado em simultâneo, uma auditoria e um estudo de dimensionamento de diversos sistemas, equipamentos e medidas de forma a reduzir os custos provenientes do edifício e a viabilidade económica da implementação dessas mudanças.**

I. INTRODUÇÃO

As mudanças climatéricas, resultantes da poluição do meio ambiente, não são nenhuma novidade do século XXI, sendo que a tentativa das reduções das emissões de carbono começou por volta da década de 80 e foi oficializado em termos globais através do Protocolo de Quioto em 1997. Foi com base neste protocolo que a Comissão Europeia (CE) publicou em 2018, retificando a diretiva de 2010/31/EU e 2012/27/EU, a diretiva 2018/844, também denominada como EPBD, Energy Performance of Buildings Directive, que visa reverter este paradigma, focando-se na eficiência energética e na performance da energia dos edifícios.

Neste âmbito, e com o intuito de atingir os objetivos estipulados no RNC2050 e no EPBD, foi desenvolvido o Plano Nacional Energia e Clima 2021-2030 (PNEC 2030), oficializado com o Decreto-Lei nº64/2020, cujo a sua principal função é ser um instrumento de política energética e climática nacional para a década 2021-2030 com a intenção de atingir um futuro neutro em carbono e trazer benefícios a nível da saúde da população, na produtividade laboral e na valorização patrimonial [1].

Como tal, este artigo apresenta uma análise complexa aos consumos energéticos de uma das unidades do Exército Português, a Academia Militar na Amadora (AMA), no qual se estudam e observam os consumos energéticos no campus, se implementam medidas de poupança e é representado em 4D numa plataforma de gestão de energia por forma a facilitar a compreensão e alteração de medidas [2].

II. REVISÃO DA LITERATURA

A. City Energy Analyst

Atualmente as cidades consomem em média mais de 2/3 da energia primária e produzem mais de 70% dos GEE (Gases de Efeito de Estufa) globais [3]. Face a este consumo enorme de energia, Portugal adotou planos estratégicos de forma a aumentar a eficiência energética dos edifícios e a redução das emissões dos GEE, sendo o PNEC 2030 e o ELPRE os planos estratégicos em vigor.

De forma a gerir onde a energia é empregue e de forma a reduzir as emissões de GEE, as cidades necessitam de compreender que edifícios causam a emissão dos GEE, mas também que impacto futuro terão medidas a adotar na redução desses mesmos gases e consumo de energia. Essa análise é feita através de modelos de energia em edifícios, designados como BEM ou UBEM quando aplicados a uma escala urbana, estes permitem a análise individual de edifícios, como o balanço energético, balanço de massa, condições atmosféricas do interior e da periferia, consumos de energia, entre outros.

A criação de um edifício num modelo UBEM consiste na modelação da geometria do edifício e dos sistemas do edifício, no entanto inserir essa informação individual para cada edifício consiste num processo demorado e complexo e como tal criaram-se arquétipos, estes são elaborados em 2 fases, sendo a primeira a segmentação e a segunda a caracterização na qual colocamos a informação de um edifício típico de uma certa categoria. Após ter os arquétipos definidos é iniciada a simulação termodinâmica. Esta simulação normalmente é executada utilizando apenas uma zona de arquétipo em regime transiente, de modo a simplificar cálculos, que também pode ser executada em regime dinâmico, obedecendo a critérios estabelecidos de acordo com o ASHRAE 90.1, ISSO 13790 e ISO 13780 [3].

O *City Energy Analyst* (CEA) consiste numa simulação combinada entre planos urbanos, sistemas de energia e processos de engenharia de forma a obter os efeitos, *trade-offs* e sinergias entre os projetos e planos de infraestruturas energéticas [4]. O *CEA* permite a construção e modelagem de modelos paramétricos de edifícios em, permitindo a sua análise consoante a luz solar, ciclo de vida e a variação das escalas espaciais e temporais [5].

A funcionalidade genérica do CEA consiste então no armazenamento, análise e visualização da informação dos modelos urbanos energéticos em escalas temporais e espaciais, analisa os serviços de energia em edifícios, as necessidades de potência dos mesmos, radiação solar nas superfícies dos edifícios, fenómeno do sombreamento próprio, interação do

edifício em estudo com a sua vizinhança, características próprias devido à sua geometria e envolvente e vários sistemas AVAC (Aquecimento, Ventilação e Ar Condicionado) e serviços de energia.

B. Auditoria Energética

A auditoria energética consiste numa análise detalhada de todos os consumos relativamente a consumos e utilização de energia relativamente ao aquecimento, arrefecimento, AQS (Águas Quentes Sanitárias), iluminação, ventilação, equipamentos, entre outros.

Pretende adquirir as informações relativas ao consumo de energia, contabilizar os consumos de energia, dispor de dados para decidir, agir para otimizar e controlar as situações com o fim de alcançar benefícios a nível económico, ambiental e social [5].

Como tal a elaboração de uma auditoria é efetuada em quatro passos, sendo eles a preparação da auditoria, intervenção no local da instalação, tratamento da informação recolhida e por fim a elaboração do relatório da auditoria energética.

Para atingir os objetivos estipulados a auditoria poderá auxiliar-se do uso de equipamentos de registo de consumos ou de simuladores dinâmicos, como o *DesignBuilder*, que adquirem valores de consumos próximos da realidade e são admissíveis desde que o CVRSME (*Coefficient of Variation of the Root Mean Squared Error)* seja inferior a 25% para o consumo elétrico relativamente a um mês e inferior a 35% se for relativamente a um ano ou mais [6].

III. CASO DE ESTUDO

O caso estudo deste artigo está dividido em 2 fases, sendo a primeira a gestão dos consumos e os dados energéticos do campus do AMA como um todo, tendo em consideração os edifícios todos da AMA bem como o seu consumo em geral e o processamento dos dados no CEA de modo a aumentar a eficiência energética do campus. A segunda fase consiste na gestão dos consumos e dos dados energéticos do edifício que aloja os alunos do 3º e 4º ano da AMA, que após a aquisição dos respetivos dados, são simulados os consumos e medidas de eficiência energética no DesignBuilder.

De forma a obter os dados para efetuar as simulações pretendidas, é efetuada uma auditoria e caracterização dos espaços do edifício, dos seus equipamentos e respetivas potencias nominais. É feito um estudo aos perfis de ocupação dos espaços, da potência instalada em iluminação, em equipamentos e ao sistema AVAC, no qual se concluiu que o edifício em questão possui um consumo equivalente a 12,5% do consumo da AMA. Sendo que o consumo elétrico anual do AMA corresponde, em média, a 970,225 MWh sendo a sua tarifa elétrica de consumo de 0,11871 €/KWh, o que corresponde a 115 175,41 €/ano. Relativamente ao edifício em estudo, e tendo em conta que a maior parte dos gastos são em tarifas noturnas, este possui um consumo anual elétrico, em média, de 120,987 MWh e sendo a sua tarifa elétrica de consumo de 0,12019 €/KWh, corresponde a 14 541,42 €/ano.

Relativamente aos consumos térmicos, neste caso o consumo de gás natural, o AMA possui aproximadamente um consumo anual, em média, de 654,195 MWh, sendo a sua tarifa de consumo de 0,0362 €/KWh, que corresponde a 23 681,86 €/ano. No que respeita ao consumo de gás natural do edifício em estudo, este possui aproximadamente um consumo de 327 MWh, que corresponde a 11 837 €/ano.

IV. MODELAÇÃO ENERGÉTICA DO CAMPUS NO CEA

Utilizando o CEA é elaborado um modelo energético que represente a AMA, no qual é atribuído os valores dos respetivos edifícios presentes no campus, sendo que em primeiro lugar é atribuído as características físicas e, de seguida, é estipulado a categoria e tipologia a que cada edifício pertence com base nas normas ISO13790 e o estilo de ocupação. Após estipuladas as categorias, são registadas as informações acerca da envolvente do edifício.

Por fim são acrescentados os dados dos ganhos internos, temperaturas de conforto e de ajuste, os sistemas AVAC e de AQS presentes em cada edifício e as suas respetivas fontes de alimentação para cada tipo de energia.

Após o registo de dados, são efetuadas diversas simulações de forma a obter a irradiação solar, os consumos anuais e a potencialidade da instalação de painéis solares em edifícios e em quais seria mais viável a sua aplicabilidade.

V. MODELAÇÃO ENERGÉTICA DO EDIFÍCIO NO DESIGNBUILDER

No DesignBuilder é elaborado um modelo geométrico BEM que representa o edifício das casernas da 3ª e 4ª Companhia, edifício que aloja os alunos do 3º e 4º ano da AM. Após feita a modelação geométrica são inseridos os dados relativamente à sua envolvente, perfis de horários de ocupação, iluminação e de equipamentos, sistemas, ventilação e infiltração.

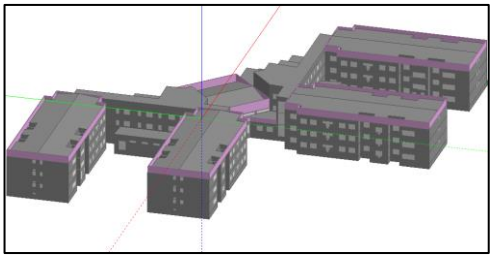


Figura 1. Modelo Geométrico do Edifício

Após a inserção dos dados comuns foram realizados 4 modelos energéticos em que difere a estrutura do sistema AVAC e o do AQS, sendo eles definidos como:

Simulação 1 – Sistema de aquecimento do espaço através de termoventiladores elétricos e aquecimentos de AQS através de caldeiras de condensação a gás natural;

Simulação 2 – Sistema de aquecimento do espaço através de radiadores a água e aquecimento de AQS através de caldeiras de condensação alimentadas com gás natural;

Simulação 3 – Sistema de aquecimento do espaço através de radiadores a água e aquecimento de AQS através de painéis solares térmicos e as caldeiras de condensação a gás natural, sendo elas as principais fontes de aquecimento da água a injetar nos radiadores;

Simulação 4 – Sistema de aquecimento do espaço através de radiadores a água e aquecimento de AQS através de 2 bombas de calor industrial, sendo a fonte de energia elétrica proveniente da rede e de um sistema de paínéis solares fotovoltaicos, sendo

a primeira modalidade constituída por uma potência de 56,7 KWp e a outra de 113,4 KWp, instalada no telhado do próprio edifício.

VI. Resultados e Discussão

A. *Simulação no CEA*

Após as atribuições dos dados necessários para os arquétipos do CEA, é efetuado as simulações de radiação solar e de consumos presentes no campus o que permitiu observar que o edifício com maior consumo em termos elétricos, consiste no edifício A, o edifício de gabinetes, laboratórios, salas de aulas, biblioteca e servidores.

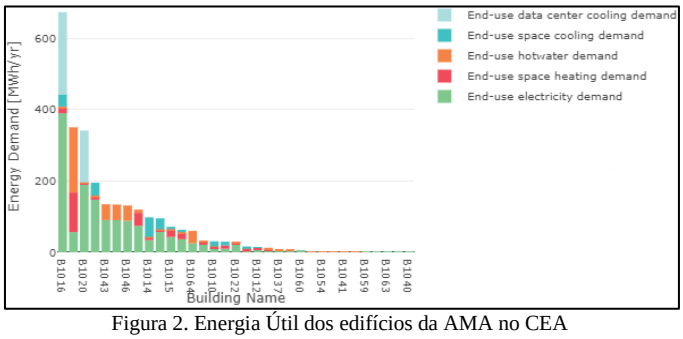


Figura 2. Energia Útil dos edifícios da AMA no CEA

Relativamente ao potencial para a instalação de painéis solares fotovoltaicos, com base na área bruta ocupada pelos edifícios, sendo que por cada metro quadrado é possível produzir em média 54,68 KWh/ano, verifica-se que o máximo de produção de eletricidade no mês de julho é de 2 168,9 MWh, com os painéis instalados nos telhados todos da AMA.

B. *Simulação no DesignBuilder*

Este modelo apresenta um grau de complexidade elevado pois apresenta todos os espaços e divisões que o edifício possui desde gabinetes, quartos, casa-de-banho, lavandaria, salas de estudos, sala de arrumações e outros, sendo que a simulação dinâmica energética foi elaborada pelo *EnergyPlus.*

Portanto, para a simulação 1, foi obtido um consumo anual elétrico de 111 474,79 KWh e um consumo anual de gás natural de 391 835,54 KWh, e tendo em conta as tarifas aplicadas à AMA, no consumo elétrico e do gás natural, perfaz uma despesa anual de 27 567,45 €. Em termos de validação anual, esta simulação obteve um CVRMSE de 4%.

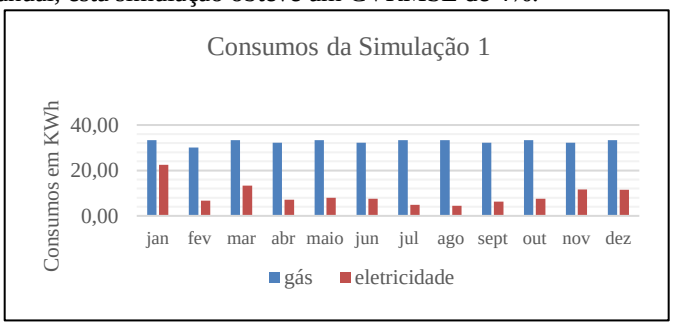


Figura 3. Consumos mensais da Simulação 1

Para a simulação 2 foi obtido um consumo anual elétrico de 71 893,57 KWh e um consumo anual de gás natural de 402 868,94 KWh e tendo em conta as tarifas aplicadas à AMA perfaz uma despesa anual de 23 209,26 €. Esta modalidade permite uma poupança anual, comparando com a simulação 1, de 4 358,19 €.

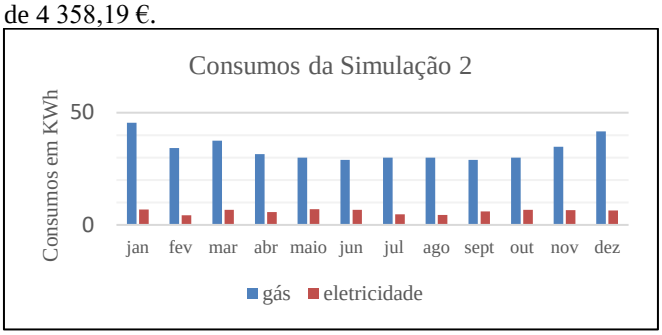


Figura 4. Consumos mensais da Simulação 2

Para implementar o sistema simulado na Simulação 2, assumindo um custo de manutenção anual e bienal equivalente a 1% e 2%, respetivamente, do investimento inicial, o valor máximo de investimento inicial corresponde a 46 311,26 €.

Tabela 1. Viabilidade Económica do sistema da Simulação 2

	Ano 0	Ano 1	Ano 2	Ano 3	…	Ano 15
Poupanças		4 358,19 €	4 358,19 €	4 358,19 €	…	4 358,19 €
NPV	0					
Obtemos que						
Investimento	**- 46 311,26 €**					
Manutenção		- 463,11 €	- 463,11 €	- 926,23 €	…	- 926,23 €
Cashflow	-46 311,26 €	3 837,51 €	3780,80 €	3 282,05 €	…	2 745,06 €
TIR	**1%**					

Para a simulação 3 foi obtido um consumo anual elétrico de 77 207,69 KWh e um consumo anual de gás natural de 346 700,75 KWh e tendo em conta as tarifas aplicadas à AMA perfaz uma despesa anual de 21 816,81 €. Esta modalidade permite uma poupança anual, comparando com a simulação 1, de 5 750, 64 €.

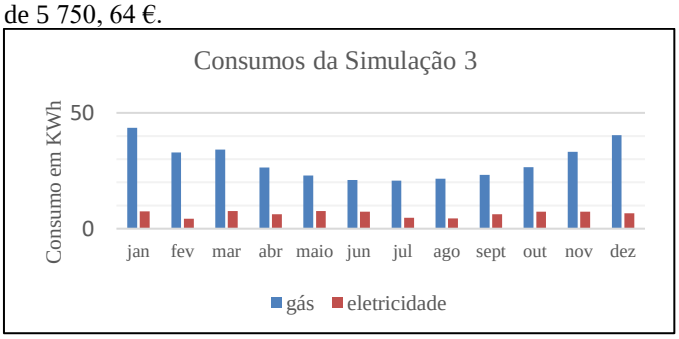


Figura 5. Consumos mensais da Simulação 3

Para implementar o sistema simulado na Simulação 3, assumindo um custo de manutenção anual e bienal equivalente a 1% e 2%, respetivamente, do investimento inicial, o valor máximo de investimento inicial corresponde a 59 507,22 €.

Tabela 2. Viabilidade Económica do sistema da Simulação 3

	Ano 0	Ano 1	Ano 2	Ano 3	…	Ano 15
Poupanças		5 750,64 €	5 750,64 €	5 750,64 €	…	5 750,64 €
NPV	0					
Obtemos que						

Investimento	**- 59 507,22 €**					
Manutenção		- 640,50 €	-1 280,99 €	- 640,50 €	…	- 640,50 €
Cashflow	- 59 507,22 €	5 034,63 €	4 338,52 €	4 886,92 €	…	4 087,36 €
TIR	**1%**					

Para a simulação 4 foi obtido um consumo elétrico de 304 696,48 KWh, sendo que devido à instalação dos paíneis fotovoltaicos de 57 KWp, estes contribuem para 30% do consumo do edifício, totalizando um consumo elétrico extraído da rede igual a 210 755,74 KWh, que perfaz um custo total de 25 330,68€ assumindo as tarifas que a AMA está sujeita. Esta modalidade permite uma poupança anual, comparando com a simulação 1, de 2 236,77 €. Sendo que deixou de haver a necessidade de haver o consumo de gás natural.

A instalação de painéis fotovoltaicos com uma potência total de 57 KWp torna-se inviável economicamente e como tal é necessário aumentar a potência instalada dos painéis fotovoltaicos, assumindo que tudo o que é produzido é consumido pelo campus e, como tal, adotou-se uma instalação de 114 KWp, que permite um custo total anual de 14 040,45 €, permitindo uma poupança anual, comparando com a simulação 1, de 13 527 €, sendo a produção elétrica dos painéis o principal fator pela diminuição dos custos elétricos.

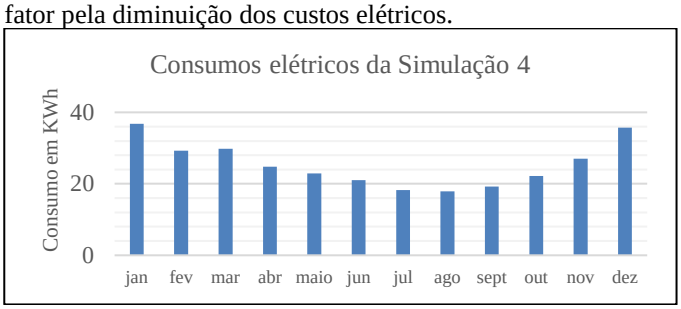


Figura 6. Consumos mensais da Simulação 4 para 57 KWp

Para implementar o sistema simulado na Simulação 4, para uma instalação de fotovoltaicos com uma potência de 114 KWp, assumindo um custo de manutenção anual e bienal equivalente a 1% e 2%, respetivamente, do investimento inicial, o valor máximo de investimento inicial corresponde a 141 616,63 €.

TABELA 3. VIABILIDADE ECONÓMICA DO SISTEMA DA SIMULAÇÃO 4

	Ano 0	Ano 1	Ano 2	Ano 3	…	Ano 15
Poupanças		13 527 €	13 527 €	13 527 €	…	13 527 €
NPV	0					
Obtemos que						
Investimento	**- 141 616,63 €**					
Manutenção		- 1 416,17 €	- 2 832,33 €	- 1 416,17 €	…	- 1 416,17 €
Cashflow	-141 616,63 €	11 931,86 €	10 380,90 €	11 581,80 €	…	9 686,87 €
TIR	**1%**					

VII. CONCLUSÃO

Tendo em conta o panorama e a conjuntura atual que se vive nas forças armadas, o termo de ordem comum a todos os ramos é de contenção de custos e racionalização dos recursos. Nesse âmbito, a eficiência no emprego dos meios e dos recursos assume um papel vital para o cumprimento das missões atribuídas.

Para poder atuar com critério e de forma eficaz no processo de redução do consumo energético e na sua eficiência é impreterível que se saiba quando, onde e quanto se consome de energia elétrica. Segundo os resultados da análise das simulações foi possível aferir os consumos e comparar os valores relativamente ao campus e a viabilidade económica da adoção de sistemas diferentes.

Através da modelação geométrica e simulação dinâmica do edifício que aloja os alunos, é possível averiguar que a modalidade adotada na simulação 1, que corresponde a que a AMA atualmente adota, corresponde à medida mais dispendiosa, pois se a AMA adotar a medida sugerida na simulação 2 para as duas casernas, ou seja para as 4 Companhias, a AMA consegue poupar 8 716,38 € anuais se optar pelo aquecimento dos quarto através do uso dos radiadores e o gás natural como fonte de aqueciemtno das águas de AQS e dos radiadores.

No entanto, a simulação 3, a adoção de paineis solares térmicos, permite poupar anualemente 11 501,28 €, no entanto necessita da instalação de um sistema complementar, o que envolve custos iniciais, mas possui um maior retorno a longo prazo, sendo este prazo dependente do investimento inicial real.

A adoção do sistema da simulação 4, é o que permite a maior poupança anual e a maior redução de emissões de GEE, porém, consiste no sistema com o investimento inicial mais alto mas também o que apresenta o maior retorno do investimento e redução de custos a longo prazo.

Por fim, e utilizando a simulação primária no *DesignBuilder*, é feito uma extração sumária dos consumos gerais e especificos do edifício e insere-se esses mesmos dados nos arquétipos do *CEA*, sendo esta metodologia a mais fácil de implementar de modo a obter arquétipos precisos e realistas dos consumos de diferentes categorias de edifícios pertencentes ao Exército Português. Esta metodologia permite a gestão e controlo dos consumos das unidades militares numa escala a nível macro (campus), mas também a um nível micro (edifício/setor de edifício).

REFERÊNCIAS BIBLIOGRÁFICA

[1] Agência Portuguesa do Ambiente, “Protocolo Quioto,” 1997. [Online]. Available: https://apambiente.pt/index.php?ref=16&subref=81&sub2ref=119&sub3ref=500.

[2] DGEG, “Diretiva do Desempenho Energético dos Edifícios.” [Online]. Available: https://www.dgeg.gov.pt/pt/areas-setoriais/energia/eficiencia-energetica/diretiva-do-desempenho-energetico-dos-edificios/diretiva-dos-edificios/

[3] Y. Chen and T. Hong, “Impacts of building geometry modeling methods on the simulation results of urban building energy models,” Appl. Energy, vol. 215, pp. 717–735, 2018, doi: 10.1016/j.apenergy.2018.02.073

[4] C. F. Reinhart and C. Cerezo Davila, “Urban building energy modeling - A review of a nascent field,” Build. Environ., vol. 97, pp. 196–202, 2016, doi: 10.1016/j.buildenv.2015.12.001

[5] CEA, “The City Energy Analyst,” 2020.

[6] J. A. Fonseca, “Energy efficiency strategies in urban communities: modeling, analysis and assessment,” p. 89, 2016, doi: http://dx.doi.org/10.3929/ethz-a-010639933

Conversor Boost totalmente integrado em Tecnologia CMOS de 130nm

Sérgio Martins Maciel Moreira
Academia Militar
Lisboa, Portugal
moreira.smm@exercito.pt

Pedro Mendonça dos Santos
IUM/AM/CINAMIL
Instituto de Telecomunicações
Lisboa, Portugal
pms@lx.it.pt

Maria Beatriz Vieira Borges
Instituto Superior Técnico
Instituto de Telecomunicações
Lisboa, Portugal
bborges@lx.it.pt

***Abstract*—Este trabalho propõe a concretização de um conversor *Boost* em modo de condução descontínua (MCD), comutado a 1,2 GHz. A proposta é totalmente integrada num processo CMOS de 130nm, sem elementos reactivos externos. O presente trabalho mostra o desempenho do circuito alimentado com uma célula fotovoltaica orgânica (OPV), para atingir uma tensão de saída nominal de 1,2V, para um valor de entrada de 500mV.**

***Index Terms*—Muito-baixa tensão, Gestão de Potência, Conversor Boost, CMOS, *Energy Harvesting*.**

I. Introdução

Os circuitos eletrónicos auto-sustentáveis em termos de energia têm cada vez mais ênfase devido ao crescimento das aplicações para a Internet das coisas (*Internet of Things*, IoT). A substituição de baterias neste tipo de sistemas é dispendioso [1] e coloca problemas ambientais a médio prazo. A disponibilidade de células solares com eficiência razoável em ambientes *indoor*, os geradores termoelétricos, e outras fontes de recolha de energia (*energy harvesting*), são soluções já testadas em sensores de redes ou aplicações biomédicas portáteis [2].

As previsões indicam que o número de sistemas deste tipo irá duplicar até 2023, o que resultará numa necessidade de fontes de energia para sensores na ordem dos milhares de milhão. Os sistemas de recolha de energia - *energy harvesters* - são usados em inúmeras aplicações e em diferentes ambientes, com vantagens na redução e manutenção dos custos de alienação associados às baterias. Contudo o uso de fontes de *energy harvesting* introduz circuitos adicionais e sistemas de gestão de energia dedicados [3].

O avanço da tecnologia de fabrico de circuitos integrados, nomeadamente a tecnologia CMOS, tem contribuído para a constante redução da dimensão dos sistemas eletrónicos, bem como da potência consumida por estes para funcionalidades idênticas [4]. O recurso a circuitos elevadores de tensão contínua ou conversores DC-DC, do tipo indutivo ou capacitivo, surgem como uma solução para converter os baixos valores de tensão das fontes de *energy harvesting* (tipicamente na ordem das centenas de mV), para valores de alimentação padrão (1,2V, 2,4V, etc.) [5].

As novas soluções para aplicações em *wearables*, através de células solares flexíveis em conjugação com baterias ultra finas, está na base da motivação para o avanço tecnológico nesta área [6].

Este trabalho procura contribuir com uma solução para a elevação da reduzida tensão imposta pela OPV, através de uma proposta totalmente integrada em tecnologia CMOS, com área de implementação diminuta, de modo a que possa ser colocada em qualquer zona, nos limites exteriores da área ativa da OPV.

II. Conversor *Boost* em tecnologia CMOS

A implementação do conversor *Boost* de comutação abrupta permite elevar a tensão da OPV. Para se gerar o sinal de comutação dos dispositivos do conversor recorreu-se ao dimensionamento de um oscilador LC de par cruzado [7].

A. Célula Fotovoltaica Orgânica

A caracterização da célula solar a usar como *energy harvester* é necessária para a construção e quantificação do modelo a incluir em simulações. Esta caracterização foi concretizada através de um multímetro/fonte Keithley K2400, um simulador solar Oriel Sol A, 69920, Newport com AM1.5G, de modo a simular a irradiação solar sobre a OPV, uma célula fotovoltaica de calibração Newport 91150V, um osciloscópio Tektronix TDS3054B de quatro canais, um multímetro Voltcraft 7905C e uma fonte de alimentação Instek GPC-9030DQ.

A célula orgânica caracterizada está representada na fotografia da figura 1. É uma célula flexível, com uma tensão de circuito aberto (V_{oc}) de cerca de 550mV e uma corrente de curto circuito (I_{sc}) de 61mA.

B. Conversor Boost em MCD

Para dimensionar o conversor *Boost* de comutação abrupta (figura 2) em MCD será necessário dimensionar os elementos do circuito, nomeadamente, o elemento armazenador de energia, uma bobina integrada, L, as dimensões e parâmetros de funcionamento do transístor NMOS $Q1$, e o condensador de filtragem C.

Para a escolha dos componentes do PDK (*Process Design Kit*) do processo CMOS foram tidos em conta vários parâmetros. Para a escolha do transístor, dado que o circuito a ser estudado é para muito baixa tensão, é necessário recorrer a um transístor com uma tensão de limiar (V_{th}) muito baixa, idealmente nula. Deste modo, foi escolhido o transístor NMOS "nativo", com tensão de limiar típica de aproximadamente 90mV.

Relativamente ao condensador de filtragem C, o seu dimensionamento será determinado por forma a obter um valor típico de

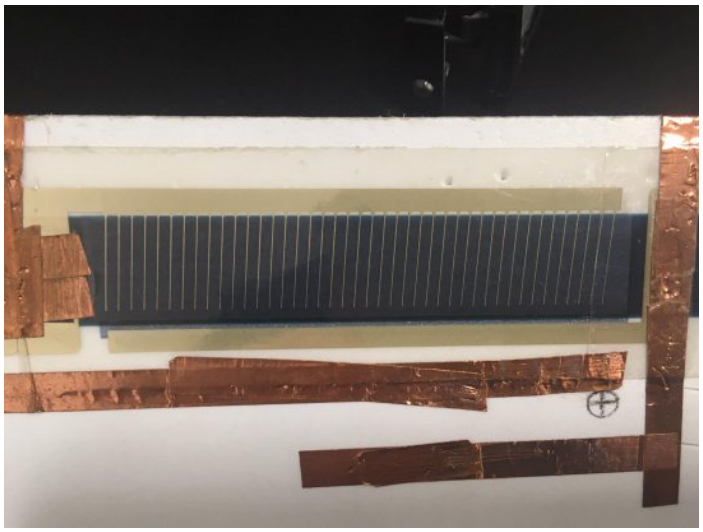


Figura 1. Célula orgânica (OPV) caracterizada.

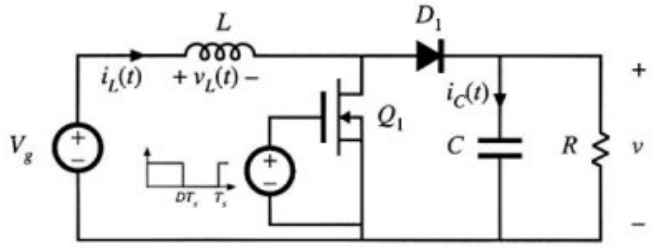


Figura 2. Conversor *Boost* de comutação abrupta [8]

.

ripple de 1% da tensão de saída. Quanto à sua implementação, será utilizado um condensador MIM disponível no processo CMOS. Uma vez que o valor da capacidade esperada para este condensador será elevada, a adopção da tecnologia MIM em detrimento da MOM é mais conveniente, uma vez que a primeira possui mais capacidade por unidade de área, conduzindo assim a uma redução da área de implantação em Silício.

Os valores finais dos elementos do conversor *Boost* estão resumidos na Tabela I, cumprindo os requisitos de área de implantação mínima e maximização da relação de conversão.

C. Oscilador LC

Os osciladores são um dos principais blocos em sistemas e circuitos de RF. Os osciladores mais usados para comutação abrupta de conversores totalmente integrados são os osciladores em anel e os osciladores LC com par cruzado. Os osciladores em anel são preferidos em muitas aplicações devido à sua pequena ocupação de área. No entanto, apresentam dispersão de frequência elevada para o tipo de aplicação em estudo e a frequência de oscilação é sensível à variação da alimentação. Por outro lado, os osciladores LC com par cruzado exibem melhor desempenho de ruído de fase em comparação com os osciladores em anel, apesar de ocuparem considerável área de Silício. O par cruzado pode ser construído usando apenas dispositivos NMOS, para além do circuito ressonante LC.

Tabela I
VALORES DOS ELEMENTOS DO CONVERSOR *Boost*

Elemento	Valor
L	$10nH$
Q1 (W/L)	$75\mu m$ / $120nm$
D1 (W/L)	$600nm$ / $2\mu m$
Q2 (W/L)	$300nm$ / $2\mu m$
C	$2.45pF$

Tendo em conta as especificações de comutação do conversor de muito-alta frequência (1.2GHz) foi escolhido e adaptado a este trabalho o oscilador estudado em [7]. Este circuito tem como saída uma onda sinusoidal com alguma distorção harmónica, e valor de frequência na gama das unidades de GHz.

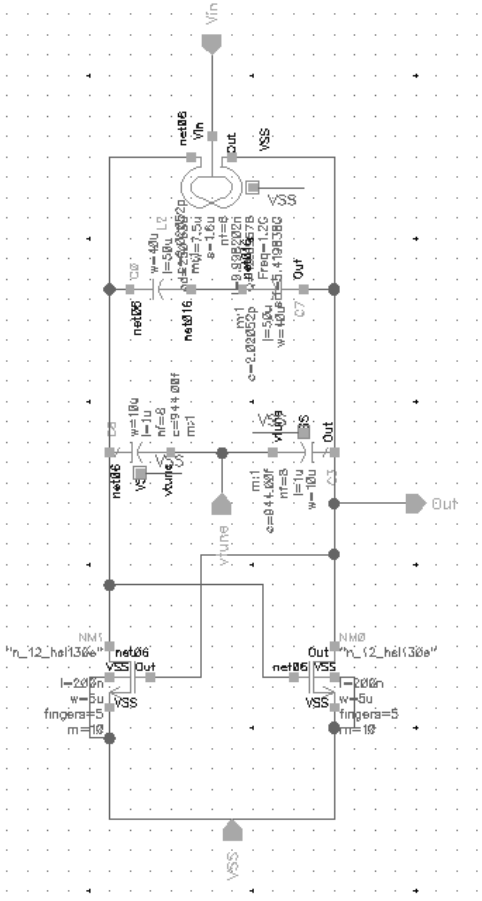


Figura 3. Oscilador LC com par cruzado, usado para comutar a *gate* do NMOS.

Este oscilador foi dimensionado para operar a uma frequência nominal de 1,2GHz. Através da tensão V_{tune} o oscilador pode variar a frequência de oscilação entre 1,25GHz e 1,31GHz (para um V_{tune} máximo de 0.6V).

III. Resultados de Simulação

Nesta secção são abordados os resultados obtidos após o dimensionamento do conversor elevador e do oscilador.

O funcionamento deste conversor a uma frequência de comutação na ordem dos GHz introduz várias dificuldades. Com efeito, a limitação imposta naturalmente ao valor máximo de indutância possibilitada em circuito integrado (20nH), implica a comutação do NMOS a uma frequência da ordem das unidades de GHz. A esta frequência, as correntes de fuga dos semicondutores e os acoplamentos capacitivos têm uma influência significativa no funcionamento do circuito. Através da figura

4 é possível perceber que o conversor *Boost* está a funcionar em modo lacunar, ou Modo de Condução Descontínua, MCD (sinal laranja). De realçar que devido às capacidades parasitas a corrente na bobina nunca se anula, ao contrário do estipulado pelo funcionamento típico deste conversor. Este facto tem consequências ao nível das perdas na saída do circuito, ou seja, reduzindo a eficiência de conversão.

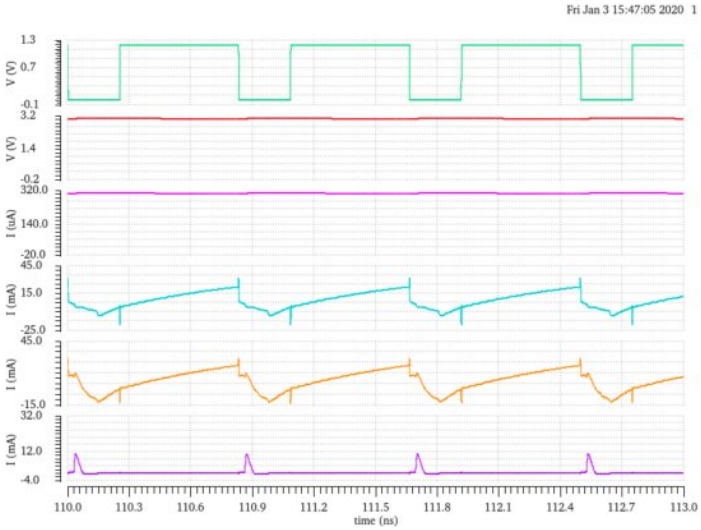


Figura 4. Resultados de simulação obtidos do conversor. (Verde - Tensão de Oscilação) (Vermelho - Saída do Conversor) (Rosa - Corrente de saída) (Azul - Corrente no Dreno) (Laranja - Corrente na Bobina) (Roxo - Corrente no Díodo)

O oscilador permite aplicar um sinal de controlo através da entrada V_{tune}, de modo a modificar a frequência do sinal de comutação do NMOS. Desta forma, poderá ser possível controlar a frequência aplicada à porta do NMOS, de modo a variar a tensão de saída do conversor *boost*. A gama de valores de frequência obtidas pode ser visto na figura 5.

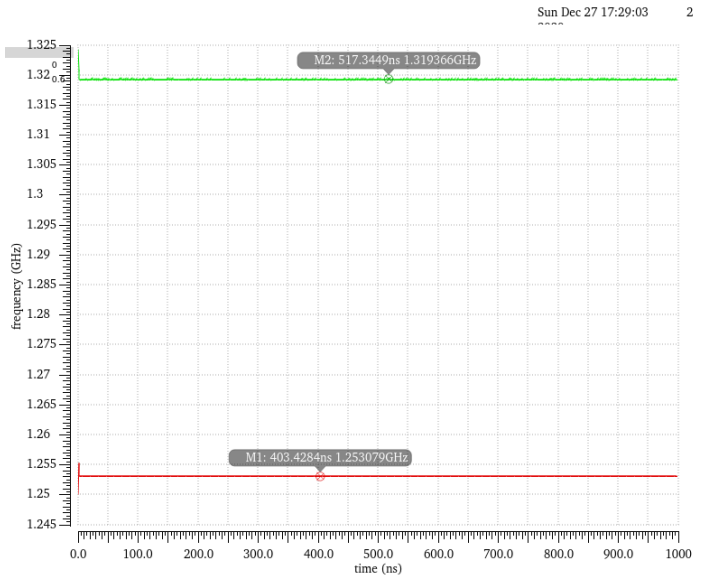


Figura 5. Frequência máxima (verde) e mínima (vermelha) obtida na saída do oscilador.

Por fim, após análise de *corners* do processo CMOS no conversor (figura 6) pode-se concluir que os valores da tensão de saída variam entre 1,1V e 1,4V, onde foram consideradas dispersões em temperatura e dispersão no funcionamento dos semicondutores.

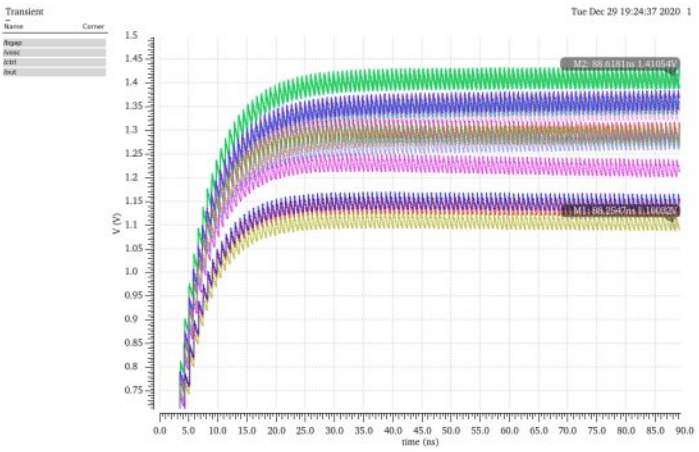


Figura 6. Análise de *corners* da tensão de saída do conversor proposto.

IV. Discussão dos Resultados de Simulação

Nesta secção, é feita a comparação da proposta com vários trabalhos já publicados sobre recolha de energia que usam o conversor *Boost* em tecnologia CMOS.

No circuito estudado em [9] é demonstrado o desenvolvimento e implementação de uma PMU (Unidade de Gestão de Potência) obtida a partir de um conversor *boost* indutivo comutado a 100kHz e com elementos reativos externos.

O circuito presente em [10] é baseado numa topologia de bombeamento de carga para inicializar a condução do circuito, vulgarmente conhecida como *charge pump*, sendo a frequência de comutação variável. Este circuito necessita de 300mV para iniciar a funcionalidade do sistema, podendo ser alimentado após arranque por 30 mV.

Outra solução de conversão de energia a partir de energy harvesting é apresentada em [11]. Neste documento é apresentado um conversor *Boost* implementado em dois estados, ligados em cascata, e projectados num processo CMOS de 0,18μm.

O circuito presente em [12] usa também um conversor *Boost* indutivo. Porém recorre a um pequeno transformador 1:1 para minimizar as capacidades parasitas, evitando o efeito de multiplicação da impedância de transformação causada por transformadores de elevada razão de transformação.

Em [13] é desenvolvido um conversor *Boost* com uma bobina totalmente integrada em tecnologia CMOS de 0,18μm, obtendo-se uma tensão de saída de 1,1 V.

Em [14] encontra-se explicado o desenvolvimento de uma solução para energy harvesting utilizando como dispositivos de obtenção de energia células de a-Si:H. O sistema apresentado tem por base um conversor *Boost*, sendo o armazenamento da energia auxiliado por um super-condensador.

Relativamente ao circuito presente em [15] é usado um *Boost* indutivo com um oscilador, um *charge pump* como circuito secundário de inicialização com uma tensão de 210 mV e uma tensão de inicialização de 7 mV. Á saída do circuito é proposto um LDO (*Low Dropout*) e um *bandgap* em cascata.

Por fim no circuito em [16] é usado um conversor *Boost* indutivo com uma tensão de arranque de 1.2V externos. Este circuito tem uma bobina SMD externa de 47μH.

Na Tabela II estão resumidas as principais características dos conversores analisados anteriormente, em comparação com esta proposta. O *layout* do circuito proposto está representado na figura 7, resultando numa área de ocupação inferior a $0.34\mu m^2$, incluindo PADs para teste CoB (*Circuit-on-Board*). Na figura são perfeitamente identificáveis as bobinas integradas do conversor (à direita) e do oscilador. Para esta área total tão reduzida contribuiu decisivamente a solução de comutação a uma frequência muito elevada, quando comparada com os trabalhos em análise.

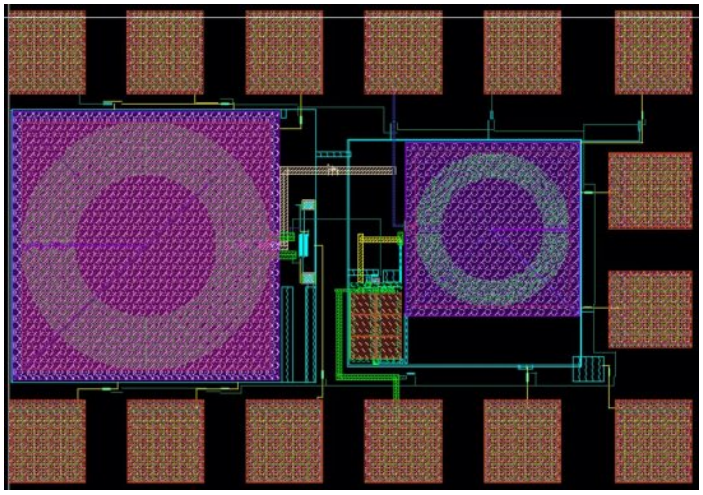


Figura 7. *Layout* final do circuito proposto.

V. Conclusões

Este trabalho propõe um conversor *Boost* totalmente integrado num processo CMOS de 130nm, apenas alimentado por uma OPV. O sistema inclui um conversor *Boost* a funcionar em modo lacunar (MCD), comutado a 1,2GHz, com recurso a um oscilador LC de par cruzado. O circuito é usado para aumentar a tensão de saída de uma OPV (na ordem das centenas de mV) para uma tensão padronizada de 1.2V. A proposta mostra que o objectivo é cumprido com uma implementação em Silício inferior a 0,34 $(\mu m)^2$, o que torna este sistema numa solução comparável ao estado-da-arte, com vantagens significativas em termos de miniaturização.

VI. Agradecimentos

Este trabalho é financiado pela FCT/MCTES através de fundos nacionais e quando aplicável cofinanciado por fundos comunitários no âmbito do projeto UIDB/50008/2020.

Referências

[1] Y. K. Teh e P. K. Mok, "Design consideration of recent advanced low-voltage CMOS boost converter for energy harvesting", *2015 European Conference on Circuit Theory and Design, ECCTD 2015*, n.º 21 mV, pp. 1–4, 2015.

[2] M. B. Machado, F. Nornberg, M. Sawan, C. Galup-Montoro e M. C. Schneider, "Analysis and design of the Dickson charge pump for sub-50 mV energy harvesting", *Microelectronics Journal*, vol. 90, pp. 253–259, 2019.

[3] D. Newell e M. Duffy, *Review of Power Conversion and Energy Management for Low-Power, Low-Voltage Energy Harvesting Powered Wireless Sensors*, out. de 2019.

[4] M. Gul, Y. Kotak e T. Muneer, *Review on recent trend of solar photovoltaic technology*, 4. 2016, vol. 34, pp. 485–526.

[5] P. Poure, S. Weber, B. Vidales, M. Madrigal e D. Torres, "High step-up DC-DC converter for renewable energy harvesting applications", *EEEIC 2016 - International Conference on Environment and Electrical Engineering*, 2016.

[6] M. Shim, J. Jeong, J. Maeng, I. Park e C. Kim, "Fully Integrated Low-Power Energy Harvesting System with Simplified Ripple Correlation Control for System-on-a-Chip Applications", *IEEE Transactions on Power Electronics*, vol. 34, n.º 5, pp. 4353–4361, mai. de 2019.

[7] G. Szczepkowski e R. Farrell, "VCO Design Using Open Loop Analysis", pp. 0–5, 2012.

[8] J. Anderson, *Fundamentals of Power Electronics*. 2013, vol. 5, pp. 447–469. URL: https://www.crcpress.com/Fundamentals-of-Picoscience/Sattler/p/book/9781466505094#googlePreviewContainer.

[9] Y. Qiu, C. Van Liempd, B. O. Het Veld, P. G. Blanken e C. Van Hoof, "5μW-to-10mW input power range inductive boost converter for indoor photovoltaic energy harvesting with integrated maximum power point tracking algorithm", *Digest of Technical Papers - IEEE International Solid-State Circuits Conference*, n.º June 2007, pp. 118–119, 2011.

[10] Q. Liu, X. Wu, M. Zhao, L. Wang e X. Shen, "30-300mV input, ultra-low power, self-startup DC-DC boost converter for energy harvesting system", *IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings, APCCAS*, n.º 60906012, pp. 432–435, 2012.

[11] A. Richelli, S. Comensoli e Z. M. Kovács-Vajna, "A DC/DC boosting technique and power management for ultralow-voltage energy harvesting applications", *IEEE Transactions on Industrial Electronics*, vol. 59, n.º 6, pp. 2701–2708, 2012.

[12] Y. K. Teh e P. K. Mok, "Design of transformer-based boost converter for high internal resistance energy harvesting sources with 21 mv self-startup voltage and 74% power efficiency", *IEEE Journal of Solid-State Circuits*, vol. 49, n.º 11, pp. 2694–2704, 2014.

[13] H. Hernández e W. Van Noije, "Fully integrated boost converter for thermoelectric energy harvesting in 180 nm CMOS", *Analog Integrated Circuits and Signal Processing*, vol. 82, n.º 1, pp. 17–23, 2014.

[14] C. Carvalho, G. Lavareda, A. Amaral, C. N. De Carvalho e N. Paulino, "A CMOS micro power switched-capacitor DC-DC step-up converter for indoor light energy harvesting applications", *Analog Integrated Circuits and Signal Processing*, vol. 78, n.º 2, pp. 333–351, 2014.

[15] Z. Luo, L. Zeng, B. Lau, Y. Lian e C.-H. Heng, "A Sub-10 mV Power Converter With Fully Integrated Self-Start, MPPT, and ZCS Control for Thermoelectric Energy Harvesting", *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2017.

[16] D. Batista, L. Oliveira e P. M. Dos Santos, "Characterization and optimization of an inductive DC-DC converter for ultra-low power energy harvesting", *Proceedings - 2019 International Young Engineers Forum, YEF-ECE 2019*, pp. 77–82, 2019.

Tabela II
COMPARAÇÃO DO ESTADO DA ARTE

Referência	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	*Este Trabalho*
Technology	0.25 μm CMOS	0.35 μm CMOS	0.18 μm CMOS	0.13 μm CMOS	0.18 μm CMOS	0.13 μm CMOS	0.065 μm CMOS	0.13 μm CMOS	0.13 μm CMOS
Topology	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo	*Boost* Indutivo
Year	2011	2012	2012	2014	2014	2014	2017	2019	2021
V_{in} (V)	0.5 2	0.03 (Start@0.3)	0.12	0.021	0.3	0.6	0.007 (Start@0.21)	0.6	0.5
V_{out} (V)	0 5	1.8	1.2	1	1.1	1.2	-	1.2	1.2
Area (mm^2)	-	1.7	0.273	1.5	0.63	0.31	2.14	0.6	0.3325
Freq. (MHz)	0.1	-	1-5	0.1	10	0.1-0.3	40	4.5	1200

Comportamento de Fachadas Envidraçadas sob a Ação de Explosões – Desenvolvimento de uma Solução de Proteção

Rui Rita
Centro de Competências para a Proteção de Infraestruturas
CINAMIL, Academia Militar
Lisboa, Portugal
rita.rjl@exercito.pt

José Pedro
Departamento de Engenharia Civil, Arquitetura e Georrecursos; Ceris
Instituto Superior Técnico
Lisboa, Portugal
jose.oliveira.pedro@tecnico.ulisboa.pt

Pedro Matias
Centro de Competências para a Proteção de Infraestruturas
CINAMIL, Academia Militar
Lisboa, Portugal
matias.pjsg@exercito.pt

Resumo — **A Engenharia Militar e a Engenharia Civil têm realizado investigação no sentido de promover o dimensionamento de infraestruturas às ações dinâmicas de explosões. Têm também investido na investigação, desenvolvimento e implementação de sistemas de proteção capazes de mitigar os impactos das explosões, tanto na estrutura em si como nos seus ocupantes.**

O vidro constitui-se como um material transparente e sustentável, amplamente utilizado em sistemas de fachadas envidraçadas modernas, nomeadamente em edifícios civis e militares. Tem caráter estratégico, como por exemplo, nos edifícios governamentais, quartéis, aeroportos, terminais rodoviários e ferroviários, hospitais e universidades.

Quando uma explosão atinge um edifício, as fachadas são um dos elementos mais vulneráveis. O sistema de proteção estudado para as fachadas envidraçadas consiste num dissipador de energia inserido num sistema de fixação pontual. O dissipador é fabricado em metamateriais de geometria alveolar hexagonal capaz de se deformar plasticamente e de absorver grande parte dos efeitos dinâmicos que seriam transmitidos para a estrutura portante do edifício. A fachada tem também o papel de proteger do exterior quem se encontra inserido dentro do espaço protegido e nesse sentido, é de extrema importância que as fachadas envidraçadas sejam compostas por vidro laminado.

Palavras-chave: Sistemas de proteção; Fachadas envidraçadas; Sistemas de fixação; Metamateriais.

I. INTRODUÇÃO

A segurança de um indivíduo é um direito humano básico e a proteção dos indivíduos é uma obrigação fundamental dos Estados. Por conseguinte, os Estados têm a obrigação de garantir os direitos humanos tomando medidas positivas de proteção contra a ameaça de atos terroristas e de levar os perpetradores de tais atos à justiça [1].

Tradicionalmente, os terroristas têm escolhido edifícios como o seu alvo preferido para ataques. Os edifícios são construídos tendo em consideração os códigos estruturais. Na maioria dos projetos a prevenção e minimização do impacto de ataques químicos, biológicos, radiológicos e nucleares (CBRN) e de engenhos explosivos está ausente na conceção [2].

A utilização do vidro como material de construção não é recente, mas nas últimas décadas têm sido propostas novas funções e desafios para a utilização do vidro com caracter estrutural. Contudo, o vidro apresenta características mecânicas que representam limitações a ter em consideração, sendo que a sua pouca capacidade de deformação a principal [3], [4].

Quando o impacto de uma explosão fratura um vidro, os estilhaços projetados representam um grande risco para aqueles que estão por perto. A utilização de vidros à prova de explosão ou protegidos contra explosões em edifícios suscetíveis de serem sujeitos a tal carga, pode reduzir significativamente, se não eliminar, os riscos associados [5].

O principal objetivo da investigação consiste no estudo de dissipadores de energia com características mecânicas capazes de mitigar os efeitos transmitidos à estrutura de suporte resultantes da ação de uma explosão próxima de uma fachada de vidro.

II. AÇÃO DE EXPLOSÃO

Uma explosão é definida como uma libertação rápida de energia em grande escala [6]. As explosões podem ser divididas em dois grupos principais de acordo com o confinamento da carga explosiva: confinadas e não confinadas. As explosões não confinadas ou externas, podem ser divididas em 3 tipos, que dependem da posição relativa da fonte da explosão e da estrutura a ser protegida: explosão aérea perfeita; explosão próxima do solo; explosão em contacto com o solo. No caso de explosões confinadas ou interiores, estas serão amplificadas pelo fenómeno de reflexão dentro da própria Construção. Existem 3 tipos de explosões confinadas, de acordo com a dimensão da ventilação em causa: explosão totalmente ventilada; explosão parcialmente confinada/ventilada; explosão totalmente confinada [7], [8].

A definição dos parâmetros de onda de choque mais frequentemente utilizada baseia-se nas expressões de Kinney e Graham [9] e nas propostas de Kingery e Bulmash, em 1984 [10].

Na Figura 1 é apresentado o perfil de variação de pressão idealizado com o tempo da explosão, caracterizando a própria explosão. A fórmula de Friendlander modificada é

frequentemente utilizada para descrever a taxa de decréscimo dos valores de pressão da fase positiva:

$$P_s(t) = P_{so} \times \left(1 - \frac{t}{t_0}\right) e^{-b\frac{t}{t_0}} \quad (1)$$

onde, P_{so} [kPa] representa o pico de sobrepressão incidente, t_0 [ms] é a duração da fase positiva, b é o coeficiente de decaimento da curva e t [ms] corresponde ao período entre o instante de chegada (t_a) e o instante em estudo [10]. Esta equação em conjunto com o gráfico apresentado permite então compreender o funcionamento da onda de choque de uma explosão.

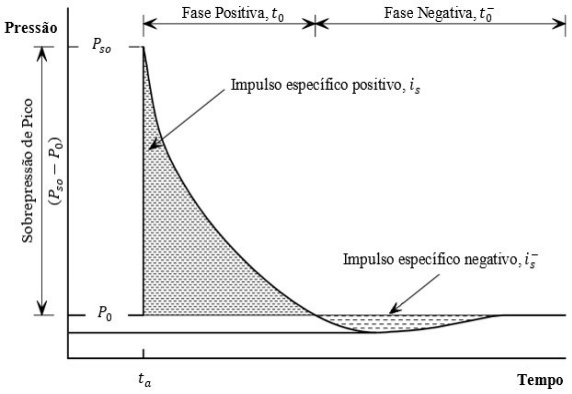


Figura 1. Perfil de pressão idealizado (adaptado de [8]).

A propagação da onda de choque descreve-se em função de um escalar designado de distância reduzida Z, cuja expressão é dada na Equação (1). R corresponde à distância entre a carga e a superfície em estudo e W é a massa de explosivo. A partir de Z (equação (2)) é possível obter a totalidade do perfil de pressões de uma explosão, através das equações de Kinney e Graham [9].

$$Z\left[m/kg^{\frac{1}{3}}\right] = \frac{R}{\sqrt[3]{W}} \quad (2)$$

A presente equação permitiu calibrar a explosão a modelar, fixando uma das grandezas e aumentando a outra, que por sua vez acresce *Z*, distância reduzida. O parâmetro *Z* permite assim ter noção do impacto da carga na estrutura.

III. Tecnologia de Fachadas Envidraçadas

A. *Envidraçados*

De acordo com o método de fabrico têm-se 4 tipos de vidro: float, recozido, temperado e termoendurecido. Relativamente à sua utilização em fachadas, o vidro pode ser: monolítico, laminado e isolante.

B. *Fixações*

Segue-se um diagrama sumário dos sistemas de fixação e dos seus vários tipos (Figura 2):

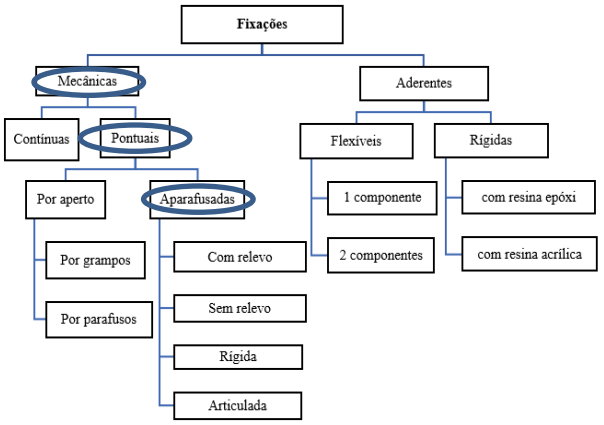


Figura 2. Sistemas de fixação.

IV. Caso de Estudo

A. *Descrição*

O caso de estudo consiste numa fachada (Figura 3) constituída por 3 colunas IPE200 com 3m de altura e espaçadas de 2m (encastradas na base e apoiadas no topo), que suportam dois painéis de vidro laminado temperado 3x2m^2 e 17.52mm de espessura. A carga de 10kg de TNT encontra-se a 5m de distância da face do vidro e a 1,5m de altura do solo.

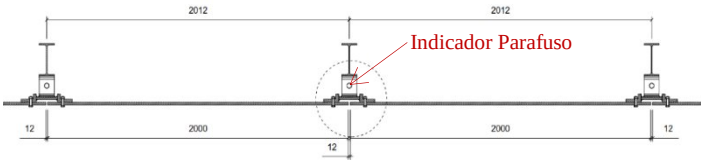


Figura 3. Vista superior da estrutura modelada.

B. *Modelação*

Todo o modelo tem a sua geometria desenhada à linha média, para trabalhar com elementos finitos de laje. A geometria do modelo foi feita e importada, quase na sua totalidade, do software AutoCAD, de modo que só era necessário caracterizar os elementos, condições de fronteira e carregamento (carga de TNT) no LS-Dyna.

C. *Resultados para a ação de uma explosão*

Um dos principais indicadores da carga que passa para a estrutura é o esforço axial e de corte nos Parafusos 1, ao longo da fachada. Na Figura 4, Figura 5 e Figura 6, são apresentados gráficos com estes resultados para uma análise de 70 ms.

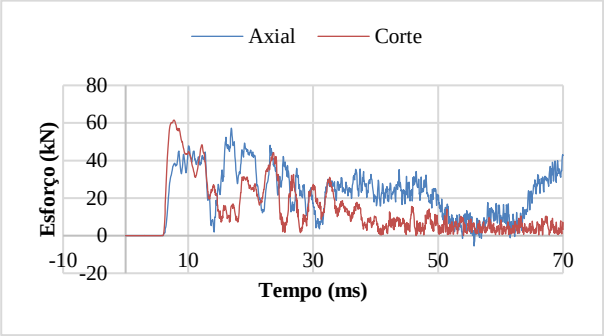


Figura 4. Esforços axial e de corte no Parafuso 1 de topo.

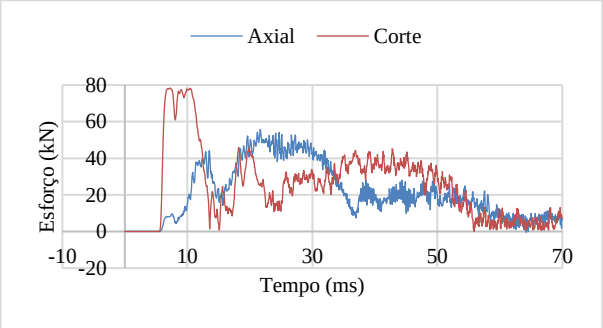


Figura 5. Esforços axial e de corte no Parafuso 1 de meia altura.

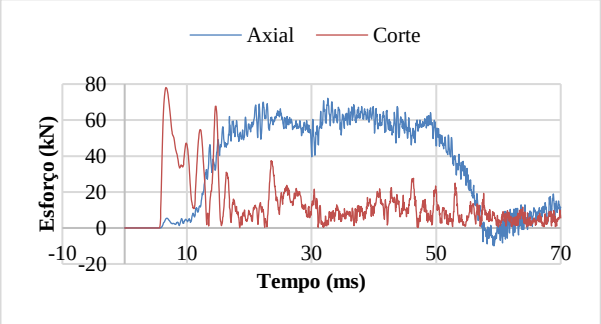


Figura 6. Esforços axial e de corte no Parafuso 1 da base.

D. *Estudo do Dissipador*

Foi modelado um dissipador em metamaterial de PETg com um patamar de cedência a 2.4MPa e uma rotura a 6MPa (Figura 7 e Figura 8).

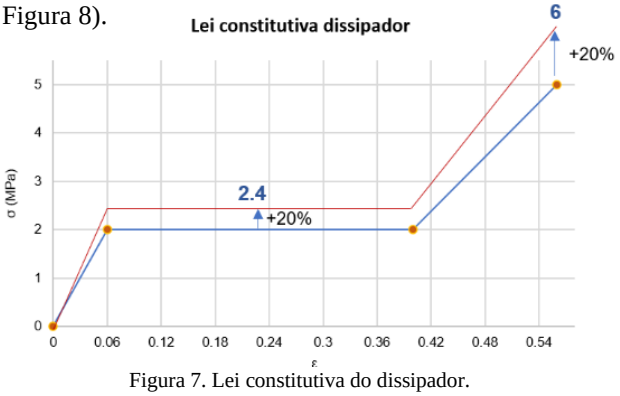


Figura 7. Lei constitutiva do dissipador.



Figura 8. Dissipador com estrutura celular hexagonal (100x100x50).

E. *Interpretação dos resultados*

Como foi dito, o esforço axial e de corte nos Parafusos 1 são indicadores principais da carga que passa para a estrutura, ao longo da fachada (topo, meia altura e base) (Figura 3 e Figura 9). Foram comparados os resultados de um modelo sem dissipador e de outro com dissipador.

No modelo com dissipador verificaram-se os segintes resultados (Figura 9, Figura 10 e Figura 11).

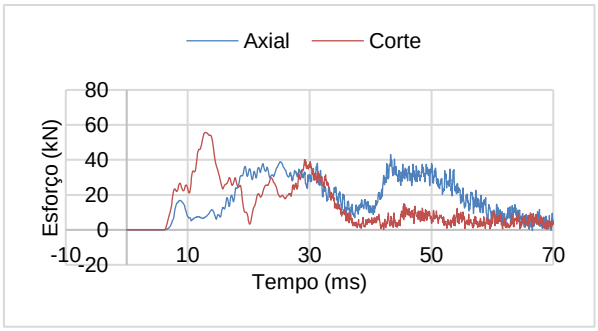


Figura 9. Esforço axial e de corte no Parafuso 1 de topo, com dissipador.

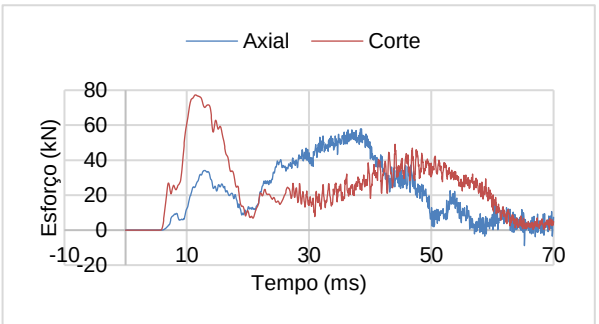


Figura 10. Esforço axial e de corte no Parafuso 1 de meia altura, com dissipador.

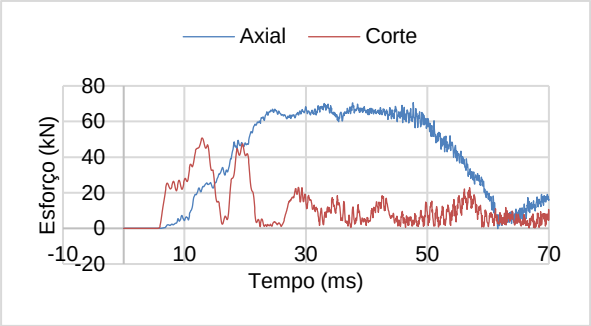


Figura 11. Esforço axial e de corte no Parafuso 1 da base, com dissipador.

De um modelo para outro (Figura 4, Figura 5, Figura 6, Figura 9, Figura 10, Figura 11, Figura 12 e Figura 13) continua a existir um pico de força elevado, nomeadamente de corte nos parafusos, que corresponde à fase em que o máximo de pressão incidente atinge o vidro que posteriormente transmite à estrutura. Continua a dar-se uma plastificação localizada devido à flexão do suporte. Verifica-se que a chapa que une as duas chapas quinadas plastifica totalmente e que a onda de choque é transmitida de uma forma mais controlada.

O vidro no modelo com dissipador, apresenta semelhante padrão de rotura (Figura 12 e Figura 13), sofrendo uma curvatura maior entre a fixação de topo e a de meia altura, do que a que apresentava no modelo de referência. Isto deve-se ao facto de o sistema de fixação com o dissipador ser menos rígido e não dificultar tanto os deslocamentos verticais.

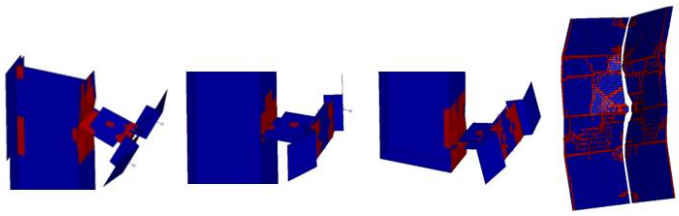


Figura 12. Resultados do modelo sem dissipador.

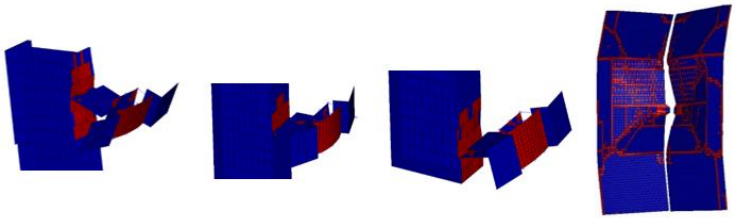


Figura 13. Resultados do modelo com dissipador.

V. Considerações Finais

Numa análise de qualquer sistema de proteção de uma estrutura é crucial considerar três elementos: o sistema de fixação, os elementos estruturais e as ações.

No presente estudo foram estudados vários aspetos relativos ao vidro e ao seu comportamento como elemento estrutural. O vidro pode ser um elemento estrutural inserido em fachadas VEC (Vidro Exterior Colado) e VEA (Vidro Exterior Agrafado). Nas fachadas exteriores de vidro agrafado, as possibilidades de soluções de fixação são muito diversas.

Para que os painéis de vidro não apresentem tantos danos, terão de possuir melhores propriedades mecânicas, maior espessura ou diferentes condições de apoio na estrutura de suporte.

Em todos os modelos se detetou uma formação clara do Mach stem, pelas características dadas à explosão, porque a fachada recebe mais carga desde meia altura até à base. Portanto, ocorre uma reflexão no plano do solo e posterior potenciação da onda de choque e do próprio impulso incidente.

Pela análise dos resultados, o dissipador não teve um impacto tão significativo com esperado. Regista-se uma certa capacidade para amortecer a ação dinâmica transmitida à estrutura, mas não consegue amortecer o que seria necessário para reduzir de forma clara os danos estrutura de suporte.

Agradecimentos

A concretização deste trabalho jamais podia ter acontecido sem o apoio e contributo de um conjunto de pessoas, às quais, quero deixar aqui, palavras sinceras de apreço e gratidão. Não foi uma jornada fácil e tendeu a piorar neste ano de 2020, porém o que concluo é que acabou bem graças a mim e a todos os que daqui para a frente irei enunciar.

Em primeiro lugar quero demonstrar o meu grande agradecimento ao Professor Doutor José Oliveira Pedro, meu orientador científico, pelo empenho, motivação, disponibilidade, pelas suas capacidades técnicas e humanas. Igualmente agradeço ao Tenente-Coronel de Engenharia Pedro Matias, meu coorientador militar pelas suas capacidades, pela abdicação do seu tempo pessoal, empenho e preocupação em prol de me apoiar na minha investigação.

Aos meus amigos e amigas, quero deixar uma palavra sincera de agradecimento.

Finalmente aos meus verdadeiros pilares, a minha família, que sempre esteve presente em todas as alturas que precisei, e que sem ela, não tinha conseguido o que consegui até hoje.

REFERÊNCIAS BIBLIOGRÁFICA

[1] «Human Rights , Terrorism and Counter-terrorism - Fact Sheet No. 32», New York, 2008.

[2] Department of Homeland Security, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, n. outubro. 2011.

[3] L. Valarinho, F. Branco, G. Chiumiento, e J. Correia, «Instabilidade lateral por flexão-torção de vigas em vidro estrutural. Estudo experimental e analítico.», *5as Jornadas Port. Eng. Estruturas*, pp. 1–16, 2014.

[4] J. M. C. P. de N. Sanches, «Análise e Dimensionamento de Sistemas Estruturais de Vidro», Universidade Técnica de Lisboa, 2013.

[5] H. S. Norville e E. J. Conrath, «Simplified Design Procedure for Blast Resistant Glazing», *ResarchGate*, n. junho, pp. 18–21, 2001.

[6] T. Ngo, P. Mendis, A. Gupta, e J. Ramsay, «Blast Loading and Blast Effects on Structures - An Overview», *Eletronic J. Struct. Eng.*, n. janeiro, pp. 76–91, 2007.

[7] Department of Defense, «Unified Facilities Criteria (UFC) - Structures To Resist the Effects of Accidental Explosions», 2008.

[8] E. Yandzio e M. Gough, «Protection of Buildings against Explosions», *Steel Constr. Inst.*, p. 120, 2011.

[9] G. Kinney e K. Graham, *Explosive shocks in air*, 2ª. Nova Iorque: Springer Science + Business Media, LLC, 1985.

[10] V. Karlos e G. Solomos, «Calculation of blast loads for application to structural components», 2013.

Detecção de Intrusões por Monitorização do Comportamento através de Mudanças de *Clusters*

Tiago Fernandes[1,2] Luis Dias[1,2] Miguel Correia[2]
[1]CINAMIL, Academia Militar, Instituto Universitário Militar – Portugal
[2]INESC-ID, Instituto Superior Técnico, Universidade de Lisboa – Portugal
fernandes.tfc@exercito.pt dias.lfxcm@exercito.pt miguel.p.correia@tecnico.ulisboa.pt

***Resumo*—O presente trabalho apresenta uma abordagem de detecção de intrusão que assinala a actividade maliciosa sem conhecimento prévio sobre ataques ou sem dados de treino. A abordagem *Cluster Change-Based Intrusion Detection* (`C2BID`) detecta intrusões através da monitorização do comportamento de máquinas (servidores, computares ou outros elementos de uma rede de computadores). Para esse efeito, o `C2BID` define e extrai características da rede, agrega máquinas com comportamento semelhante utilizando o *clustering*, e analisa depois como as máquinas se movem entre *clusters* ao longo de um período de tempo. Isto contrasta com os trabalhos anteriores na área que param na etapa de *clustering*. Avaliamos experimentalmente este sistema com um conjunto de dados de avaliação (artificiais) e um conjunto de dados do reais, obtendo melhor F-Score do que as soluções anteriores.**

***Palavras-Chave*—Detecção de intrusões, análise de *clusterings*, mudanças de comportamento, análise de segurança**

I. Introdução

No último século, as telecomunicações, o hardware e o software têm tido uma função vital da nossa sociedade, traduzindo-se numa enorme dependência da Internet e, consequentemente, na necessidade de a proteger. A *detecção de intrusões* tornou-se um tópico de investigação importante devido aos avanços nas tecnologias e ao número crescente de ataques em redes de computadores. Actualmente, os Sistemas de Detecção de Intrusão (SDI) estão concebidos para identificar ameaças e possíveis incidentes [1]. Embora estas e outras medidas de segurança permitam detectar e bloquear alguns ataques em tempo real, outros ataques são mais elusivos e podem causar danos mais graves. Especificamente, as Ameaças Persistentes Avançadas (APA) levam frequentemente semanas ou mesmo meses a ser detectadas, conforme relatórios de [2] uma APA leva uma média de 58 dias para ser detectada. Por conseguinte, os mecanismos de segurança tradicionais não fornecem protecção suficiente e as organizações devem investigar o tráfego e os registos para procurar padrões anómalos em janelas de tempo maiores.

Existem duas abordagens clássicas de detecção de intrusões: a detecção baseada em assinaturas e a detecção baseada em anomalias. A detecção baseada na assinatura identifica ataques conhecidos através da detecção de padrões observados no atacantes. A detecção de anomalias tenta encontrar padrões que não se coadunam com o comportamento normal esperado [3]. Ambas as abordagens requerem conhecimento prévio, respectivamente das assinaturas e do comportamento normal, algo que é inconveniente e que contornamos neste trabalho.

As técnicas de aprendizagem automática dividem-se em duas categorias: supervisionada e não supervisionada [4].

Métodos não supervisionados – técnicas por nós utilizadas – é interessante para a detecção de intrusão porque, por definição, não requer conhecimento prévio, ao contrário dos métodos clássicos baseados em assinaturas ou em anomalias. A aprendizagem não supervisionada e especificamente o *clustering* (agregação) têm recebido alguma atenção no contexto da detecção de intrusão. Um algoritmo de *clustering* é aplicado a vectores de dados, cada vector representando uma entidade (por exemplo, uma máquina ou um utilizador), para agrupar entidades com comportamento semelhante, ou seja, com valores semelhantes. Os grupos ou *clusters* resultantes podem ser analisados manualmente e assinalados como maliciosos ou pode ser aplicado um método automático de análise como: detecção outliers, limiares, ou considerando pequenos *clusters* suspeitos.

Muitos trabalhos assumem que apenas uma pequena parte do tráfego é malicioso, por exemplo, [5]–[7]. Isto leva a que ataques com várias máquinas, por exemplo, uma botnet, não seja facilmente detectado. Além disso, os atacantes podem frequentemente contornar os sistemas baseados em aprendizagem automática, executando ataques a baixo ritmo ou em múltiplas janelas de tempo, por exemplo, fazendo um *Port Scan* lento [5]. Alguns modelos [8], [9] dependem de *clustering* e definição de limiares, o que está associado a um período de treino, podendo ser evitado pelos atacantes. Outros dependem da classificação manual, pelo menos numa fase inicial [7], [10].

Neste artigo propomos uma nova abordagem para a detecção de intrusão em redes de computadores baseada na aprendizagem não supervisionada: *Cluster Change-Based Intrusion Detection* (`C2BID`). A nossa abordagem utiliza o *clustering*, tal como os trabalhos acima referidos, mas o *clustering* é apenas um primeiro passo para compreender se uma máquina é maliciosa ou não. A ideia principal da abordagem do `C2BID` é detectar intrusões através da monitorização das mudanças de comportamento de uma máquina. Para esse fim, o sistema define e extrai dados da rede – especificamente dados de fluxo de rede [11]–[13] –, agrega máquinas com comportamento semelhante utilizando o *clustering*, depois analisa como as máquinas se movem entre *clusters* (agrupamentos) ao longo

de um período de tempo e detecta movimentações anormais. Isto contrasta com os trabalhos anteriores na área que essencialmente param na etapa do *clustering*.

C2BID analisa o movimento de máquinas entre *clusters*, incluindo o aparecimento de novos *clusters*, através de *clustering* sequencial em sequências de janelas de tempo. Ao estudar o comportamento temporal dos *clusters* é possível identificar comportamentos anómalos e formação de *clusters* suspeitos. Isto resulta numa maior precisão do que a marcação de apenas *clusters* unitários e numa análise mais rápida do que a análise manual. C2BID utiliza a ideia de características dinâmicas – características definidas durante a execução, com base na actividade observada no porto TCP/UDP – inspirada no DynIDS [6]. Isto permite analisar o tráfego em muitos portos, evitando ao mesmo tempo a maldição da dimensionalidade [14], ou seja, perdendo a capacidade de detectar ataques devido a um número excessivo de características (por exemplo, mais de 1000 características, quando há 2^{16} portos). C2BID melhora os trabalhos anteriores ao correlacionar múltiplas janelas de tempo para detectar ataques a diferentes velocidades e lidar com limitações de janelas fixas...

A nossa avaliação mostra que este sistema foi capaz de detectar não só os ataques etiquetados, mas também encontrou ataques não etiquetados (não reportados) em ambos os conjuntos de dados, destacando as vantagens da sua abordagem não supervisionada. Além disso, este sistema obteve valores mais elevados para o F-score e reduziu a taxa de falsos positivos.

II. A ABORDAGEM DO C2BID

C2BID visa detectar automaticamente as máquinas suspeitas, analisando a forma como estas mudam de *cluster* para *cluster*, num determinado período de tempo. As máquinas que são suspeitas em termos destas mudanças, são assinalados como anómalas. O comportamento das máquinas é caracterizado utilizando características extraídas de dados da rede, por exemplo obtidos em routers com a característica Netflow [11]–[13], pelo que esta é uma abordagem de detecção de intrusão baseada em rede.

A figura 1 representa a abordagem que tem quatro etapas: extracção de características, *clustering*, criação de caminho históricos e detecção de *outliers*, cada uma delas é descrita pormenorizadamente nas secções seguintes.

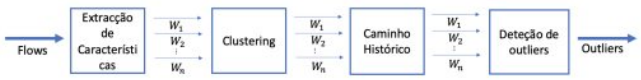


Figura 1. Fases da abordagem C2BID

A. Extracção de características

C2BID utiliza dois períodos de tempo distintos. Primeiro, a deteção é realizada no período de análise $\mathcal{T}_a$, e.g., 1 dia. Segundo, as características são extraídas da rede de acordo com janelas mais pequenas de várias durações, $\mathcal{W} = \{w_1, w_2, ..., w_n\}$. O tamanho da janela w_n tem de ser pelo menos quatro vezes menor que $\mathcal{T}_a$, e.g., alguns minutos. O sistema realiza *clustering* para $w_i \in \mathcal{W}$ durante $\mathcal{T}_a$ e analisa como os *clusters* mudam ao longo do tempo.

Para cada janela de duração $w_i \in W$, são extraídas características de todos os fluxos que aparecem nessa janela. Os fluxos são agregados por máquina, identificados por endereço IP, de modo a que as características sejam associadas a uma máquina e a caracterizem. Para simplificar, consideramos uma associação bijectiva entre máquina e endereços IP. Isto é uma simplificação porque as máquinas podem ter alguns endereços IP diferentes e os endereços IP podem mudar devido à utilização de DHCP. Contudo, conjecturamos que o mau comportamento pode ser observado através da inspecção das comunicações num dos endereços IP da máquina e assumimos que os endereços IP mudam suficientemente lentamente em comparação com o nosso tempo de análise, pelo que os resultados não são afectados.

Consideramos dois conjuntos de características: características fixas e características dinâmicas. As características fixas são sempre as mesmas. Consideramos 16 características fixas, que são normalmente utilizadas na literatura [5]–[7]. A primeira metade das 16 características fixas, com IP de origem como chave de agregação, são: número de diferentes IP contactados pela máquina, número de fluxos em que a máquina é a origem, número de diferentes portos de origem utilizadas pela máquina, número de diferentes portos de destino contactadas pela máquina, soma do comprimento total dos pacotes recebidos pelo anfitrião, soma do comprimento total dos pacotes enviados pela máquina, tamanho médio dos pacotes enviados e a relação entre o número de pacotes enviados e a sua duração. Estas características fixas descrevem a actividade geral da rede de uma máquina. Os outros 8 são semelhantes, mas para os IPs de destino.

Consideramos também um conjunto de características dinâmicas ou características baseadas em portos, seguindo uma ideia recentemente proposta por Dias *et al.* [6]. Alguns ataques são dirigidos a portos TCP/UDP específicos, por exemplo, SSH para o porto 22, pelo que é importante ter características para esses portos. Contudo, há 2^{16} portos vezes 2 (TCP e UDP), sendo que de 0-1023 são Portos de Sistema e de 1024-49151 são Portos de Utilizador [15], pelo que o número de características seria excessivo. Portanto, para cada período $\mathcal{T}_a$ a abordagem escolhe $\mathcal{N}_p$ portos de acordo com alguns critérios e utiliza 4 características para cada um destes portos: número de pacotes enviados do porto, número de pacotes enviados para o porto, número de pacotes recebidos no porto e número de pacotes recebidos do porto.

O resultado da etapa de extracção das características é um *vector de características* para cada máquina. Na avaliação consideramos apenas as máquinas que são internas à organização, uma vez que o número de máquinas externas tende a ser muito maior e menos interessante (apenas uma pequena fracção do tráfego dessas máquinas está presente nos fluxos).

B. Clustering

Após a extracção das características, os vectores das características são fornecidos como entrada para o algoritmo de

clustering. A ideia é agrupar máquinas com comportamento semelhante com base nas características fixas e nas características baseadas em $\mathcal{N}_p \times 4$ portos.

Como mencionado acima, o algoritmo de *clustering* seleccionado foi o K-means. Este algoritmo tem um hiperparâmetro: o número de *clusters*, k. Para definir o valor de k por cada janela de tempo $w_i \in \mathcal{W}$, utilizamos o método de cotovelo [16]. A ideia é testar vários números de k para atingir o número óptimo de *clusters*. O objectivo é atingir o valor de k onde a distância média desde a observação até ao centro do *cluster* tem uma descida mais acentuada. Este valor de k dá uma distribuição equilibrada das entidades sem cair em *overfitting*. A métrica euclidiana é utilizada para determinar a distância entre dois pontos.

O resultado do *clustering* é uma relação entre máquina-*cluster* para todas as janelas de tempo $w_i \in \mathcal{W}$. Cada máquina aparece num *cluster* em cada janela de tempo.

C. Caminho histórico

Dado um período de análise de duração $\mathcal{T}_a$ e janelas de duração $w_i \in \mathcal{W}$ dentro do período de análise, definimos o H de uma máquina h como a sequência de *clusters* em que h aparece. Da secção anterior é claro que H tem um *clusters* por período de duração w_i, mas é necessária uma clarificação: se h não tem fluxos num período, é atribuído a um *cluster* especial que contém hospedeiros inactivos. Para cada h e para cada período $\mathcal{T}_a$, há um caminho histórico H_i correspondendo a uma janela $w_i \in W$. Um caminho histórico representa o comportamento de uma máquina num período $\mathcal{T}_a$ olhando para janelas de tamanho w_i; diferentes ataques são mais fáceis de detectar em janelas de durações diferentes, como mostrado nas experiências.

Para construir o caminho histórico é necessário fazer a classificação dos *clusters*, ou seja, identificar quais os *clusters* que sobrevivem, desaparecem ou emergem entre duas janelas temporais. Isto não é trivial porque os *clusters* mudam, pelo que a abordagem tem de avaliar quais os *clusters* que são semelhantes em intervalos de tempo consecutivos.

A classificação dos *clusters* é feita de acordo com a proposta de Landauer *et al.* [17]. Dois *clusters* são considerados semelhantes se eles tiverem um certo limiar de sobreposição o_t (por exemplo, 50%), ou seja, o número elementos contidos em C' que teriam sido atribuídos aos *clusters* C se tivessem sido utilizados para a geração do mapa de cluster C. A sobreposição é utilizada para expressar matematicamente as relações de *clusters* (Equação (1)). Dividir a união destes dois conjuntos intersectados pela união de todos os conjuntos significa que o valor resultante está no intervalo $[0, 1]$, com 1 indicando uma correspondência perfeita e 0 indicando não haver qualquer correspondência. Dois conjuntos são considerados semelhantes se a sobreposição estiver entre $]0.5, 1]$. Na Equação (1), R_{curr} são as máquinas em C, R'_{prev} são as máquinas em C que também estariam em C', R'_{curr} são as máquinas de C', e R_{next} são as máquinas de C' que também estariam em C. Cada *clusters* recebe um ID único que é utilizado para o representar em todas as janelas de tempo em que aparece.

$$Overlap(C, C') = \frac{|\left(R_{curr} \bigcap R'_{prev}\right) \bigcup \left(R_{next} \bigcap R'_{curr}\right)|}{|R'_{curr} \bigcup R'_{prev} \bigcup R_{next} \bigcup R_{curr}|} \quad (1)$$

A secção seguinte explica a detecção do *outlier*. O resultado das etapas de criação do caminho histórico é um conjunto de caminhos históricos.

D. Deteção de outliers

A detecção de *outliers* é realizada com base no tipo de alterações de *cluster* que uma máquina fez entre janelas de tempo no período analisado. As alterações relevantes podem ser: de um *cluster* para outro, para o mesmo *cluster* ou de um *cluster* para a inactividade.

A detecção de *outliers* é feita em três fases (Figura 2):

- Calculando a probabilidade de cada máquina fazer um determinado conjunto de alterações, tendo em conta todas as alterações feitas no $\mathcal{T}_a$ analisado. Este cálculo é feito em paralelo para todas as diferentes janelas de tempo $\mathcal{W} = \{w_1, w_2, ..., w_n\}$;
- Aplicação do RRCF para detectar valores anormais de probabilidades;
- Filtrar os resultados do RRCF

Cada período de duração $\mathcal{T}_a$ é analisado individualmente. Estes períodos podem ser subdivididos em períodos de tempo $\mathcal{T}_s$, de uma forma em que o máximo W_n tenha pelo menos uma transacção no período $\mathcal{T}_s$, ou seja, $2T_s \times W_n < \mathcal{T}_s < \mathcal{T}_a$. Estas divisões são analisadas em paralelo. Entidades identificadas em pelo menos um período como *outliers* são consideradas como uma potencial ameaça. Estas divisões visam reduzir a possibilidade de uma máquina ser completamente excluído da análise porque, como detalhado mais tarde, uma máquina inactiva por mais de 60% do período $\mathcal{T}_s$ não é considerada.

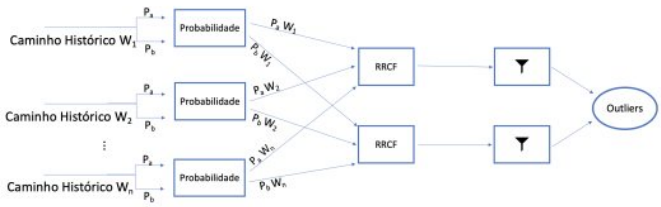


Figura 2. Modelo para deteção de *outliers*

1) Probabilidade: A probabilidade de cada entidade é calculada em paralelo pela divisão $\mathcal{T}_s$ e pela janela temporal ($\mathcal{W} = w_1, w_2, ..., w_n$). O produto final consiste num valor numérico que expressa a probabilidade de um IP alternar entre *clusters* no período estudado, tendo em conta todas as transições nesse período $\mathcal{T}_s$. As máquinas que não têm uma expressão considerável durante um período $\mathcal{T}_s$ têm de ser removidas. Consideramos um limiar de 60%, ou seja, todas as entidades que estejam inactivas durante pelo menos 60% do tempo são removidas. A partir das transições de todas as entidades é criada uma matriz de transição, esta matriz

expressa a frequência absoluta de cada transição entre dois *clusters*. Todas as transições de um *cluster* para a inactividade são excluídas, uma vez que estas transições não fornecem informações úteis relativamente a intrusões na rede.

Após a remoção, a soma de todas as linhas e colunas é calculada e a matriz é normalizada com o valor obtido, a matriz tornou-se uma matriz de frequências relativas.

Para obter o valor numérico para o conjunto de transições efectuadas por uma máquina, soma-se a probabilidade (para efeitos de cálculo, a transformação $f(x) = -\log(x)$ é aplicada) correspondente a uma transição da máquina. Qualquer valor em falta, que não exista na matriz de transição, é obtido através do percentil equivalente.Finalmente, os valores de cada probabilidade das diferentes janelas de tempo são combinados por hospedeiro numa forma vectorial, por exemplo $P_{entidade} = (P_{w_1}^{entidade}, ..., P_{w_n}^{entidade})$.

2) Robust Random Cut Forest: O RRCF [18] é um algoritmo não supervisionado que detecta *outliers*. Este algoritmo produz uma métrica para cada entidade, sendo capaz de lidar com dados em *streaming*, dimensões irrelevantes e valores duplicados que podem mascarar os *outliers*.

Os *outliers* são as entidades com o valor métrico mais elevado. Para a detecção de *outliers*, uma regra de decisão é definida com base no percentil mais baixo a partir do qual um hospedeiro é considerado um *outlier*.

3) Filtro: O RRCF não faz distinção entre valores de alta e baixa probabilidade. Tendo em conta que o objectivo é encontrar máquinas que tomem um caminho invulgar (alta probabilidade), é necessário remover aqueles que o RRFC identificou e não têm um caminho invulgar (baixa probabilidade). Este processo utiliza dois mecanismos: um filtro para valores mais baixos e uma lista branca. A lista branca é definida com base na arquitectura da rede. Pode incluir servidores DNS ou web, que têm padrões de tráfego diferentes de outras máquinas.

Por fim, o `C2BID` identifica os *outliers* como produto final.

III. Avaliação

O objectivo desta avaliação foi fazer a comparação com outras abordagens.

A. Métricas

Consideramos um *outlier* como sendo uma entidade, identificada por um endereço IP, assinalado pelo `C2BID`. Nas expressões seguintes, consideramos os Verdadeiros Positivos (TP) como hospedeiros correctamente classificados como *outliers*, os Verdadeiros Negativos (TN) como hospedeiros correctamente classificados como não *outliers*, os Falsos Positivos (FP) como hospedeiros erradamente classificados como *outliers* e os Falsos Negativos (FN) como hospedeiros erradamente classificados como não *outliers*. As métricas utilizadas na avaliação são Precisão (PREC, fracção *outliers* reais), Recall (REC, fracção *outliers* corretamente classificados) e o F-Score (medida de detecção global).

B. Caracterização do dataset

Utilizámos dois *dataset*s. O primeiro, *CIC-IDS2018* **Data˙Cic**, que designamos como o conjunto de dados artificiais, foi criada para testar e avaliar os SDIs da rede. Os seus autores desenvolveram uma abordagem sistemática para produzir um conjunto de dados de referência diversificado e abrangente. Na sua abordagem, criaram perfis de utilizadores com representações abstractas da actividade vista na rede. Os comportamentos benignos foram gerados utilizando perfis B. Tal perfil foi concebido para extrair o comportamento abstracto de um grupo de utilizadores humanos, encapsulando os comportamentos das máquinas dos utilizadores através da utilização de várias técnicas de aprendizagem automática e de análise estatística. O comportamento malicioso é gerado utilizando perfis M. Estes perfis visam descrever um cenário de ataques sem ambiguidades, de tal forma que os humanos possam interpretar estes perfis e, consequentemente, identificar os seus ataques. A topologia da rede representa uma empresa média típica, com 6 sub-redes, implantada numa plataforma de computação em nuvem.

Considerámos 6 cenários de ataque: Brute Force, ataques pela web, ataques de infiltração, DDoS e port scan . Em todos os dias, excepto no dia 4, os ataques ocorreram em dois períodos distintos, um ataque de cada vez. Os ataques foram realizados a partir de uma ou mais máquinas, utilizando o Kali Linux, foi criada uma rede específica (dentro da gama de IPs públicos) apenas para máquinas atacantes.

O segundo conjunto de dados, *dataset* militar ou *conjunto de dados reais*, foi obtido a partir do Sistema de Informação de Segurança e Gestão de Eventos em produção nessa rede, que recolhe eventos de Netflow a partir de routers internos [19]. A recolha destes fluxos pode dar-nos uma visão do mau comportamento das máquinas internas, não detectado pelos sistemas de segurança implantados. O conjunto de dados corresponde a um mês completo, com aproximadamente 5.500 computadores e 160 GB de dados. Os ataques foram ataques Brute Force (contra SSH e RDP) precedidos por um port scan a um ritmo lento (intervalo de 5 segundos). As principais razões para a escolha destes ataques foram: (1) ter ataques que passam despercebidos aos meios tradicionais de protecção; (2) para captar actividades de reconhecimento interno (por exemplo, port scan) e ataques lentos de dicionários utilizados por atacantes com informação privilegiada.

C. Resultados com o conjunto de dados artificiais

A contagem dos positivos foi feita considerando todos os IPs assinalados pelo `C2BID` em cada $\mathcal{T}_a$. Este método de contagem é susceptível aos FPs, uma vez que cada ataque conta apenas como um TP. Apenas os IPs internos foram analisados uma vez que o sistema necessita de uma fonte contínua de informação que é difícil de obter com os IPs externos. No caso particular deste conjunto de dados, todos os atacantes têm um IP externo e todas as vítimas têm um IP interno. Para cada dia, há uma vítima. A lista branca são todos os IPs internos contactada por mais de 90 % dos IP internos, tendo em conta todos os dias.

C2BID assinalou alguns IPs que não foram identificados como maliciosos pelos autores[1]. Inicialmente consideramo-los FPs, mas uma nova inspecção verificou-se que eram TPs.

Conseguimos identificar todas as vítimas durante todos os dias. Obtivemos, no total dos 9 dias, um PREC de $0,789$, REC de 1, e F-score de $0,882$. Se (erradamente) considerássemos como TP apenas os IPs marcados pelos autores e os outros como FPs, obteríamos um PREC de $0,473$, REC de 1, e F-score de $0,643$.

D. Resultados com o conjunto de dados reais

Os ataques identificados foram: (1) port scan lento com ritmo de 5s (atacante e vítima); (2) brute force RDP (atacante e vítima); e (3) brute force SSH (atacante). Também identificámos algumas máquinas não envolvidas em ataques emulados, mas marcados como *outliers* devido a uma má configuração confirmada pelo Centro de Operações de Segurança.

Em resumo, os alertas levantados pelo C2BID correspondiam a ameaças reais ou anomalias. Fomos capazes de identificar atacantes e vítimas num universo de 5000 hospedeiros. No total, este sistema provou ser útil num cenário prático sem esforço significativo de implantação, uma vez que apenas precisa de ser alimentado com eventos NetFlow.

E. Comparação com diferentes abordagens

Esta secção compara C2BID com três obras anteriores na área: OutGene [5], DynIDS [6], e FlowHacker [7]. Seleccionámos estes três porque são recentes. Não comparámos com mais soluções porque seriam mais antigas, não há implementações disponíveis, e/ou não seguiam as mesmas suposições relativamente à não necessidade de dados de treino.

Todas as três abordagens têm duas fases: extracção de características e *clustering*. Diferem uma da outra em termos de características e algoritmos de *clustering* utilizados. Um IP é considerado um *outlier* se estiver num *cluster* com apenas um elemento. Consideram-se apenas como *outliers* os IPs que estão isolados numa janela de tempo, específica, não analisando as mudanças de *cluster* ao longo do tempo.

Para a contagem de positivos utilizámos o mesmo método que antes: número de IPs diferentes marcados como *outliers* em cada $\mathcal{T}_a$ (1 dia). Este método de contagem difere dos utilizados pelos autores dos três trabalhos, o que leva a resultados diferentes dos fornecidos nos trabalhos originais. Esta alteração deve-se ao facto do C2BID não ser adequado para detecção em pequenas janelas de tempo, por exemplo, de minutos, como fazem estas obras; C2BID monitoriza as alterações de *clusters* ao longo de várias destas janelas de tempo.

Em todos os casos, foi possível obter melhores valores de PREC e F-score com C2BID, com ambos os conjuntos de dados. Para o conjunto de dados reais, o REC foi o mesmo em quase todos os algoritmos. A principal diferença entre estas abordagens e o C2BID é que o C2BID produziu muito mais FPs.

[1]dia 1: 172.31.65.123 e 172.31.67.109; dia 2: 172.31.66.112; dia 4: 172.31.65.56; dia 5: 172.31.69.19; dia 9: 172.31.66.100

IV. Trabalho relacionado

Existem vários artigos e livros sobre detecção de intrusão baseados em aprendizagem automática. Um estudo anterior, realizado por Leung e Leckie [20], utilizou *clusters* para detecção de intrusões na rede. Os autores apresentam o seu próprio algoritmo de *clustering*, (fpMAFIA), e testam-no com um conjunto de dados (KDD 99).

Alguns trabalhos recentes não utilizam o *clustering* e baseiam-se no conhecimento do que é um bom comportamento. Cinque *et al.* usou entropia para inferir desvios de uma linha de base [21]. DeepLog foi inspirado no processamento de linguagem natural e interpreta os registos como elementos de uma sequência que segue as regras gramaticais [22]. Kitsune utiliza um conjunto de redes neuronais chamadas *autoencoders* para distinguir entre padrões de tráfego normal e anormal colectivamente [23]. AI^2 era um sistema baseado em log onde a matriz de densidade, decomposição matricial e o replicador ANN (redes neuronais) eram usados para modelar o comportamento de união de diferentes máquinas dentro de um grande conjunto de dados brutos [24]. Este sistema foi capaz de aprender e defender-se contra ataques invisíveis. Marchetti *et al.* desenvolveu um sistema de detecção automática e precoce APA [25]. Extraiu e analisou registos de fluxo para construir uma análise comparativa do comportamento passado de cada hospedeiro através do cálculo das pontuações. A estrutura poderia identificar exfiltrações entre outros.

A monitorização de *clusters* permite-nos correlacionar alterações em *clusters* de duas janelas de tempo consecutivas. Ao longo do tempo os *clusters* podem sofrer algumas alterações. Estas alterações são detectáveis através da associação de *clusters* em múltiplas janelas de tempo. MClusT é uma estrutura que utiliza gráficos bipartidos e probabilidades condicionais para monitorizar transições definidas numa determinada taxonomia [26]. Landauer *et al.* baseou a sua abordagem em técnicas de avaliação de *clusters* onde os mesmos elementos são observados e agrupados ao longo do tempo [17]. Utilizam a evolução dos *clusters* para processar dados de registo em streaming, em lugar de se limitarem a conjuntos de dados de tamanho fixo. Para detectar anomalias, os autores verificaram se um valor futuro se encontra dentro do intervalo de previsão, utilizando a última entrada registada e assim criaram uma previsão para os próximos valores. Os autores identificam uma grande quantidade de FP nos resultados da avaliação do seu sistema. C2BID aplica um sistema de classificação semelhante ao apresentado em [17] para construir o caminho histórico. Utilizámos o binómio *clusters* e entidade em vez de log e entidade. C2BID diminui os FPs porque utiliza um método diferente de detecção *outliers* e estuda NetFlows em vez de logs. Por outro lado o MClusT, não se baseia na associação de *clusters* e probabilidade condicional, mas na associação directa entre elementos em diferentes janelas de tempo.

Os métodos de *clustering* em cibersegurança só foram aplicados a janelas de tempo específicas, não havendo estudo da correlação entre várias janelas de tempo. Os trabalhos em séries temporais não se aplicam directamente à cibersegurança e por vezes dependem de métodos de aprendizagem supervisionados. Os métodos de classificação de *clusters* existentes produzem uma grande quantidade de FP. Avançamos nos trabalhos anteriores considerando múltiplas janelas de tempo e compreendendo o movimento de máquinas entre *clusters*, através de técnicas de *clustering* em séries sequenciais e várias janelas de tempo.

V. Conclusão

Neste artigo é apresentado `C2BID`, uma abordagem de detecção de intrusão numa rede de computadores, baseada em aprendizagem não supervisionada, que detecta ataques indefinidos sem assinaturas e dados de treino. A nossa abordagem não está centrada na detecção de intrusões em tempo real, pois precisamos de um período considerável de fluxos para obter resultados. A abordagem baseia-se no *clustering*, ou seja, na agregação de máquinas com padrões de tráfego semelhantes; na análise temporal, ou seja, no comportamento de uma máquina num período de tempo; e na monitorização, ou seja, na análise de alterações de *clustering* para detectar outliers.

Nas experiências, quase todos os *outliers* assinalados eram ataques ou máquinas mal configuradas. Ao correlacionar mais do que uma janela temporal, foi possível detectar ataques que ocorreram em diferentes velocidades.

`C2BID` foi capaz de reduzir o número de FPs mesmo em grandes conjuntos de dados em comparação com outras abordagens como OutGene, FlowHacker, e DynIDS. Quando comparado com trabalhos anteriores, `C2BID` conseguiu melhores resultados tanto com um conjunto de dados artificial como num cenário real.

Referências

[1] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang e J. Han, "When intrusion detection meets blockchain technology: a review", *IEEE Access*, vol. 6, pp. 10 179–10 188, 2018.

[2] Fireye e Mandiant, "Special Report", M-TRENDS, Report, 2020.

[3] M. H. Bhuyan, D. K. Bhattacharyya e J. K. Kalita, "Network anomaly detection: methods, systems and tools", *IEEE Communications Surveys & Tutorials*, vol. 16, n.º 1, pp. 303–336, 2013.

[4] A. L. Buczak e E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", *IEEE Communications Surveys & Tutorials*, vol. 18, n.º 2, pp. 1153–1176, 2015.

[5] L. Dias, H. Reia, R. Neves e M. Correia, "OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zooms", em *Network and System Security*, J. K. Liu e X. Huang, eds., Cham: Springer International Publishing, 2019, pp. 199–220, ISBN: 978-3-030-36938-5.

[6] L. Dias, M. Correia e S. Valente, "Go With the Flow: Clustering Dynamically-Defined NetFlow Features for Network Intrusion Detection with DynIDS", in submission, 2020.

[7] L. Sacramento, I. Medeiros, J. Bota e M. Correia, "Flowhacker: detecting unknown network attacks in big traffic data using network flows", em *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2018, pp. 567–572.

[8] T. Zoppi, A. Ceccarelli e A. Bondavalli, "Evaluation of Anomaly Detection Algorithms Made Easy with RELOAD", em *Proceedings of the International Symposium on Software Reliability Engineering*, 2019, pp. 446–455.

[9] T. Zoppi, A. Ceccarelli, L. Salani e A. Bondavalli, "On the educated selection of unsupervised algorithms via attacks and anomaly classes", *Journal of Information Security and Applications*, vol. 52, 2020.

[10] D. Gonçalves, J. Bota e M. Correia, "Big data analytics for detecting host misbehavior in large logs", em *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2015, pp. 238–245.

[11] B. Claise, *Cisco systems netflow services export version 9*, IETF Request For Comments 3954, 2004.

[12] B. Claise, B. Trammell e P. Aitken, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, IETF Request For Comments 7011, set. de 2013.

[13] M. Wang, B. Li e Z. Li, "sFlow: Towards resource-efficient and agile service federation in service overlay networks", em *Proceedings of the 24th IEEE International Conference on Distributed Computing Systems*, 2004, pp. 628–635.

[14] M. Verleysen e D. François, "The curse of dimensionality in data mining and time series prediction", em *International Work-Conference on Artificial Neural Networks*, 2005, pp. 758–770.

[15] M. Cotton, L. Eggert, J. Touch, M. Westerlund e S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry.", *RFC*, vol. 6335, pp. 1–33, 2011.

[16] P. Bholowalia, "EBK-Means: A Clustering Technique based on Elbow Method and K-Means in WSN", *International Journal of Computer Applications*, 2014.

[17] M. Landauer, M. Wurzenberger, F. Skopik, G. Settanni e P. Filzmoser, "Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection", *Computers and Security*, vol. 79, pp. 94–116, 2018.

[18] S. Guha, N. Mishra, G. Roy e O. Schrijvers, "Robust random cut forest based anomaly detection on streams", *33rd International Conference on Machine Learning (ICML)*, vol. 6, pp. 3987–3999, 2016.

[19] L. F. Dias e M. Correia, "Big data analytics for intrusion detection: an overview", em *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*, IGI Global, 2020, pp. 292–316.

[20] K. Leung e C. Leckie, "Unsupervised anomaly detection in network intrusion detection using clusters", em *Proceedings of the 28th Australasian Conference on Computer Science*, 2005, pp. 333–342.

[21] M. Cinque, R. Della Corte e A. Pecchia, "Entropy-based security analytics: Measurements from a critical information system", em *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2017, pp. 379–390.

[22] M. Du, F. Li, G. Zheng e V. Srikumar, "Deeplog: Anomaly detection and diagnosis from system logs through deep learning", em *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1285–1298.

[23] Y. Mirsky, T. Doitshman, Y. Elovici e A. Shabtai, "Kitsune: an ensemble of autoencoders for online network intrusion detection", *arXiv preprint arXiv:1802.09089*, 2018.

[24] K. Veeramachaneni, I. Arnaldo, A. Cuesta-Infante, V. Korrapati, C. Bassias e K. Li, "AI^2: Training a Big Data machine to defend", em *Proceedings of the 2nd IEEE International Conference on Big Data Security on Cloud*, 2016, pp. 49–54.

[25] M. Marchetti, F. Pierazzi, M. Colajanni e A. Guido, "Analysis of high volumes of network traffic for advanced persistent threat detection", *Computer Networks*, vol. 109, pp. 127–141, 2016.

[26] M. Oliveira e J. Gama, "Bipartite graphs for monitoring clusters transitions", em *International Symposium on Intelligent Data Analysis*, Springer, 2010, pp. 114–124.

Aplicação de Metodologia "Reliability Centered Maintenance 3" (RCM3) ao sistema de refrigeração do sistema de armas Pandur II 8x8

Filipe Emanuel Carvalho da Silva, Énio Chambel
Academia Militar
Lisboa, Portugal
silva.fec@exercito.pt, enio.chambel@academiamilitar.pt

Virgínia Infante
Instituto Superior Técnico, Universidade de Lisboa
Lisboa, Portugal
virginia.infante@tecnico.ulisboa.pt

Resumo — **A evolução do paradigma da manutenção ao longo do tempo originou várias mudanças, tanto nas tarefas de manutenção realizadas como nos objetivos da manutenção e gestão de ativos, assumindo-se como uma área de interesse fundamental para as organizações. No caso específico do Exército Português, o processo de modernização gradual que atravessa, resultou no aumento da complexidade dos equipamentos à sua disposição, colocando novos desafios à manutenção, sempre com o objetivo de atingir a prontidão e o nível de custos adequado.**

Neste estudo, a metodologia de manutenção RCM3 foi aplicada ao sistema de arrefecimento das Pandur II 8x8. Esta metodologia centra-se na fiabilidade do equipamento e permite identificar e avaliar os riscos associados aos modos de falha apresentados, bem como desenvolver estratégias para gerir e minimizar estes riscos. Foi efetuada uma análise funcional do sistema estudado, seguida de uma análise dos modos de falha e efeitos, e de uma análise de risco. As respetivas ações de mitigação foram propostas de acordo com o processo de decisão RCM3 e foram comparadas com o plano de manutenção existente, retirando ilações acerca da sua adequação, da robustez do sistema estudado, e das lacunas existentes no processo de gestão de manutenção das Pandur II.

I. INTRODUÇÃO

A exigência associada às missões do Exército, quer em território nacional, quer no estrangeiro em forças nacionais destacadas, combinada com o grau de prontidão necessário, exige uma grande disponibilidade dos recursos humanos, e do equipamento à sua disposição. Desta forma, a manutenção desempenha sem dúvida um papel essencial no bom funcionamento e fiabilidade do equipamento, sendo responsável por assegurar que este cumpra a sua tarefa quando solicitado. O sistema de armas Pandur II 8x8 é um equipamento moderno e versátil da maior importância para o Exército Português (EP) e para o cumprimento da sua missão. Esta aquisição marcou uma nova fase na modernização do EP, tendo sido amplamente utilizado tanto a nível nacional como no estrangeiro, tendo participado em exercícios na Lituânia e, mais recentemente, utilizado no teatro de operações da República Centro-Africana.

Por ser um dos equipamentos mais recentes ao serviço do EP, e sendo utilizado por poucos países da Organização do Tratado do Atlântico Norte (OTAN), afigura-se ainda como um equipamento um pouco desconhecido, relativamente a requisitos e necessidades de manutenção. Desta forma, Portugal efetua o plano de manutenção proposto pelo fabricante, havendo assim espaço para uma análise crítica e adaptação às necessidades decorrentes da utilização operacional das Pandur II ao serviço do EP. O sistema de arrefecimento foi escolhido para ser analisado neste estudo porque é um dos sistemas com maior incidência de falhas, e com maior potencial de melhoria. Do total de 2038 ordens de trabalho corretivas analisadas, 126 estão relacionadas com o sistema de arrefecimento, o que corresponde a cerca de 6,2% das falhas registadas para todo o sistema de armas. Este artigo descreve a aplicação da metodologia "Reliability Centered Maintenance 3" (RCM3) ao sistema de arrefecimento das Pandur II, para rever a adequação do plano de manutenção atual e propor possíveis melhorias.

II. METODOLOGIA

A. Metodologia RCM3

A origem da metodologia RCM está relacionada com a indústria da aviação comercial e surgiu da necessidade de aumentar a fiabilidade das aeronaves e diminuir os custos associados às suas ações de manutenção. Em 1978, Nowlan e Howard Heap da United Airlines, prepararam um relatório para o Departamento de Defesa dos EUA [1]onde a designação RCM foi utilizada pela primeira vez. O processo RCM espalhou-se rapidamente por outras áreas fora da aviação, e desde 1978 surgiram várias versões do trabalho de Nowlan e Heap, que também foram chamadas RCM, no entanto, e embora algumas destas versões apresentassem melhorias e otimizações do processo original, muitas outras surgiram, menos rigorosas e com tentativas de acelerar algumas das etapas do procedimento

original, que se revelariam imprecisas e com resultados diferentes de uma metodologia RCM "verdadeira".

A fim de obter um procedimento credível que pudesse ser utilizado sem mal-entendidos, a primeira norma relacionada com este tema, a SAE JA1011 [2], foi publicada juntamente com o guia SAE JA1012 [3], em 1999. Uma das tarefas mais notáveis na área foi, como anteriormente mencionado, a metodologia proposta por John Moubray (RCM 2) que se tornaria uma obra de referência na definição das normas anteriores e amplamente utilizada por várias organizações em diferentes áreas da indústria [4].

A metodologia RCM permite desenvolver e otimizar programas de manutenção para sistemas físicos, e quando corretamente aplicada permite aumentar a sua fiabilidade, o que resulta numa série de outros resultados positivos, tais como redução do tempo de paragem, diminuição dos custos associados, aumento da segurança e produtividade. Também permite obter programas de manutenção com uma quantidade de trabalho programado muito inferior aos métodos tradicionais e, quando utilizada para a revisão de programas de manutenção existentes, permite obter uma diminuição na quantidade de manutenção programada, normalmente na ordem dos 40% a 70%. A norma SAE JA1011 define "RCM como um processo específico utilizado para identificar as políticas que devem ser implementadas para gerir os modos de falha que podem causar a falha funcional de qualquer bem físico num determinado contexto operacional" [2]. Por fim, para definir a RCM3 de forma concreta, o seu autor, Marius Basson, refere que corresponde a "um processo utilizado para definir o número mínimo necessário e seguro de ações de manutenção, engenharia e outras estratégias de gestão de risco para garantir um nível tolerável de segurança, integridade ambiental e capacidade operacional lucrativa, tal como especificado pelas normas de gestão de ativos da organização em que está inserida" [5].

Em geral, o processo RCM está dividido em 5 fases (tal como se apresenta na figura 1), que representam de forma genérica uma síntese da sequência lógica do trabalho que deve ser realizado durante a implementação desta análise [6]:

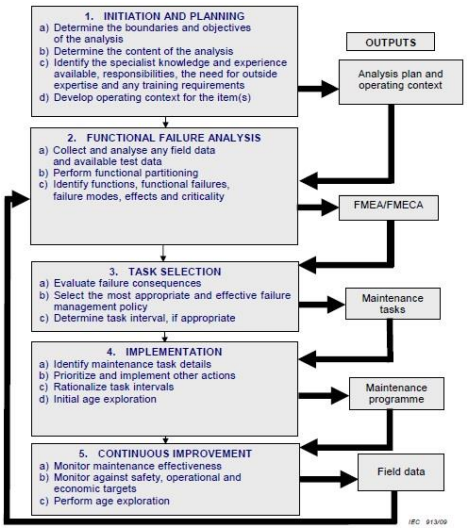


Figura 1. Visão Geral da RCM [6]

O processo RCM3, requer 8 perguntas a serem respondidas durante toda a sua aplicação [3], [5]:

- Quais são as condições operacionais?
- Quais são as funções e normas de desempenho associadas ao activo no seu contexto operacional actual?
- Como é que o activo não cumpre as suas funções?
- O que causa cada estado de falha (modos de falha)?
- O que acontece quando cada falha ocorre?
- Quais são os riscos associados a cada falha (quantificação do risco inerente)?
- O que deve ser feito para reduzir os riscos intoleráveis a um nível tolerável (utilização de estratégias proactivas de gestão do risco)?
- O que pode ser feito para reduzir ou gerir os riscos toleráveis de uma forma economicamente viável?

III. CASO DE ESTUDO

O caso de estudo consiste na aplicação de todas as etapas definidas pela metodologia RCM3 ao sistema de refrigeração das Pandur II, para obtenção de um plano de manutenção proposto. O EP possui uma frota de 188 Pandur II, divididas em 9 versões diferentes, todas com o mesmo sistema de refrigeração.

A. Contexto Operacional

A primeira tarefa a fazer após a definição do sistema a ser estudado na análise RCM3 é a definição do contexto operacional (CO) [5]. Nesta análise, o CO das Pandur II ao serviço do EP, foi definido tendo em consideração o clima e as condições do terreno das regiões do país onde estas são utilizadas (nomeadamente as regiões onde se encontram as unidades da Brigada de Intervenção). Foi também tida em consideração a tipologia de uso das viaturas (exercícios, treino das forças, etc.) bem como o seu nível de utilização médio por ano (medido em Horas de Motor).

B. Análise Funcional

Para poder realizar uma análise funcional do sistema de refrigeração, foi necessário identificar os limites do sistema, o que significa identificar claramente quais os componentes que o constituem. De seguida, as funções dos componentes identificados foram definidas e registadas nas fichas de informação (folhas onde se registou toda a informação gerada ao longo do processo) definidas para esta análise.

C. Análise de Modos de Falha

Após a realização da análise funcional, foram identificados os modos de falha de cada um dos componentes analisados. Tal foi conseguido através da análise do registo de todas as falhas ocorridas neste sistema entre janeiro de 2014 e abril de 2020, o que corresponde a um total de 126 ordens de trabalho analisadas. Para além dos modos de falha identificados através da análise das falhas ocorridas, foi também uma análise de engenharia com o objetivo de identificar outros modos de falha possíveis e prováveis de ocorrer.

D. Efeitos de Falha

A descrição dos efeitos da falha é uma fase muito importante, pois fornece as informações necessárias para a análise de risco que é realizada para cada modo de falha identificado. Nesta descrição, como o nome indica, foram definidas as consequências resultantes dos modos de falha (tanto as consequências operacionais como os sinais de alerta das ocorrências) e a sua frequência estimada (utilizada para definir a probabilidade de ocorrência do modo de falha ao realizar a análise de risco), que foi determinada estimando o seu "Mean Time Between Failures" (MTBF).

Por sua vez o MTBF de cada modo de falha foi estimado com recurso à distribuição de Weibull [7]:

$$MTBF = \eta\Gamma(\frac{1}{\beta} + 1). \quad (1)$$

Em que β e η correspondem aos parâmetros da distribuição, e Γ é a função Gama da distribuição estatística. O parâmetro de escala ou "vida caraterística" η, corresponde ao intervalo de tempo no qual ocorrem 62,3% das falhas, e apresenta as mesmas dimensões que a variável *t* (seja horas, quilómetros, ciclos, etc.). Por sua vez, o parâmetro de forma β é um valor adimensional, responsável pela forma da distribuição, e traduz o mecanismo de degradação, permitindo relacionar a distribuição com as fases de vida do equipamento. As variações deste valor refletem-se no comportamento da distribuição, aproximando-se, para certos valores, de outras distribuições de probabilidade utilizadas em estudos de fiabilidade [8]:

- β=1: a distribuição de Weibull assume a forma da distribuição exponencial, o que permite representar a fase de vida útil;
- β<1: a distribuição de Weibull assume a forma da distribuição gama, o que permite representar o período de mortalidade infantil.
- β>1: a distribuição de Weibull assume a forma da distribuição normal (se $\beta = 3{,}5$) ou da distribuição log-normal (se $\beta = 2$), o que se adequa ao período de desgaste.

Existem na literatura diversas formas de determinar estes parâmetros da distribuição, sendo que neste artigo se utilizou o método da máxima verosimilhança com censura de dados à direita (em virtude do conjunto de dados de falha não ser completo, isto é, não serem conhecidos os tempos de falha dos componentes de todas as viaturas da frota), que consiste na maximização da função de verosimilhança (para a distribuição de Weibull), que se representa a seguir [9]:

$$L(\eta,\beta) = \prod_{i=1}^{n}[\frac{\beta}{\eta}\left(\frac{t_i}{\eta}\right)^{\beta-1} e^{-\left(\frac{t_i}{\eta}\right)^{\beta}}]^{\delta_i} \quad [e^{-\left(\frac{t_i}{\eta}\right)^{\beta}}]^{\delta_i} \quad (2)$$

Esta equação requer a utilização de métodos numéricos para que se possa obter uma aproximação da sua maximização, tendo sido para tal utilizado o Solver predefinido do Excell. Os resultados obtidos encontram-se na tabela 1.

Tabela 1. Resultados obtidos com censura de dados

	MTBF (Horas de Motor)	***Parâmetros obtidos***
Sensor de nível	4134.37	η = 4330.66 β = 1.14
Válvula Descompressão	3696.19	η = 3267.94 β = 0.8
Sujidade no Radiador	3478.83	η = 3742.36 β = 1.26
Fugas	1827.43	η = 1514.86 β = 0.74

Foi considerado, em virtude dos registos de falha analisados que todos os modos de falha associados aos componentes Sensor de nível e Válvula de descompressão apresentam a mesma probabilidade de falha e consequentemente o mesmo *MTBF*. Para além destes 2 componentes foram ainda determinados os MTBF para os modos de falha relacionados com a acumulação de sujidade no radiador e as fugas de líquido de refrigeração (tal como se apresenta na Tabela 1). Para os componentes ou modos de falha cujos registos de falhas ocorridos são inexistentes ou insuficientes para aplicar estes modelos matemáticos foi considerado que a sua probabilidade de ocorrência é baixa.

E. Análise de Risco

O risco associado a cada modo de falha previamente identificado, foi determinado de acordo com a metodologia proposta por Marius Basson [5] que define o risco como a combinação da severidade do modo de falha com a sua probabilidade de ocorrência.

$$Risco = Severidade\ X\ Probabilidade\ de\ Ocorrência \quad (3)$$

Para esta análise RCM3 foi criada uma matriz de risco específica com 5 níveis de severidade e 5 níveis de probabilidade de ocorrência. A severidade foi classificada em 4 parâmetros de consequências: Segurança e Saúde, Ambiental, Operacional e Económica. A combinação de ambos os parâmetros permite classificar o risco em 25 níveis diferentes divididos em 4 categorias (baixo, médio, grave e alto). Se a classificação de risco corresponder a uma classificação grave ou alta, então é inaceitável e algo deve ser feito para reduzir o risco associado.

F. Estratégias de Mitigação de Risco

Após a análise de risco, as estratégias de mitigação de risco foram definidas com base no diagrama de decisão RCM3.

IV. ANÁLISE E DISCUSSÃO DE RESULTADOS

O novo plano de manutenção propõe a realização de 4 novas tarefas (não contempladas no plano do fabricante) e a alteração da periodicidade de realização de 2 tarefas já existentes, o que não é uma grande diferença face ao plano de manutenção existente. As novas ações propostas consistem na alteração da frequência de inspeção de 2 componentes, na inclusão da inspeção periódica de um componente que anteriormente não era efetuada, um teste de funcionamento (que também não era efetuado) e na substituição programa de um componente (que também não se encontrava planeada).

O plano de manutenção obtido prevê a realização de ações de manutenção programada (nomeadamente inspeções e substituições) para alguns dos componentes e corretiva (pós avaria) para a grande maioria dos componentes, e nenhuma tarefa de manutenção preditiva ou sob-condição. Os valores obtidos para os *MTBF* com os dados disponíveis (Tabela 1) são valores elevados e que são reveladores de um período de vida elevado (muito mais elevado do que a utilização média das viaturas) para os componentes a que se referem. Não obstante, os parâmetros obtidos para a distribuição de Weibull mostram que as falhas apresentam um caráter aleatório ($\beta \approx 1$) o que as torna impossíveis de prever. Recorrendo a bases de dados de vida de componentes, é possível confirmar que para a grande maioria dos componentes que constituem um sistema de refrigeração típico, os seus valores de *MTBF* são também geralmente elevados, o que suporta esta decisão de não efetuar manutenção sob-condição para estes componentes. Também na literatura é possível encontrar informação que confirma a pouca ou nenhuma utilização deste tipo de procedimentos de manutenção em sistemas de refrigeração, tal como refere James [10] que efetua uma revisão de literatura focada nos temas da fiabilidade, manutibilidade e disponibilidade cobrindo os aspetos mecânicos, elétricos e tribológicos de automóveis e que conclui que existem vários trabalhos relacionados com fiabilidade e análise de óleo de motor mas nenhum identificado que se relacionasse com a análise do óleo da transmissão ou com o líquido de refrigeração, apesar da sua importância para o desempenho geral do motor e das viaturas.

V. CONCLUSÕES

Fazendo um balanço do trabalho realizado, é possível tirar uma série de lições a respeito da manutenção do Sistema de refrigeração das Pandur II, quer ao nível do procedimento relativo ao registo e tratamento da informação respeitante às avarias, quer ao nível das tarefas de manutenção efetuadas, das quais resultaram um conjunto de propostas que se acredita trazerem melhorias para EP em termos da execução e gestão da manutenção do sistema de armas Pandur II e que pode ser estendido a todos os equipamentos do Exército. Tendo isto em consideração, para além do plano de manutenção proposto, este trabalho identificou a necessidade de melhorar o registo de falhas no Exército Português:

- Recomendação de obrigatoriedade de incluir informações relativas ao modo de falha nos registos de falha. Podem ser utilizados, por exemplo, os modos de falha identificados nesta dissertação;
- Recomendação de obrigatoriedade de incluir informações sobre Horas de Motor, Quilómetros e Horas do Trem de Potência nos registos de falha;
- Definição de um procedimento generalizado a ser utilizado na abertura e no encerramento das ordens de trabalho, de forma que o tempo de abertura corresponda efetivamente ao tempo desde a deteção da falha até a sua reparação;

Após a análise efetuada ao longo deste trabalho, é possível concluir que se trata de um sistema robusto, com vários componentes com poucas ou nenhuma falha, e no caso dos componentes com modos de falha mais recorrentes, apresentam valores elevados de *MTBF*. No caso destes últimos modos de falha, a determinação da distribuição de Weibull associada revelou valores do parâmetro β próximos de 1, confirmando que as taxas de falha revelam que os componentes se encontram na fase de vida útil, apresentando falhas aleatórias e difíceis de prever.

O plano de manutenção do fabricante também se mostrou adequado, necessitando apenas de alguns ajustes para mitigar os riscos associados aos modos de falha mais recorrentes, porém a impossibilidade de obtenção de valores de taxa de falha (ou *MTBF*) que forçaram a utilização de bases de dados, torna-se uma limitação, pois impede que sejam definidas ações de manutenção para esses componentes, com maior precisão e mais adequadas à realidade de utilização operacional desse sistema específico. Outra mais-valia desta dissertação reside no facto de ter mostrado que é possível realizar uma análise deste tipo, sem a necessidade de grandes investimentos e com recursos em ferramentas disponíveis no EP.

Em relação à aplicação da metodologia RCM3, esta trouxe algumas diferenças em relação à metodologia RCM2, nomeadamente:

- Foi considerado o contexto operacional do equipamento em análise, o que permitiu ter em consideração os requisitos operacionais associados à utilização das Pandur II
- Os modos de falha foram divididos em causa e mecanismo, identificando-se a falha concreta e a causa potencial que estará na sua origem;
- A análise de risco e o diagrama de decisão tiveram em consideração as consequências e a sustentabilidade ambiental;
- A descrição dos efeitos da falha é feita de forma mais detalhada e fornecendo mais informações para apoiar a decisão;
- O próprio diagrama de decisão RCM3 apresenta algumas diferenças face ao diagrama de decisão RCM2 na maneira como propõe lidar e tratar o risco.

Como trabalhos futuros, propõe-se na sequência deste artigo, a realização dos seguintes trabalhos:

- Estender a análise RCM3 a todo o sistema de armas Pandur II, tratando-o como um único sistema;
- Adotar esta metodologia para outros sistemas de armas do Exército Português;
- Sensibilização de todos os envolvidos na gestão e execução da manutenção de sistemas de armas para a importância de um registo mais preciso e objetivo das ordens de trabalho relativas às falhas, de forma a facilitar e permitir a recolha e tratamento de dados de fiabilidade;
- Analisar a viabilidade da aplicação de estratégias de manutenção preditiva relacionadas com a aplicação de modelos matemáticos e computacionais, envolvendo

modelos de inteligência artificial, ao sistema de refrigeração da Pandur II.

AGRADECIMENTOS

Os autores agradecem ao Capitão de Material André Graça, gestor da frota de Pandur II, à data da realização deste trabalho, pela disponibilidade em colaborar e fornecer os dados necessários acerca das falhas da Pandur. Agradecem também ao 1º Sargento Carlos Simões pela disponibilidade em colaborar na previsão dos tempos de reparação estimados.

REFERÊNCIAS BIBLIOGRÁFICA

[1] F.S.Nowlan and Howard Heap, "Reliability centred maintenance," 1978.

[2] SAE, *SAE JA1011 - Evaluation Criteria for Reliability-Centered Maintenance (RCM) Process*, vol. 4970. United States of America, 2009.

[3] SAE, *SAE JA1012- A Guide to the Reliability-Centered Maintenance (RCM) Standard*. Warrendale, Pensylvania, United States of America, 2002.

[4] J. Moubray, *RCM II - Reliability Centered Maintenance*, 2nd Editio. Oxford: Butterworth-Heinemann, 1999.

[5] M. Basson, *RCM 3: Risk-Based Reliability Centered Maintenance*. South Norwalk: Industrial Press, INC., 2018.

[6] BSI, *BS EN 60300-3-11 : 2009 Dependability Management — Reliability Centered Maintenance*. United Kingdom, 2009.

[7] R. Gondim and M. Duarte, "Aplicação da estatística na manutenção preditiva," *FAMAT em Rev.*, vol. 05, pp. 211–223, 2005.

[8] ReliaWiki, "The Weibull Distribution." [Online]. Available: http://reliawiki.org/index.php/The_Weibull_Distribution. [Accessed: 15-Sep-2020].

[9] D. N. Murthy, M. Xie, and R. Jiang, *Weibull Models*. New Jersey: John Wiley and Sons, Inc., 2004.

[10] A. T. James, "Reliability, availability and maintainability aspects of automobiles," *Life Cycle Reliab. Saf. Eng.*, no. 0123456789, 2020, doi: 10.1007/s41872-020-00130-3.

Índice de Autores

Almeida, João 18
André, António 18, 22

Baptista, António 32
Bernardino, Alexandre 37
Bernardo, Jóni 43
Borges, Maria Beatriz 47

Chambel, Énio 43, 63
Chambino, Luís 37
Correia, Miguel 26, 57
Costa, António 14

Dias, Luís 26, 57

Fernandes, Tiago 57
Filipe, Eduardo 14

Gomes, Gilberto 26

Infante, Virgínia 63

Martins, Maria João 32
Matias, Pedro 10, 14, 52
Moreira, Sérgio 47

Oliveira, Ricardo 32
Osório, Eduardo 10

Passos, Manuel 22
Pedro, José 10, 52
Pinto, Alexandre 22

Ramos, Tiago 18
Rita, Rui 52

Santos, Pedro 47
Silva, Carlos 43
Silva, Filipe 63
Silva, José 37



EXÉRCITO PORTUGAL

GNR GUARDA NACIONAL REPUBLICANA

ACADEMIA MILITAR MILITARY ACADEMY

CINAMIL MILITARY ACADEMY RESEARCH CENTER