Segurança da Informação nas Camadas Física e de Enlace em redes 5G e IoT: Uma Revisão Sistemática

Roger W. Coêlho, Elvio J. Leonardo, Luciana A. F. Martimiano e Ronan A. Silva

***Resumo*— As redes 5G e a Internet das Coisas (IoT) possibilitam novas oportunidades de negócios e serviços. A segurança da informação é uma preocupação constante, ainda mais quando novas tecnologias e protocolos são desenvolvidos. Diante disso, este artigo apresenta uma Revisão Sistemática (RS) sobre a segurança da informação nas camadas física e de enlace nas redes 5G e IoT. Como estratégia da revisão foram utilizadas *strings* de buscas nas bases digitais usadas pela comunidade científica e 23 estudos foram selecionados.**

***Palavras-Chave*— Redes 5G, Internet das Coisas (IoT), Software Defined NetWork (SDN), Network Function Virtualization (NFV), Reconhecimento de Padrão, Inteligência Artificial (IA), Revisão Sistemática.**

***Abstract*— 5G networks and the Internet of Things (IoT) can enable new business opportunities and services. Information security is a constant concern, even more so when new technologies and protocols are developed. Therefore, this paper presents a Systematic Review (SR) on information security in the physical and data link layers of 5G and IoT networks. As a review strategy, search strings were used in the digital databases used by the scientific community, and 23 studies were selected.**

***Keywords*— 5G Networks, Internet of Things (IoT), Software Defined NetWork (SDN), Network Function Virtualization (NFV), Pattern Recognition, Artificial Intelligence (AI), Systematic Review.**

I. Introdução

Mais pessoas acessam as redes de dados para enviar mensagens, efetuar ligações e para conectar-se à Internet. Nesse contexto, há uma grande expansão no consumo de dados pelos usuários [1]. Possuir uma infraestrutura capaz de transmitir as informações em altas velocidades e que permita o uso de equipamentos de Internet das Coisas (IoT) é uma forma de promover a evolução das aplicações existentes e de construir novos tipos de atividades para o desenvolvimento tecnológico da sociedade.

A comunicação celular denominada 5G, ou 5ª geração, não é apenas uma evolução das redes de dados, mas também, um sistema com muitas funcionalidades e novos serviços capazes de melhorar a transmissão da informação, permitindo alta demanda a recursos de rede. A rede 5G visa a busca pela menor latência e menor consumo de energia, justamente para facilitar a implementação e conexão de novos dispositivos e uso da IoT [2].

O uso de equipamentos em ambientes, como agro 4.0, cidades inteligentes, entre outros, exige requisitos complexos que incluem segurança da informação, recursos de rede eficiente e baixa latência, tudo isso combinado com automação, programação e gerenciamento da rede, permitindo que as informações sejam consumidas e transmitidas de forma confiável. A segurança da rede é um objeto crítico que deve possuir atenção, não somente na condução de protocolos, como também, com hardwares e softwares usados no 5G [3].

A segurança no 5G é importante pelo fato da rede ser projetada para uso intenso de equipamentos IoT, que possuem baixa capacidade energética e baixo processamento. Esses dispositivos são alvos preferidos dos cibercriminosos, ainda mais, quando, os dados transmitidos são essenciais para a análise de informações de uma determinada atividade crítica. Questões básicas de segurança, como confidencialidade, disponibilidade e integridade são os principais desafios na IoT e no 5G [4].

Técnicas como Software Defined Network (SDN), Virtualização de Função de Rede (NFV) e Inteligência Artificial (IA) contribuem para melhorar a eficiência do controle e bloqueio de possíveis atividades de cibercriminosos efetuadas nas redes 5G e IoT [5]. Analisar o uso dessas técnicas nas camadas física e de enlace é importante para que todo o sistema esteja seguro. Nota-se que existem poucos trabalhos na literatura que abordam o desenvolvimento de técnicas de segurança dedicados às camadas física e de enlace e que usam SDN, NFV e IA. Por isso, este trabalho contribui com uma Revisão Sistemática (RS) sobre discussões da segurança nestas camadas para as redes 5G e IoT, buscando estudos que usam técnicas de SDN, NFV e IA.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta as metodologias para o planejamento da revisão sistemática; a Seção 3 apresenta os resultados sobre a revisão sistemática; a Seção 4 apresenta as conclusões.

II. Metodologia

Nesta seção é apresentada a metodologia usada para a realização da RS. Todos os elementos usados como forma de elucidar quais foram os passos realizados para o desenvolvimento deste trabalho.

A RS segue os critérios apresentados em [6]. Vale salientar que esses princípios básicos podem ser genéricos, essenciais

Roger W. Coêlho, Departamento de Informática (DIN), Universidade Estadual de Maringá (UEM), Maringá-PR, e-mail: roger.coelho04@gmail.com; Elvio J. Leonardo, Departamento de Informática (DIN), Universidade Estadual de Maringá (UEM), Maringá-PR, e-mail: ejleonardo@uem.br; Luciana A. F. Martimiano, Departamento de Informática (DIN), Universidade Estadual de Maringá (UEM), Maringá-PR, e-mail: lafmartimiano@uem.br; Ronan A. Silva, Departamento de Informática, Instituto Federal do Paraná (IFPR), Pinhais-PR, e-mail: ronan.silva@ifpr.edu.br. Este trabalho é financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) (88887.668985/2022-00).

e válidos para qualquer RS. De acordo com as diretrizes, uma RS possui três etapas, planejamento, condução e relatório.

A primeira etapa, a de planejamento, refere-se à identificação da necessidade de uma RS. Embora existam estudos que visam a investigar problemas de segurança nas redes 5G e IoT, observa-se que não foi encontrada nenhuma revisão que considere as camadas física e de enlace. Nesse sentido, a RS apresentada aqui é oportuna e relevante.

A segunda etapa, dentro do planejamento, é o desenvolvimento do protocolo de revisão e a definição da ferramenta que será usada na RS, que neste caso é a StArt [7] desenvolvida pela UFSCar. O protocolo define o procedimento da etapa de condução, que inclui as ações de definição das questões de pesquisa, seleção da estratégia de busca, definição dos critérios de inclusão e exclusão dos estudos, definição dos critérios de avaliação da qualidade do estudo e finalmente seleção dos dados que serão extraídos dos estudos. O protocolo da RS é aprimorado durante todo o processo.

Uma parte importante e crucial para o desenvolvimento da RS passa pelas questões de pesquisas. Ao responder tais questionamentos é verificado se os objetivos, quanto aos estudos relevantes à temática pesquisada, são atingidos. A Tabela I, apresenta as questões usadas para identificação de estudos relevantes.

TABELA I
QUESTÃO PRINCIPAL (QP) E QUESTÕES SECUNDÁRIAS (QSS)

Id	Questões de Pesquisa
QP	**Quais são as pesquisas disponíveis na literatura que abordam a segurança da informação em redes 5G e IoT que têm como objetivo usar técnicas para evitar, mitigar e bloquear ataques nas camadas física e de enlace utilizando a SDN, NFV e a IA?**
QS1	Quais tipos de ataques nas camadas física e de enlace nas redes 5G e IoT os estudos têm considerado para a segurança da informação?
QS2	Quais técnicas de segurança da informação têm sido propostas para solucionar o problema de ataques nas camadas física e de enlace nas redes IoT e 5G?
QS3	Como os estudos existentes em redes 5G e IoT têm sido avalidados quanto à segurança da informação nas camadas física e de enlace (survey, experimentos, revisões sistemáticas, mapeamentos sistemáticos, estudo de caso, etc)?
QS4	Como o uso de *Software Defined Network* (SDN) e *Network Function Virtualization* (NFV) contribuem para o gerenciamento da segurança da informação em redes 5G e IoT?
QS5	Como a Inteligência Artificial (IA) pode ser usada para o reconhecimento de padrões de possíveis ataques nas camadas física e de enlace das redes 5G e IoT?

Após a etapa de protocolo, o próximo passo foi a de buscas por estudos em bases amplamente usadas pela comunidade científica, que indexam periódicos e conferências em segurança da informação em redes 5G e IoT. Nesta RS, foi decidido que os estudos fossem encontrados de forma automatizada por meio de *strings* de buscas. As fontes selecionadas são as bibliotecas digitais: ACM Digital Library; IEEE Xplorer; Springer; Science Direct; e Web of Science.

As fontes das bases digitais fornecem oportunidades de realizar uma pesquisa sofisticada por meios das *strings* de buscas com a combinação de operadores booleanos. As *strings* usadas em cada bases de dados são:

- **ACM Digital Library**: “Information Security AND ("5G"OR "IoT") AND (Physical Layer OR MAC Layer) AND ("software defined network"OR "network function virtualization"OR "pattern recognition")”;
- **IEEE Xplorer**: “Information Security AND ("5G"OR "IoT") AND (Physical Layer OR MAC Layer)”. “(5G OR IoT) AND ("software defined network"OR "network function virtualization"OR "pattern recognition")”;
- **Springer**: “Information AND Security AND (5G AND IoT) AND (Physical Layer OR MAC Layer) AND ("software defined network"OR "network function virtualization"OR "pattern recognition")”;
- **Science Direct**: “Information AND Security AND ("5G"AND "IoT") AND (Physical Layer OR MAC Layer) AND ("software defined network"OR "network function virtualization"OR "pattern recognition")”;
- **Web of Science**: “(((((((ALL=(5G)) AND ALL=(IoT)) AND ALL=(Information Security)) AND ALL=(Link Layer)) AND ALL=(Physical Layer)) AND ALL=(Network Access Layer)) AND ALL=(pattern recognition)) OR ALL=(SDN) OR ALL=(NFV)”.

Todas as buscas são baseadas em termos relevantes na área pesquisada, que muitas vezes são usadas em título, resumo e palavras-chave. Essa estratégia visa evitar que muitos estudos irrelevantes sejam retornados como possíveis resultados válidos. Após a realização das buscas, os critérios de inclusão e exclusão devem ser aplicados como forma de seleção dos estudos que farão parte do RS. Os critérios de seleção são apresentados a seguir:

- **Critérios de Inclusão**:
  - (I) Estudos que consideram a segurança da informação nas camadas física e de enlace nas redes 5G e IoT;
  - (I) Trabalhos na língua inglesa para citação e atualização referente a revisão sistemática;
  - (I) Trabalhos que usam *Software Defined Network* (SDN), *Network Function Virtualization* (NFV) e reconhecimento de padrões;
  - (I) Estudos com mais de quatro páginas;
  - (I) Trabalhos publicados a partir de 2010.
- **Critérios de Exlusão**:
  - (E) Estudos que não consideram a segurança da informação nas camadas física e de enlace nas redes 5G e IoT;
  - (E) Estudos que não estejam na língua inglesa;
  - (E) Chamadas de periódicos ou eventos para enviar trabalhos;
  - (E) Trabalhos que não usam *Software Defined Network* (SDN), *Network Function Virtualization* (NFV) e reconhecimento de padrões;
  - (E) Estudos com menos de quatro páginas;
  - (E) Trabalhos com *score* igual a zero;
  - (E) Trabalhos publicados antes de 2010.

Vale salientar que alguns estudos que possuem *score* igual a zero atribuídos pela ferramenta StArt foram aproveitados pelo fato de possuírem relevância. Ao utilizar ferramentas de auxílio para o desenvolvimento da RS, é necessário a avaliação criteriosa dos estudos, mesmos daqueles que porventura não

atinjam o *score* desejado durante a atribuição da *string* de busca.

Os critérios de avaliação de qualidade são definidos para garantir que todos os estudos incluídos na RS atinjam um nível aceitável de qualidade. Os seguintes critérios de qualidade foram atribuídos para a avaliação da qualidade dos estudos:

- 3 pontos para expressões encontradas no título;
- 2 pontos para expressões encontradas no resumo;
- 1 ponto para expressões encontradas em palavras-chave;
- 0 pontos para nenhuma expressão encontrada.

O último passo, relacionado ao desenvolvimento do protocolo de RS, é a seleção das características dos dados que foram extraídos dos artigos encontrados na pesquisa. Os recursos usados estão listados a seguir:

- Título;
- Autores;
- Ano de publicação;
- Repositório de publicação;
- Tipo de veículo de publicação;
- Quais tipos de ataques;
- Tipos de técnicas em segurança da informação;
- Automatização da segurança por SDN e NFV;
- Uso da inteligência artificial para reconhecimento de padrões de ataques.

Após o processo de busca inicial, foram encontrados 4059 estudos e destes somente 143 foram pré-selecionados. Por meio do uso da ferramenta, estudos duplicados foram removidos. Após a realização da leitura dos títulos e resumos dos estudos candidatos, apenas 23 trabalhos foram selecionados. Em seguida, foi realizado a leitura dos 23 trabalhos, na íntegra, o que permitiu que o número final de trabalhos selecionados fosse exatamente os 23 estudos.

III. Resultados

Nesta seção são apresentados os resultados obtidos pela RS. Os dados resultantes da pesquisa foram compilados na ferramenta StArt. Após, foram usadas as informações para o detalhamento e escolha de estudos significativos para a presente RS.

Na primeira etapa, as bases da ACM Digital Library, IEEE Xplorer, Springer, Science Direct e Web of Science, foram usadas para retornar estudos provenientes das *strings*, que foram utilizadas em cada mecanismo de pesquisa. No primeiro momento, um total de 4059 estudos foram retornados para serem analisados.

A base que obteve mais retorno de estudos foi a Web of Science, com um total de 1845 trabalhos; a ACM Digital Library obteve como retorno 249 estudos, sendo a base de dados que apresentou menor número de trabalhos regressados. Esses dados foram obtidos após a verificação de estudos duplicados por meio da ferramenta StArt.

Na segunda etapa foi realizada a aplicação dos critérios de inclusão e exclusão nos estudos em cada base de dados. Esses critérios contribuem para a verificação da relevância dos trabalhos, conforme informações pré-definidas por estes critérios como parte da elaboração da RS.

Um total de 3916 estudos foram rejeitados com base no uso dos critérios de exclusão, ou seja, esses trabalhos foram considerados com pouca ou nenhuma relevância para a RS. Um total de 143 estudos foram pré-selecionados para serem analisados e posteriormente lidos os resumos e os textos na íntegra. Esses dados mostram que apesar das *strings* de busca das bases retornarem vários trabalhos muitos não atingiram as condições de relevância para a RS.

Nos 143 estudos selecionados foram aplicados os critérios de inclusão e exclusão para a seleção dos trabalhos mais relevantes. Nessa etapa, houve a leitura dos resumos e títulos integralmente, e foram selecionados 23 estudos, um total de 120 estudos foram rejeitados.

A Tabela II mostra por quais critérios de exclusão os 120 trabalhos foram rejeitados.

TABELA II
EXTRAÇÃO - ESTUDOS REJEITADOS

Critério	Frequência	Porcentagem
Estudos que não consideram a segurança da informação nas camadas física e de enlace nas redes 5G e IoT	102	85%
Trabalhos que não usam *Software Defined Network* (SDN), *Network Function Virtualization* (NFV) e reconhecimento de padrões	40	33,33%
Estudos com menos de quatro páginas	4	3,33%
Trabalhos com score igual a zero	26	21,67%

A maioria dos estudos foi rejeitada pelo critério de exclusão: "estudos que não consideram a segurança da informação nas camadas física e de enlace nas redes 5G e IoT". Apesar das bases de dados retornarem trabalhos de segurança sobre as redes 5G e IoT, a maioria não tratava da segurança nas camadas física e de enlace. Um outro critério de exclusão que também se destacou foi o de estudos que não usam SDN, NFV e reconhecimento de padrões. Estudos que possuem baixa classificação, quanto ao retorno das *strings* de buscas, foram excluídos da RS. Alguns estudos que foram classificados inicialmente como relevantes, após a leitura na integra foram excluídos devido algum critério de exclusão.

A Tabela III mostra por quais critérios de inclusão os 23 trabalhos foram aceitos.

TABELA III
EXTRAÇÃO - ESTUDOS ACEITOS

Critério	Frequência	Porcentagem
Estudos que consideram a segurança da informação nas camadas física e de enlace nas redes 5G e IoT	23	100%
Trabalhos na língua inglesa para citação e atualização referente a revisão sistemática	23	100%
Trabalhos que usam *Software Defined Network* (SDN), *Network Function Virtualization* (NFV) e reconhecimento de padrões	12	52,17%
Estudos com mais de quatro páginas	23	100%
Trabalhos publicados a partir de 2010	23	100%

Vale ressaltar que, apesar de alguns artigos não atenderem

ao critério de inclusão sobre SDN, NFV e reconhecimento de padrões, eles foram selecionados por possuírem importância quanto ao critério sobre segurança na camada física e de enlace das redes 5G e IoT.

Os 23 trabalhos selecionados possuem mais de quatro páginas e estão compreendidos entre 2016 e 2021. Isso mostra que os estudos sobre a camada física e de enlace nas redes 5G com uso de equipamentos IoT são relativamente recentes.

Como próxima etapa, os 23 estudos foram lidos na íntegra para uma nova verificação se algum critério de exclusão pudesse ser novamente aplicado. Porém, não foi identificado nenhum critério de exclusão que pudesse ser usado para remoção de algum trabalho. A Tabela IV apresenta os 23 estudos selecionados.

TABELA IV
ESTUDOS EXTRAÍDOS DA REVISÃO SISTEMÁTICA

Estudos	Base de Dados	Ano da Publicação
[3]	Science Direct	2020
[8]	IEEE Xplorer	2021
[9]	IEEE Xplorer	2018
[5]	IEEE Xplorer	2020
[10]	Science Direct	2021
[11]	IEEE Xplorer	2018
[12]	IEEE Xplorer	2020
[13]	Science Direct	2019
[14]	IEEE Xplorer	2021
[15]	Science Direct	2020
[4]	ACM Digital Library	2018
[16]	IEEE Xplorer	2016
[17]	IEEE Xplorer	2018
[18]	IEEE Xplorer	2017
[19]	IEEE Xplorer	2021
[20]	IEEE Xplorer	2018
[21]	IEEE Xplorer	2016
[22]	IEEE Xplorer	2017
[23]	IEEE Xplorer	2021
[24]	IEEE Xplorer	2020
[25]	IEEE Xplorer	2021
[26]	Science Direct	2018
[27]	IEEE Xplorer	2019

Ao todo, dezessete dos vinte e três estudos selecionados, foram extraídos da base de dados do IEEE Xplorer. Por sua vez, cinco estudos foram extraídos da Science Direct e a ACM Digital Library possui um estudo selecionado. As bases da Web of Science e Springer não tiveram estudos selecionados pela RS, ao passo que os trabalhos foram removidos pelos critérios de exclusão.

Ao analisar os estudos percebe-se que há possibilidades de aprofundamento e realização de trabalhos explorando a segurança das redes 5G e IoT nas camadas física e de enlace. Como constatações positivas, os estudos encontrados abrem possibilidades de pesquisas para os cientistas que estão preocupados com esse tema ou que querem ser inseridos neste grupo de pesquisadores. Tais possibilidades podem ser empreendidas em técnicas que usam SDN, NFV e reconhecimento de padrões, para a automação da segurança da rede.

Explorar possíveis ataques do dia zero, e reconhecer o seu padrão nas camadas física e de enlace, permite que a automação da segurança seja realizada por meio da programação de rede usando o SDN e NFV. Alguns dos trabalhos selecionados exploram ataques conhecidos nas camadas física e de enlace por meio do uso de técnicas de IA. Isso possibilita, o destaque de que, a área de IA pode oferecer contribuições e impactar na identificação de ataques e automatização da segurança nas redes 5G e IoT.

Outro ponto que pode ser explorado é a análise do protocolo que a rede 5G e IoT foram projetadas para a identificação de possíveis erros que podem causar prejuízo quanto a segurança da informação. Estudos quando a análise da segurança de protocolos em novas tecnologias de transmissão e arquiteturas de redes emergentes, podem contribuir no processo de automatização e segurança das redes.

Como trabalhos futuros, serão desenvolvidos estudos sobre técnicas de automatização da segurança das camadas física e de enlace nas redes 5G e IoT, tendo como ferramentas de auxílio o SDN, NFV e reconhecimento de padrões, como forma de mitigar, evitar e bloquear possíveis problemas de segurança.

A. Trabalhos Selecionados na RS

Nesta subseção são apresentados alguns trabalhos desenvolvidos pela comunidade acadêmica que foram identificados durante o processo de RS. Dessa forma, podem ser elucidadas algumas informações pertinentes sobre o estado da arte e quais são os procedimentos usados pelos autores na elaboração dos seus estudos.

Uma proposta usa técnicas de SDN, NFV e IA para realizar uma abordagem contra-ataques de segurança nas redes 5G, com o objetivo de criar um Sistema de Detecção de Intrução (IDS) baseado em multicamadas [15]. O sistema proposto permite a verificação, mitigação e bloqueio de diferentes ataques de segurança, como *Spoofing*, Sobrecarga de tabela de fluxo, Negação de Serviço (DoS), *Control Plane Saturation* e Sequestro de Localização de *host*.

A proposta de um algoritmo que visa a recomendação para os requisitos de privacidade de um dispositivo conectado na rede 5G e IoT por meio do *Location-based Services* (LBS) é descrito em [8]. Os autores apresentam um protocolo de autenticação cruzada, o qual é base do uso do algoritmo. Nesse protocolo, as autenticações são realizadas por meio da camada física especificando chaves de autenticação entre os dispositivos e os terminais da rede 5G.

Em [23] é apresentado um novo esquema de detecção de ataques, do tipo *Spoofing*, baseado na representação virtual de canal em redes 5G. Existem duas estratégias de detecção, uma para ambientes de rádio estático por meio de teste de Neyman-Pearson (NP), e outra para rádio dinâmico, em que, a correlação de canais está mudando constantemente. Nesse caso, a estrutura de detecção é *online* baseada em uma Rede Neural *feedforward* com uma única camada oculta.

A proposta apresentada em [25] é um *framework* que tem como objetivo usar a técnica de V-MIMO (*Virtual Multiple-Input Multiple-Output*) para identificação de possíveis vulnerabilidades na camada física de redes IoT com sensores de baixa potência centrados na rede 5G. Esse *framework* apresenta uma técnica transferência de energia e informações seguras com o uso do V-MIMO, permitindo que os sensores vizinhos sejam

reunidos como um *cluster* para operar cooperativamente para a recepção e transmissão de dados.

IV. Conclusões

A análise dos resultados mostra estudos relevantes na área de segurança da informação em redes 5G e IoT. É fato que, a sociedade como a conhecemos, está passando por um processo de evolução tecnológica caracterizado pelas novas tecnologias de transmissão de redes de dados, como o 5G e IoT, que permitem transmitir informações de todas os tipos de serviços possíveis.

Assim, realizou-se uma RS direcionada ao tema específico: segurança da Informação nas camadas física e de enlace em redes 5G e IoT. Foram elaboradas seis questões de pesquisas com o intuito de obter respostas e retornar possíveis estudos na temática pesquisada. Ao todo 23 estudos foram identificados, que podem ser utilizados como fonte de pesquisa para desenvolvimentos de trabalhos na área de segurança da informação nas camadas física e de enlace das redes 5G e IoT.

A RS mostrou que alguns pesquisadores estão trabalhando em projetos que têm como base a segurança nas camadas física e de enlace no 5G e IoT, outros publicaram *surveys* e taxonomia para relatar sobre o assunto. Como constatações positivas, os estudos encontrados abrem possibilidades de pesquisas em segurança da informação para tecnologias de transmissão emergentes, no caso o 5G e IoT. Isso permite que, novas técnicas, algoritmos e protocolos surjam, contribuindo para que a comunidade de segurança da informação possa disponibilizar soluções para problemas que podem causar prejuízos nas redes 5G e IoT.

Agradecimentos

Este trabalho é financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) (88887.668985/2022-00).

Referências

[1] Tiago Varum, Amélia Ramos, and João N. Matos. *Planar microstrip series-fed array for 5G applications with beamforming capabilities*. In *2018 IEEE MTT-S International Microwave Workshop Series on 5G Hardware and System Technologies (IMWS-5G)*, pages 1–3, agosto, 2018.

[2] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Security for 5g mobile wireless networks. *IEEE Access*, 6:4850–4874, 2018.

[3] Sabrina Sicari, Alessandra Rizzardi, and Alberto Coen-Porisini. 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, 179:107345, outubro, 2020.

[4] Hamed Rahimi, Ali Zibaeenejad, Parsa Rajabzadeh, and Ali Akbar Safavi. On the Security of the 5G-IoT Architecture. In *Proceedings of the international conference on smart cities and internet of things - SCIOT '18*, pages 1–8, Mashhad, Iran, 2018. ACM Press.

[5] Rabia Khan, Pardeep Kumar, Dushantha Nalin K. Jayakody, and Madhusanka Liyanage. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Commun. Surv. Tutorials*, 22(1):196–248, 2020.

[6] Georgios Spanos and Lefteris Angelis. The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58:216–229, maio, 2016.

[7] UFSCar. *StArt*. disponível em: http://lapes.dc.ufscar.br/resources-and-downloads/tools, janeiro, 2022.

[8] Hua Zhao, Mingyan Xu, Zhou Zhong, and Ding Wang. A fast physical layer security-based location privacy parameter recommendation algorithm in 5G IoT. *China Commun.*, 18(8):75–84, agosto, 2021.

[9] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong, and Xiqi Gao. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Select. Areas Commun.*, 36(4):679–695, abril, 2018.

[10] G.C. Amaizu, C.I. Nwakanma, S. Bhardwaj, J.M. Lee, and D.S. Kim. Composite and efficient DDoS attack detection framework for B5G networks. *Computer Networks*, 188:107871, abril, 2021.

[11] Ihsan H. Abdulqadder, Deqing Zou, Israa T. Aziz, and Bin Yuan. Enhanced Attack Aware Security Provisioning Scheme in SDN/NFV Enabled over 5G Network. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–9, Hangzhou, julho, 2018. IEEE.

[12] Xingwang Li, Huang Mengyan, Yuanwei Liu, Varun G Menon, Anand Paul, and Zhiguo Ding. I/Q Imbalance Aware Nonlinear Wireless-Powered Relaying of B5G Networks: Security and Reliability Analysis. *IEEE Trans. Netw. Sci. Eng.*, pages 1–1, 2020.

[13] Rasheed Hussain, Fatima Hussain, and Sherali Zeadally. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*, 101:843–864, dezembro, 2019.

[14] Xi Li, Carlos Guimaraes, Giada Landi, Juan Brenes, Josep Mangues-Bafalluy, Jorge Baranda, Daniel Corujo, Vitor Cunha, Joao Fonseca, Joao Alegria, Aitor Zabala Orive, Jose Ordonez-Lucena, Paola Iovanna, Carlos J. Bernardos, Alain Mourad, and Xavier Costa-Perez. Multi-Domain Solutions for the Deployment of Private 5G Networks. *IEEE Access*, 9:106865–106884, 2021.

[15] Ihsan H Abdulqadder, Shijie Zhou, Deqing Zou, Israa T. Aziz, and Syed Muhammad Abrar Akber. Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Computer Networks*, 179:107364, outubro, 2020.

[16] Saoreen Rahman, Shamim Al Mamun, Mahtab Uddin Ahmed, and M. Shamim Kaiser. PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pages 2531–2536, Chennai, India, março, 2016. IEEE.

[17] Pooja Singh, Praveen Pawar, and Aditya Trivedi. Physical Layer Security Approaches in 5G Wireless Communication Networks. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 477–482, Jalandhar, India, dezembro, 2018. IEEE.

[18] Fei Pan, Yixin Jiang, Hong Wen, Runfa Liao, and Aidong Xu. Physical Layer Security Assisted 5G Network Security. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, Toronto, ON, setembro, 2017. IEEE.

[19] Anil Kumar Yerrapragada, Taylor Eisman, and Brian Kelley. Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications. *IEEE Open J. Commun. Soc.*, 2:2232–2242, 2021.

[20] Yuan Gao, Su Hu, Wanbin Tang, Yi Li, Yunchuan Sun, Dan Huang, Shaochi Cheng, and Xiangyang Li. Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges. *IEEE Access*, 6:26350–26357, 2018.

[21] Sreeram Munisankaraiah and A Arun Kumar. Physical layer security in 5G wireless networks for data protection. In *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, pages 883–887, Dehradun, India, outubro, 2016. IEEE.

[22] Li Sun and Qinghe Du. Physical layer security with its applications in 5G networks: A review. *China Commun.*, 14(12):1–14, dezembro, 2017.

[23] Weiwei Li, Ning Wang, Long Jiao, and Kai Zeng. Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks. *IEEE Access*, 9:60419–60432, 2021.

[24] Ning Wang, Long Jiao, Amir Alipour-Fanid, Monireh Dabaghchian, and Kai Zeng. Pilot Contamination Attack Detection for NOMA in 5G mm-Wave Massive MIMO Networks. *IEEE Trans.Inform.Forensic Secur.*, 15:1363–1378, 2020.

[25] Ankita Jaiswal, Sushil Kumar, Omprakash Kaiwartya, Neeraj Kumar, Houbing Song, and Jaime Lloret. Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications. *IEEE Systems Journal*, 15(2):2810–2821, junho, 2021.

[26] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 101:55–82, janeiro, 2018.

[27] Jie Chang, Yihan Xiao, and Zhen Zhang. Wireless Physical-Layer Identification Assisted 5G Network Security. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–5, Paris, France, abril, 2019. IEEE.