Desafios de Segurança para Verticais de Aplicação em Redes 5G

Álvaro Sobrinho, Matheus Vilarim, Amanda Barbosa, Danilo F. S. Santos e Edmar Candeia Gurjão

***Resumo*— Neste artigo são apresentados desafios de segurança para sistemas de comunicação móveis de quinta geração (5G) e suas verticais de aplicação. Foram categorizadas ameaças relacionadas com verticais de aplicação, como, por exemplo, cidades inteligentes e Indústria 4.0. Árvores de ataque e defesa foram definidas para discutir de maneira mais aprofundada sobre alguns ataques identificados. Com base nos resultados obtidos, é possível destacar a relevância de um conjunto de ameaças e ataques. Por exemplo, ataques de negação de serviços são bastante críticos para todas as verticais de aplicação.**

***Palavras-Chave*— Verticais de Aplicação, Segurança, 5G.**

***Abstract*— This paper presents security challenges for fifth-generation mobile communication systems (5G) and vertical applications. We categorized threats to vertical applications, such as smart cities and Industry 4.0. We defined attack and defense trees to discuss some identified attacks further. Based on our results, it is possible to highlight the relevance of a set of threats and attacks. For instance, denial-of-service attacks are very critical for all vertical applications.**

***Keywords*— vertical applications, Security, 5G.**

I. Introdução

A implantação de infraestruturas para o uso dos sistemas de comunicação móveis de quinta geração (5G) é necessária e, portanto, estudos sobre verticais de aplicação são relevantes. Comunicações 5G possibilitam mais largura de banda, baixa latência e cobertura ampla de sinais [1]. Com isso, provê suporte para várias verticais, tais como saúde e cidades inteligentes, sistemas de energia e sistemas de transporte. Entretanto, considerando que software é parte fundamental da nova arquitetura de redes 5G, segurança e privacidade são atributos críticos. Além disso, o 5G utiliza uma série de novas tecnologias que incluem *Network Slicing* (NS), *Software Defined Networks* (SDN), *Network Function Virtualization* (NFV) e *Multi-Access Edge Computing* (MEC).

Neste contexto, a academia, indústria e outros atores necessitam de uma visão geral e crítica de tecnologias associadas com a segurança e privacidade em redes 5G, considerando os diversos cenários de ameaça. Redes 5G estão sujeitas a diversos ataques, seja pela possibilidade de interconexão entre vários objetos com a Internet, ou pela maior possibilidade de utilização em ambientes de infraestrutura crítica. Por exemplo, a conexão entre dispositivos na Internet das coisas (*Internet of Things* - IoT) pode resultar em vulnerabilidades nas redes 5G visto que muitos desses elementos são implementados com *hardware* e software genéricos e sem tratamento de segurança [2].

Verticais de aplicação habilitadas por redes 5G trazem novos desafios de segurança e privacidade que podem comprometer os consumidores e provedores de serviços. Neste contexto, a análise de desafios de segurança e a apresentação de soluções para mitigação de problemas são relevantes. Entretanto, existem poucos estudos publicados na literatura científica com discussões abrangentes com foco na segurança e privacidade de verticais de aplicação. Autores geralmente discutem sobre desafios relacionados a verticais específicas, como IoT industrial (por exemplo, os estudos apresentados por Jiang *et al.* [3] e Varga *et al.* [4]). Outros exemplos de trabalhos relacionados possuem foco em desafios de segurança relacionados com MEC [5], [6] e NS [7].

Portanto, neste artigo são discutidos desafios de segurança para 5G e verticais de aplicação. As principais contribuições com este estudo, no contexto de verticais de aplicação e 5G, são: (1) uma discussão sobre ameaças e ataques conhecidos; (2) uma discussão sobre soluções para a mitigação ameaças e ataques identificadas na literatura; e (3) apresentação de árvores de ataques e defesa para verticais de aplicação.

O restante deste artigo está organizado da seguinte maneira. Nas Seções II e III são apresentados exemplos de ameaças/ataques e soluções identificados na literatura, respectivamente. Na Seção IV, alguns ataques e possíveis soluções são mapeados usando árvores de ataque e defesa. Por fim, na Seção V são apresentadas conclusões.

II. Principais Ameaças e Ataques Identificados

As seguintes ameaças gerais podem ser destacadas: *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), dispositivos zumbis, personificação, sequestro, redirecionamento, varredura, *botnets*, falsificação, *malware*, contaminação piloto, esgotamento de recursos e buracos de minhoca adaptativos. Com base no estudo realizado, os ataques de *downgrade* são outras ameaças relevantes que podem ser destacadas. Por exemplo, se um adversário forçar o *downgrade* do 5G para redes de gerações anteriores, uma vertical de aplicação ficará vulnerável a ameaças não resolvidas, como, por exemplo, *International Mobile Subscriber Identity (IMSI) Catchers* [8].

As ameaças DoS e DDoS são bastante críticas para todas as verticais de aplicação destacadas. Por exemplo, na saúde inteligente, a indisponibilidade de serviços pode resultar na falta de atendimento/tratamento de um paciente. As seguintes ameaças podem ser destacadas para cada vertical de aplicação:

Álvaro Sobrinho, Ciência da Computação, Universidade Federal do Agreste de Pernambuco, Garanhuns-PE, e-mail: alvaro.alvares@ufape.edu.br; Matheus Vilarim, Amanda Barbosa, Danilo F. S. Santos e Edmar Candeia Gurjão, Universidade Federal de Campina Grande, Campina Grande-PB, e-mail: matheus.vilarim@ee.ufcg.edu.br; amanda.silva@ee.ufcg.edu.br; danilo.santos@dee.ufcg.edu.br; ecg@dee.ufcg.edu.br. Este trabalho foi parcialmente financiado pela TED 413068 ANATEl-UFCG .

- **Cidades inteligentes:** composta por um conjunto de dispositivos embutidos (sensores e atuadores) controlados por um ponto central. Aplicações de cidades inteligentes dependem de sensores distribuídos por diferentes coisas (por exemplo, um ônibus) para melhorar a eficiência e a qualidade do gerenciamento. Esta vertical de aplicação é bastante dependente de IoT (por exemplo, *Internet of Drones* (IoD)) e acesso sem fio de tecnologias subjacentes, como *Software Defined Radio* (SDR) e *Cognitive Radio* (CR), para a coleta inteligente de informações em ambientes dinâmicos e heterogêneos. Um adversário pode maliciosamente (1) usar bandas de espectro de maneira não autorizada, (2) saturar o canal de controle cognitivo, (3) comprometer dispositivos IoT diretamente ou por meio de uma conexão remota, (4) afetar a detecção de espectro, (5) interromper o mecanismo CR, (6) extrair dados de configuração de SDR no contexto da camada física, (7) transmitir mensagens entre drones alegando ser um retransmissor de rede, (8) usar uma interface maliciosa drone para obter acesso a comunicação entre drones legítimos e transmitir assinaturas repetidas ou atrasadas para se verificar ao líder da rede, (9) interromper a operação dos drones para impedir serviços (por exemplo, entrega de produtos) e (10) usar ferramentas SDR de baixo custo para gerar sinais falsos com navegação falsa e enganar o *Global Positioning System* (GPS) dos drones para calcular posições falsas.
- **Indústria 4.0:** a quarta revolução industrial depende de conceitos como sistemas ciberfísicos, IoT e computação em nuvem para melhorar a eficiência e a produtividade. Assim, IoT industrial e os sistemas ciberfísicos são discutidos neste artigo como parte da Indústria 4.0. Um adversário pode maliciosamente (1) atualizar e redefinir indevidamente equipamentos industriais, (2) tornar equipamentos industriais indisponíveis, (3) ataques em tempo real em ambientes ciber-físicos de sistemas industriais que interrompem/danificam a infraestrutura física ou degradam o desempenho injetando dados falsos por usuários mal-intencionados, (4) atualização não autorizada de subsistemas legados na planta, (5) usar certificados de *hardware* comprometidos ou código malicioso inativo para realizar ataques, (6) instalar software indesejado em dispositivos industriais, (7) realizar uma conexão de dispositivo indesejada a uma rede de fábrica, (8) realizar acesso não autorizado a recursos de fábrica (por exemplo, rede e armazenamento/recuperação de dados), (9) realizar acesso não autorizado a recursos de fábrica durante a transferência entre domínios de segurança que executam sua rede núcleo, (10) comprometer a frequência de comunicação ou uso de espectro de diferentes pares transmissores-receptores próximos no ambiente de produção e (11) executar comandos não autorizados na planta.
- **Transporte inteligente:** vertical relacionada com cidades inteligentes. O transporte inteligente pode incluir, por exemplo, carros inteligentes e sistemas ferroviários inteligentes. Esta vertical de aplicação está relacionada também com conceitos como Internet de veículos (*Internet of Vehicles - IoV*) e é bastante dependente de redes veiculares. Um adversário pode maliciosamente (1) transmitir informações sem sentido ou falsas para manipular outros veículos, (2) executar ataques de falsificação do sistema de posicionamento global para enganar veículos inocentes, (3) realizar ataques DoS na IoV, (4) prejudicar a disponibilidade de veículos e serviços de redes, (5) aproveitar veículos maliciosos e comprometidos para publicar informações falsas para causar danos ao sistema, (6) forjar a identidade e afirmar ser um veículo autêntico e válido usando o identificador na rede (representação de nó), (7) usar veículos maliciosos para adicionar intervalos de tempo de atraso à mensagem transmitida sem nenhuma alteração (veículos vizinhos recebem mensagens sensíveis ao tempo quando não são mais necessárias), (8) monitorar e analisar o tráfego de rede e roubar informações confidenciais do veículo (por exemplo, localização do veículo e identidade - a *Road Side Unit* (RSU) é uma superfície de ataque), (9) comportar-se como uma RSU e (10) interferir na transmissão impedindo a comunicação entre veículos em um alcance de transmissão e recepção.
- **Serviço público**: vertical que também se relaciona com cidades inteligentes, dado que uma cidade requer serviços como, por exemplo, segurança pública e aplicações táticas. Esta vertical também se relaciona com conceitos como o IoD. Um adversário pode maliciosamente (1) acessar equipamentos ou dispositivos do usuário em uma bolha tática, (2) vazar informações operacionais sobre as capacidades dos agentes de segurança pública (por exemplo, número de agentes ou drones em campo, dados do dispositivo e localização), (3) interromper os serviços de segurança pública, (4) espionar e bloquear (interferir) atividades táticas, (5) comprometer e assumir o controle de drones (por exemplo, usando armas embutidas), (6) usar drones maliciosos para atacar nós do MEC e roubar informações táticas e (7) relatar dados falsos de GPS para violar o regulamento da zona de exclusão aérea e/ou causar riscos de colisão.
- **Rede elétrica inteligente**: vertical relacionada com cidades inteligentes, dado que os avanços tecnológicos nas redes elétricas se relacionam com as redes inteligentes. Por exemplo, *Smart Energy Meters* (SEM) podem ser instalados em residências de comunidades para medir o consumo de energia para fins de cobrança. Um adversário pode maliciosamente (1) espionar o SEM doméstico, (2) modificar o SEM doméstico, (3) interromper o SEM doméstico, (4) desequilibrar a carga de energia para fornecer informações enganosas às entidades de borda e (5) conectar-se aos dados mais próximos do *gateway* do plano de dados para realizar ataques físicos na rede elétrica. Além disso, no contexto do SEM, uma vez que o invasor intercepta os dados de consumo de energia (ou seja, escuta o SEM doméstico), é possível inferir o comportamento das pessoas em uma residência da comunidade para realizar assaltos.
- **Saúde inteligente**: vertical relevante, que possui o potencial de auxiliar na melhoraria do diagnóstico, monitoramento e tratamento de pacientes. Portanto, as aplicações lidam com informações clínicas muito confidenciais

e privadas. Essa vertical está relacionada com cidades inteligentes. Aplicações de saúde inteligente reutilizam a infraestrutura da cidade inteligente para fornecer cuidados de saúde com mais eficiência na vida diária dos cidadãos. Um adversário pode (1) vazar dados confidenciais de forma maliciosa para causar perdas financeiras a estabelecimentos de saúde, (2) vazar dados confidenciais para expor a privacidade dos pacientes, (3) interromper serviços de saúde (por exemplo, cirurgias remotas), (4) comprometer a disponibilidade de dados para comprometer o tratamento de pacientes, (5) realizar movimentação de itens valiosos em um estabelecimento de saúde, (6) realizar a adulteração de dados clínicos para comprometer o tratamento de pacientes e (7) degradar a qualidade de serviços de saúde.

- **Agricultura inteligente**: vertical relacionada com os avanços tecnológicos na agricultura. O objetivo é otimizar atividades como o gerenciamento do processo de plantação. Um adversário pode (1) adulterar os sensores da fazenda para causar danos, (2) acessar sistemas agrícolas (por exemplo, sistema de apoio à decisão e drones), (3) falsificar dados para interromper o funcionamento dos sistemas agrícolas (por exemplo, setores de cultivo ou pecuária), (4) interromper a disponibilidade de dados de posicionamento/clima e (5) degradar a qualidade de serviços de monitoramento de plantações. Da mesma forma que cidades inteligentes e serviços públicos, as ameaças de drones também afetam essa vertical. Por exemplo, drones em um IoD podem monitorar plantações remotamente.

Além das verticais de aplicação discutidas acima, com base em exemplos de ameaças, outras podem ser beneficiadas por redes 5G. Por exemplo, educação inteligente é uma vertical relevante para setores públicos e privados, que podem impactar positivamente no aprendizado de estudantes. Algumas superfícies de ataque são tecnologias imersivas, como realidade aumentada e realidade virtual.

III. Exemplos de Soluções

Algumas das soluções identificadas neste estudo focam na segurança e privacidade em redes 5G e verticais de aplicação, como, por exemplo, transporte inteligente [9], indústria 4.0 [10], cidades inteligentes [11], serviços públicos [12], redes elétricas inteligentes [13] e saúde inteligente [14]. Soluções podem ser usadas para a detecção ou mitigação de ameaças específicas, como, por exemplo, espionagem, DDoS, *spoofing*, *jamming*, rastreamento, DoS, *IMSI Catchers*, *Distributed Reflection Denial of Service* (DRDoS), inundação e poluição.

Outras soluções gerais podem abordar, por exemplo, a segurança de *software-defined mobile networks* [15], políticas de segurança [16], esquemas de segurança (incluindo modelos e protocolos) [17], arquiteturas de segurança (e *frameworks*) [18], plataformas de segurança (e sistemas) [19], algoritmos (e métodos) [20], segurança baseada em inteligência artificial [21], segurança baseada em blockchain [22] e *testbeds* para experimentação em redes 5G [23].

IV. Definições de Árvores de Ataque e Defesa

Árvores de ataque e defesa são utilizadas para a modelagem e avaliação de segurança. Este tipo de modelo estende o conceito de árvores de ataque, permitindo que nós que representam medidas defensivas sejam usados em qualquer nível da árvore. Isso amplia as capacidades de modelagem das árvores de ataque e as torna adequadas para representar as interações entre um atacante e um defensor.

A. Cenário de Saúde Inteligente

Na Figura 1 é apresentado um exemplo de uma árvore de ataque e defesa para o cenário de degradação do sinal da rede 5G em saúde inteligente. Observa-se que há um objetivo principal (Ataque à Rede 5G) do qual deriva-se um subobjetivo primário (Ataque de Degradação do Sinal à Vertical de Saúde Inteligente). Os nós seguintes são divididos em subobjetivos secundários (*Sniffing* das Mensagens de Conexão *Radio Resource Control* (RRC) e Perda da Conexão ou Degradação de *Quality of Service* (QoS)), que são refinamentos conjuntivos, implicando na condição que ambos sejam necessariamente cumpridos para que o subojetivo primário esteja satisfeito. Também é proposto um conjunto de soluções para a segurança da camada física.

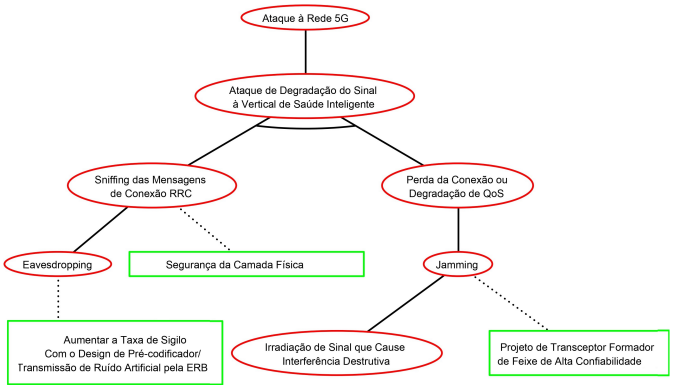

Fig. 1. Árvore de ataque e defesa para o cenário de degradação do sinal em saúde inteligente.

Em seguida, pode-se constatar que a captura se dá por *eavesdropping* na interface aérea. Propõe-se então como contramedida aumentar a taxa de sigilo com o *design* de pré-codificador e transmissão de ruído artificial pela estação rádio base. O ataque que causa perda da conexão ou degradação de QoS é realizado por meio do *Jamming*, que pode ser mitigado por meio do projeto de transceptor *beamforming* de alta confiabilidade [24]. Uma vez que não sejam tomadas medidas para mitigação das vulnerabilidades já citadas, poderá ser realizada a irradiação de sinal que cause interferência destrutiva no sinal da rede legítima.

B. Cenário de Indústria 4.0

Na Figura 2 é apresentado um exemplo de uma árvore de ataque e defesa para o cenário de interrupção em serviço industrial. Observa-se que há um objetivo principal (Ataque à Rede 5G) do qual deriva-se um subobjetivo primário (Ataque de

Interrupção aos Equipamentos da Indústria 4.0). O nó seguinte apresenta o subobjetivo secundário (Ataque de *Sniffing* Sobre a Célula de Rede), do qual derivam-se os refinamentos conjuntivos e a contramedida de implantação de uma *radio access network* 5G para IoT industrial. Tais refinamentos consistem em coleta dos dados da célula e criação de uma estação rádio base falsa. É possível mitigar a captura das informações com criptografia dos dados processados pela célula de rede.

Em seguida, pode-se constatar a conexão dos equipamentos à estação rádio base falsa. Propõe-se então como contramedida o uso de algoritmo que monitora os equipamentos e verifica se estão exercendo a função esperada. Uma vez que não sejam tomadas medidas para mitigação de vulnerabilidades, o atacante poderá desvincular equipamentos da rede legítima e a paralisar a linha de produção.

C. Cenário de Cidades Inteligentes

Na Figura 3 é apresentado outro exemplo de uma árvore de ataque e defesa para o cenário de DDoS em cidades inteligentes. Observa-se que há um objetivo principal (Ataque à Rede 5G) do qual deriva-se um subobjetivo primário (Ataque de DDoS ao Vertical de Cidades Inteligentes). Os nós seguintes são divididos em subobjetivos secundários (Ataque Lógico e Ataque Físico), que são refinamentos conjuntivos, implicando na condição que ambos sejam necessariamente cumpridos para que o subojetivo primário esteja satisfeito.

Pode-se constatar que o ataque lógico deve ser realizado pela infecção dos drones, a qual pode se dar por meio da atualização de *firmware* maliciosa. Propõe-se então como contramedida a verificação da integridade e autenticidade de atualizações. O ataque físico consistirá da saturação dos recursos de rádio da estação base, que tem como contramedida a implementação de mecanismos para segurança da camada física. Uma vez que não sejam tomadas medidas para mitigação de vulnerabilidades na camada física, dois novos refinamentos conjuntivos podem ser realizados, que são: a captura de parâmetros de conexão 5G RRC e disparo contínuo de mensagens de conexão RRC. A limitação ao atendimento de requisições de conexão RRC repetitivas em curto espaço de tempo é uma possível solução para mitigação.

Para que o atacante realize a captura de parâmetros, é necessário que realize alguma técnica de *eavesdropping*. Isto pode ser prevenido por meio de estratégias, como uso de mensagens de sinalização encriptadas. Se medidas contra o disparo contínuo de mensagens não forem tomadas, o atacante poderá usar uma rede de drones zumbis ou SDR (refinamentos disjuntivos), para executar a inundação da estação base com requisições de conexão RRC. Para combater essas ações maliciosas, deve ser utilizado um sistema de detecção e mitigação de *botnets*. No caso do SDR, deve ser realizada a identificação e bloqueio de dispositivos não homologados que tentem se conectar a rede.

V. Conclusões

É possível observar que várias das vulnerabilidades, ameaças e ataques destacados em artigos científicos são também destacados como preocupações da indústria, governos e instituições de padronização. Este tipo de relação pode servir como uma maneira de prover suporte à demonstração de viabilidade prática de problemas em 5G. Neste contexto, é recomendado que as ameaças que coincidem entre as literaturas sejam analisadas com mais cuidado, porém, sem negligenciar o restante das ameaças identificadas. Recomendações da ITU, como, por exemplo, ITU X.1813[1], são exemplos de fontes relevantes para a identificação de ameaças relacionadas com serviços verticais, tais como DDoS e espionagem de tráfego/dados para enlaces de comunicação.

Agradecimentos

Os autores agradecem a todos os estudantes da UFCG que participaram do desenvolvimento deste trabalho. Os autores também agradecem ao núcleo de PDI VIRTUS/UFCG pelo suporte no desenvolvimento dessa pesquisa.

Referências

[1] R. Khan, P. Kumar, D. N. K. Jayakody e M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Communications Surveys & Tutorials*, v. 22, pp. 196–248, 2020.

[2] D. C. G. Valadares, N. C. Will, Á. Sobrinho, A. Dantas, I. Morais, P. Graciliano e D. F S Santos, "Segurança em Cenários de Internet das Coisas em Redes 5G: Desafios e Recomendações," *Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, 2022.

[3] B. Jiang, J. Li, G. Yue e H. Song, "Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges," *IEEE Internet of Things Journal*, v. 8, pp. 10430–10451, 2021.

[4] P. Varga, J. Peto, and A. Franko, D. Balla, D. Haja, F. Janky, and G. Soos, D. Ficzere, M. Maliosz e L. Toka, "5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps," *Sensors*, v. 20, pp. 10430–10451, 2020.

[5] Quoc-Viet Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, Le, B. Long Won-Joo Hwang e Z. Ding, "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," *IEEE Access*, v. 8, pp. 116974-117017, 2020.

[6] F. Spinelli e V. Mancuso, "Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility," *IEEE Communications Surveys & Tutorials*, v. 23, pp. 596-630, 2021.

[7] S. Wijethilaka e M. Liyanage, "Survey on Network Slicing for Internet of Things Realization in 5G Networks," *IEEE Communications Surveys & Tutorials*, v. 23, pp. 957-994, 2021.

[8] M. Chlosta, D. Rupprecht, C. Pöpper e Thorsten Holz, "5G SUCI-catchers: still catching them all?," *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021.

[9] A. Hussein, I. H. Elhajj, A. Chehab e A. Kayssi, "SDN VANETs in 5G: An architecture for resilient security services," *International Conference on Software Defined Systems (SDS)*, 2017.

[10] F. Al-Turjman e S. Alturjman, "Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications," *IEEE Transactions on Industrial Informatics*, v. 14, pp. 2736-2744, 2018.

[11] A. Akhunzada, and S. u. Islam e S. Zeadally, "Securing Cyberspace of Future Smart Cities with 5G Technologies," *IEEE Network*, v. 34, pp. 336-342, 2020.

[12] M. Schmittner, A. Asadi, e M. Hollick, "SEMUD: Secure multi-hop device-to-device communication for 5G public safety networks," *IFIP Networking Conference (IFIP Networking) and Workshops*, 2017.

[13] H. Xuesong, L. Wei, Z. Tao, H. Haidong, Y. Kangle e P. Pei, "An Endogenous Security Protection Framework adapted to 5G MEC in Power Industry," *China Automation Congress (CAC)) and Workshops*, 2021.

[14] M. Ghassemian, M. Smith-Creasey e M. Nekovee, "Secure Non-Public Health Enterprise Networks," *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2020.

[1] https://www.itu.int/rec/T-REC-X.1813/en

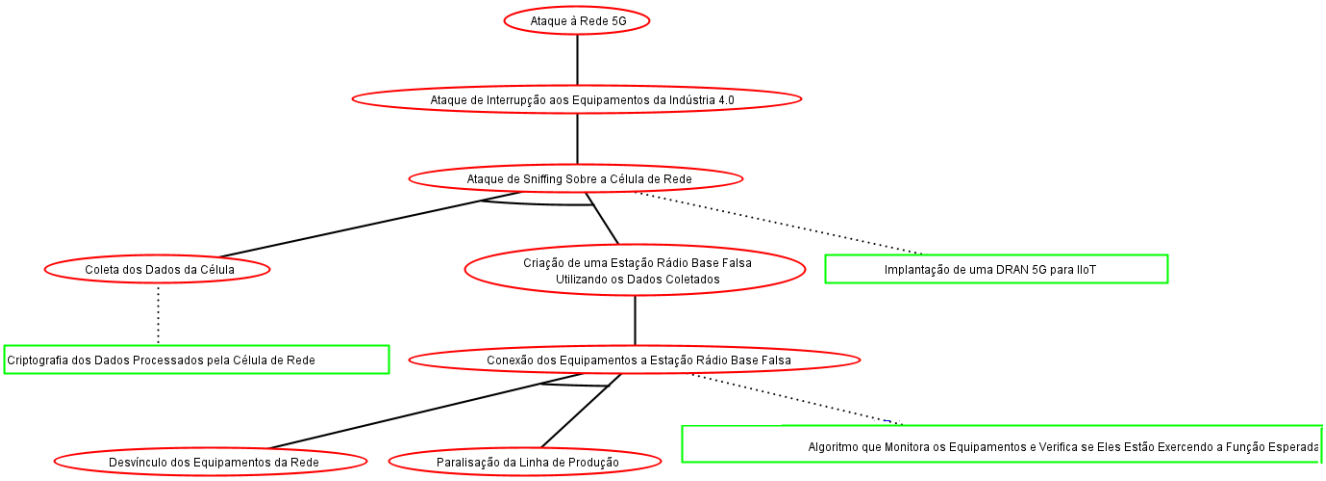

Fig. 2. Árvore de ataque e defesa para o cenário de interrupção em serviço industrial.

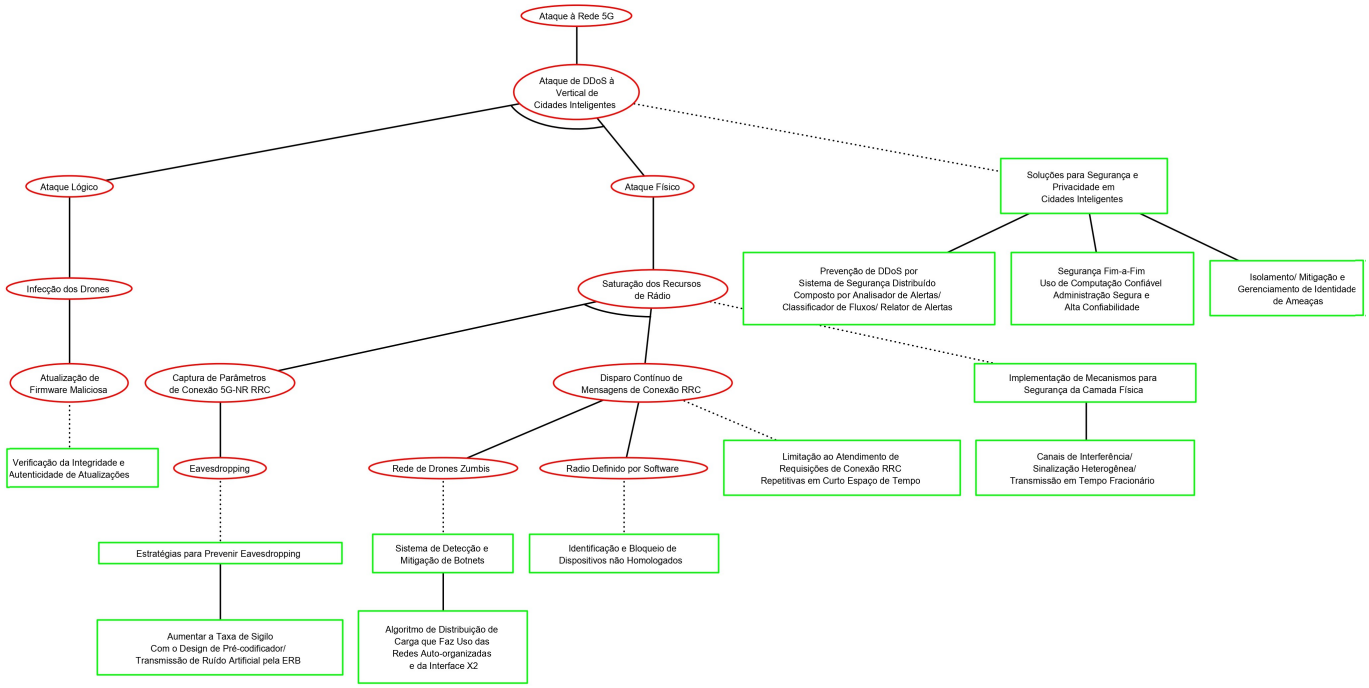

Fig. 3. Árvore de ataque e defesa para o cenário de DDoS em cidades inteligentes.

[15] M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, and E. M. De Oca, and A. Valtierra e C. Jimenez, "Security for Future Software Defined Mobile Networks," *International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015.

[16] G. Zhao, F. Zhang, L. Yu, H. Zhang, Q. Qiu e S. Xu, "Collaborative 5G Multiaccess Computing Security: Threats, Protection Requirements and Scenarios," *ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K)*, 2021.

[17] A. Ksentini e P. A. Frangoudis, "Toward Slicing-Enabled Multi-Access Edge Computing in 5G," *IEEE Network*, v. 34, pp. 99-105, 2020.

[18] A. Vijay e K. Umadevi, "Secured AI guided Architecture for D2D Systems of Massive MIMO deployed in 5G Networks," *International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019.

[19] J. Ortiz, Sanchez-R. Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber, Jean-Philippe Wary, D. Ayed, P. Bisson, M. Christopoulou, G. Xilouris, E. M. de Oca, G. Gür, G. Santinelli, V. Lefebvre, A. Pastor e D. Lopez, "INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and beyond Networks," *International Conference on Availability, Reliability and Security*, 2020.

[20] Bin-hui Tang, e Zhen-xing Zhou, "High-Speed Mobile Communication Network and Wireless Sensor Network Convergence Service Traffic Prediction Model and Security Mechanism Design," *International Conference on Computing and Pattern Recognition*, 2021.

[21] A. Thantharate, R. Paropkari, V. Walunj, C. Beard e P. Kankariya, "Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond," *Annual Computing and Communication Workshop and Conference (CCWC)*, 2020.

[22] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen e D. Zhang, "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," *IEEE Network*, v. 35, pp. 130-137, 2021.

[23] A. Gabrielson, K. Bauer, D. Kelly, A. Kearns e W. M. Smith, "CUE: A Standalone Testbed for 5G Experimentation," *IEEE Military Communications Conference (MILCOM)*, 2021.

[24] R. Zhang, J. Zhou, J. Lan, B. Yang and Z. Yu, "A High-Precision Hybrid Analog and Digital Beamforming Transceiver System for 5G Millimeter-Wave Communication,"in IEEE Access, vol. 7, pp. 83012-83023, 2019.