Métodos Formais para a Análise de Segurança de Redes 5G: Desafios e Oportunidades

Álvaro Sobrinho, Leandro Dias da Silva e Danilo F. S. Santos

***Resumo*— Neste artigo são discutidos cenários de aplicação de métodos formais, como, por exemplo, análise de segurança de protocolos usados em sistemas de comunicação móveis de quinta geração (5G). São também apresentados desafios e oportunidades relacionados com a aplicação de métodos formais no contexto de segurança cibernética de sistemas 5G. Foi possível observar que a aplicação de métodos formais para a segurança em cenários de aplicação 5G é ainda pouco explorada em pesquisas científicas. Mais estudos são necessários com foco, por exemplo, na análise de viabilidade de ameaças e verificação formal de conformidade com políticas de segurança.**

***Palavras-Chave*— Métodos Formais, Segurança, 5G.**

***Abstract*— This article discusses application scenarios of formal methods, such as security analysis of protocols used in fifth-generation (5G) mobile communication systems. We also present challenges and opportunities for applying formal methods in the context of the cybersecurity of 5G systems. The application of formal methods for security in 5G application scenarios is still little explored in scientific research. More studies are needed with a focus, for example, on threat feasibility analysis and formal verification of compliance with security policies.**

***Keywords*— Formal Methods, Security, 5G.**

I. Introdução

A arquitetura de segurança em sistemas de comunicação móveis de quinta geração (5G) é composta por funções de rede e componentes responsáveis pela proteção de comunicações de ponta a ponta, com o objetivo de fornecer confidencialidade, integridade, disponibilidade, autenticidade e não repúdio. As funções de segurança de rede são usadas para proteger, por exemplo, o acesso do equipamento do usuário (*User Equipment* - UEs) na rede de acesso por rádio em toda a pilha de protocolos da interface aérea. Entretanto, como as gerações passadas, sistemas 5G possuem vulnerabilidades conhecidas. Na Figura 1 são apresentados alguns exemplos de vulnerabilidades conhecidas em 2G, 3G, 4G e 5G. Pode-se observar que algumas vulnerabilidades permanecem existentes entre as diferentes gerações.

Considerando as vulnerabilidades existentes, diferentes soluções têm sido propostas na literatura científica para a proteção de redes 5G e de cenários de aplicação, como, exemplo, na *Internet of Things* (IoT) industrial e saúde inteligente [2], [3], [4]. Embora existam várias técnicas passíveis de aplicação para a segurança em 5G, neste trabalho, o foco está no uso de métodos formais. O uso de técnicas com formalização matemática rígida possui bastante potencial para aumentar a confiança em soluções para 5G e nas redes 5G. Por exemplo, protocolos, esquemas, arquiteturas e sistemas podem ser verificados formalmente para assegurar que propriedades de segurança desejadas são contempladas [5]. A verificação automática de modelos (*model checking*) é um exemplo de técnica formal passível de aplicação em sistemas 5G [6].

Fig. 1. Exemplos de vulnerabilidades conhecidas em redes 2G, 3G, 4G e 5G.

Neste contexto, neste artigo são discutidos cenários de aplicação de métodos formais para a segurança de sistemas 5G. Além disso, são apresentados desafios e oportunidades de pesquisa. As principais contribuições com este estudo, no contexto de sistemas 5G, são: (1) apresentar e discutir sobre cenários de aplicação de métodos formais; e (2) apresentar e discutir sobre desafios e oportunidades na aplicação de métodos formais.
Estas discussões oferecem subsídios para novas pesquisas sobre a aplicação de métodos formais para aumentar a segurança em redes 5G.

O restante deste artigo está organizado da seguinte maneira. Na Seção II são apresentados trabalhos similares ao apresentado neste artigo. Na Seção III são discutidos cenários de aplicação de métodos formais com base na literatura científica atual. Na Seção IV são discutidos desafios e oportunidades. Por fim, na Seção V são apresentadas conclusões e futuras direções de pesquisa.

II. Trabalhos Relacionados

A síntese de conhecimento difundido por meio de pesquisas científicas é relevante e bastante benéfica para a comunidade em geral, dado que este tipo de trabalho pode fornecer subsídios para novas iniciativas na área de segurança em 5G [1]. Portanto, estudos sobre aspectos de segurança cibernética

Álvaro Sobrinho, Núcleo de Inovação Tecnológica e Empreendedorismo, Universidade Federal do Agreste de Pernambuco, Garanhuns-PE, e-mail: alvaro.alvares@ufape.edu.br; Leandro Dias da Silva, Instituto de Computação, Universidade Federal de Alagoas, Maceió-AL, e-mail: leandrodias@ic.ufal.br; Danilo F. S. Santos, VIRTUS - Núcleo de PDI, Universidade Federal de Campina Grande, Campina Grande-PB, e-mail: danilo.santos@virtus.ufcg.edu.br.

e privacidade são relevantes para apoiar indústrias, governos e comunidades científicas na melhoria da confiança de sistemas 5G. Por exemplo, Khan *et al.* [1] discutiram questões gerais de segurança e privacidade, considerando tecnologias 5G importantes tais como *Software Defined Networks* (SDN), *Network Function Virtualization* (NFV) e *Network Slicing* (NS).

Além disso, Hofer-Schmitz e Stojanović [5] discutiram a aplicação de métodos formais para verificação de protocolos usados no ambiente IoT. Os autores apresentam uma visão geral da área e discutem abordagens existentes.

Outro exemplo de trabalho foi apresentado por Stojanović *et al.* [7]. Os autores discutiram sobre a aplicação de métodos formais no contexto de segurança de protocolos relacionados com *Vehicle-to-Everything* (V2X). É apresentada uma visão geral sobre a arquitetura de comunicação de carros conectados e protocolos relevantes. Transporte inteligente é uma vertical de aplicação bastante discutida em pesquisas sobre 5G [8].

Basin *et al.* [13] analisaram a literatura científica sobre o uso da ferramenta Tamarin para formalizar protocolos, modelos adversários e propriedades. O Tamarin é um exemplo de ferramenta consolidada para a verificação de protocolos de segurança criptográficos.

Entretanto, existe uma carência de discussões sobre a aplicação de métodos formais para a segurança de redes 5G. O escopo em estudos publicados na literatura é geralmente mais amplo (visão geral sobre diversas soluções para segurança) ou específico (como nos trabalhos descritos acima).

III. Visão Geral sobre Ameaças em 5G

Como destacado anteriormente, a arquitetura de segurança 5G é composta por funções de rede e componentes que protegem as comunicações de ponta a ponta. O *3rd Generation Partnership Project* (3GPP) publicou a especificação técnica 33.501, que estabelece a arquitetura, recursos, mecanismos e procedimentos de segurança praticados em 5G. A arquitetura de segurança 3GPP 5G inclui vários elementos e conceitos de arquitetura de segurança.

Entretanto, os novos cenários de conexões altamente dinâmicas e densas proporcionadas por redes 5G inevitavelmente ampliam o número de agentes de ameaças, devido, por exemplo, ao alto volume de dispositivos IoT conectados à rede. Portanto, os desenvolvedores de sistemas devem garantir a tríade confidencialidade, integridade e disponibilidade (*Confidentiality, Integrity, and Availability* - CIA) para aumentar segurança. No entanto, garantir a tríade CIA apresenta desafios relevantes, à medida que ocorrem avanços na implantação de redes 5G no mundo.

A confidencialidade em 5G pode ser ameaçada de várias maneiras. Entre elas, destacam-se as possibilidades de roubo de dados. Um adversário pode explorar vulnerabilidades de rede de maneira passiva ou ativa. Ao ter acesso e analisar dados que trafegam pela rede, informações relevantes podem ser obtidas passivamente. Se as credenciais ou chaves de acesso forem roubadas, os algoritmos de criptografia forem comprometidos, a elevação de privilégios for executada, ocorrer movimentação lateral ou um interno mal-intencionado facilitar o acesso não autorizado, informações confidenciais poderão ser obtidas ativamente.

Existem outras maneiras de explorar as vulnerabilidades de integridade na arquitetura de rede 5G. A rede de acesso por rádio 5G é ameaçada com transmissões de sinais falsos de sincronização que podem ser usados para coletar informações críticas e prejudicar o funcionamento dos serviços de comunicação. A qualidade de serviço em 5G pode ser degradada e ações prejudiciais podem realizadas, modificando o tráfego, os dados ou as funções do controlador. Essas modificações podem ser uma falsificação, adulteração, repetição com alteração de carimbos de data/hora e representação.

Por fim, a disponibilidade é uma questão crítica em sistemas 5G. Com a quantidade massiva de dispositivos na rede, a possibilidade de indisponibilização de serviço é uma ameaça evidente. *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS) são exemplos de ataques relacionados com esta ameaça. Ataques DDoS podem estar relacionados com IoT [3].

Além das ameaças gerais, como as redes 5G são habilitadoras dos cenários de aplicação, ameaças especificas devem ser consideradas e mitigadas. Na Figura 2 são apresentados alguns exemplos de ameaças relacionadas com o cenário de Indústria 4.0. Neste artigo, IoT industrial e sistemas físico-cibernéticos são considerados como parte da Indústria 4.0. Neste caso, é ilustrada uma fábrica de produtos habilitada por uma rede 5G e *Multi-access Edge Computing* (MEC). Por exemplo, um adversário pode realizar interrupções no contexto da rede portadora (*bearer network*). Além disso, pode realizar acesso ilegal a rede de acesso, espionando dados confidenciais da fábrica ou realizando movimentações indesejadas em dispositivos na fábrica (serviços industriais MEC). É possível também realizar consumo indevido de fatias de rede e controle indevido de funções de rede no *core* 5G. Estes exemplos de ameaças são relevantes tanto para redes industriais públicas quanto para redes industriais privadas.

IV. Cenários de Aplicação de Métodos Formais

Na Figura 3, considerando a literatura científica, são destacados cenários de aplicação e métodos formais usados para segurança em 5G. Na literatura, pode-se identificar estudos com foco em propostas de protocolos (ou esquemas) de segurança. Métodos formais são usados neste tipo de estudo como ferramentas para identificação de vulnerabilidades e prova de conformidade com comportamentos desejados. Por exemplo, Houmer *et al.* [10] utilizam a ferramenta *Automated Validation of Internet Security Protocols and Applications* (AVISPA)[1] para validar um esquema de autenticação de segurança em comunicações V2X baseadas em 5G. AVISPA possui uma linguagem formal modular e expressiva para a modelagem e verificação formal. Yan *et al.* [11] utilizaram redes de Petri coloridas para analisar formalmente o protocolo 5G *Authentication and Key Agreement* (5G-AKA).

Além disso, Peltonen *et al.* [12] aplicaram a ferramenta Tamarin[2] para analisar formalmente, em um modelo simbólico, a segurança de protocolos de *handover* para 5G. Basin *et al.* [13] também utilizam a ferramenta Tamarin para analisar

[1]https://www.avispa-project.org/

[2]http://tamarin-prover.github.io/

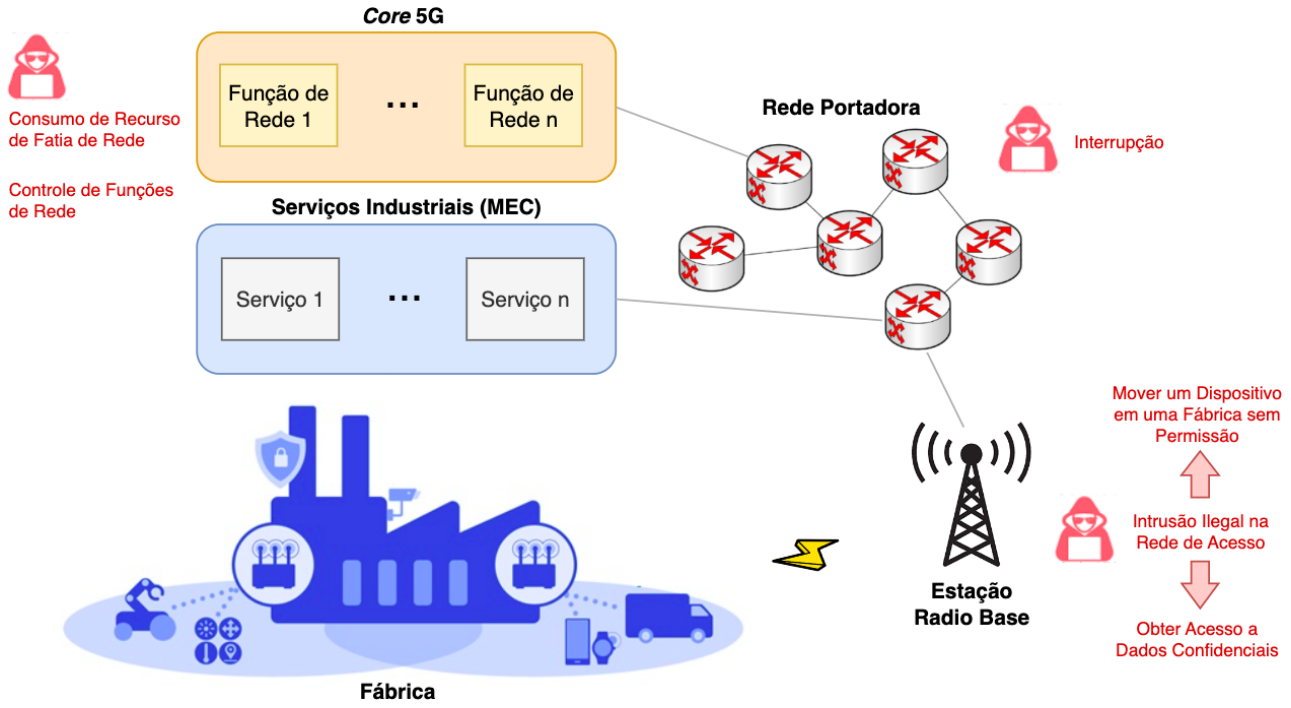

Fig. 2. Exemplos de ameaças relacionadas com o cenário de Indústria 4.0.

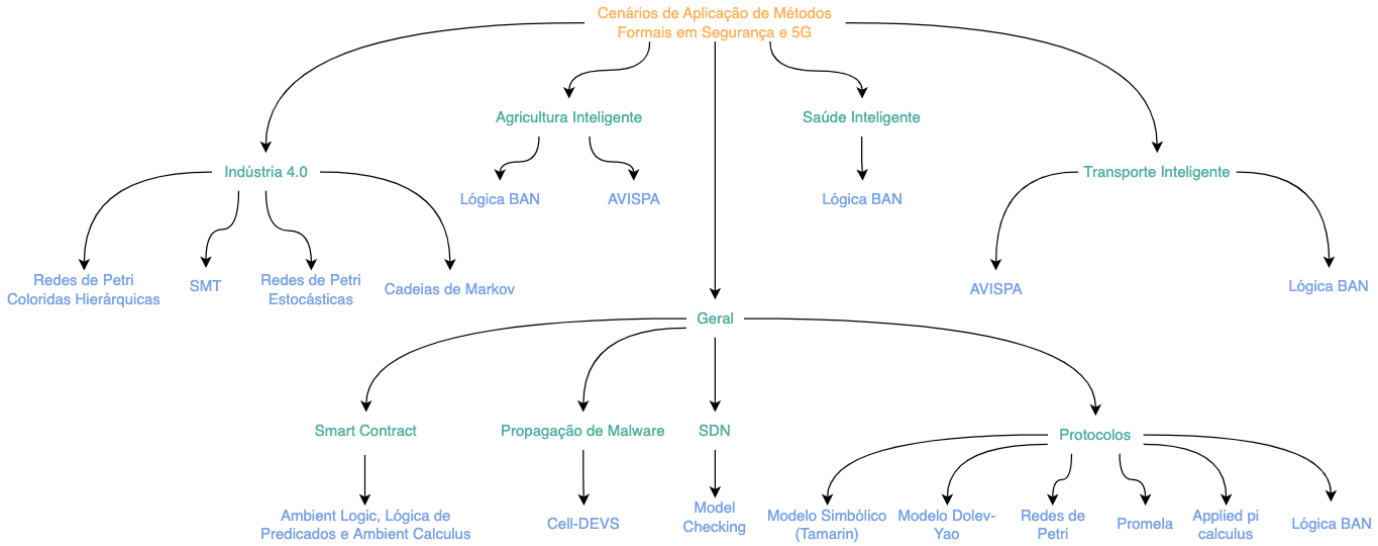

Fig. 3. Visão geral, considerando a literatura científica, sobre cenários de aplicação (Indústria 4.0, agricultura inteligente, saúde inteligente e transporte inteligente) e métodos formais usados para segurança em 5G.

formalmente o 5G-AKA. Hofer-Schmitz [14] utilizou *applied pi calculus* para modelar formalmente a especificação de segurança do protocolo para IoT chamado de EnOcean. O autor verificou formalmente o protocolo por meio do verificador de modelos ProVerif[3] (modelo Dolev-Yao). Akman *et al.* [15] também utilizaram a ferramenta ProVerif para analisar o arcabouço *Authentication and Key Management for Applications*. Zhang *et al.* [17] e Ding *et al.* [16] utilizaram a mesma linguagem e ferramenta para analisar o protocolo 5G EAP-TLS e o protocolo de configuração remota de SIM, respectivamente. Kim *et al.* [18] propuseram e verificaram formalmente um esquema de segurança para *inter-gNB-DU handover* no contexto de V2X baseado em 5G. Os autores realizaram a verificação formal com base na lógica BAN e na ferramenta Scyther[4]. Nyangaresi [19] usou a mesma lógica para analisar uma proposta de protocolo com o foco em 5G HetNets, considerando autenticação e acordo de chaves. Outro método formal identificado na análise da literatura incluiu a linguagem Promela (ferramenta SPIN[5]) [20].

Outros exemplos de trabalhos com a aplicação de métodos

[3]https://bblanche.gitlabpages.inria.fr/proverif/

[4]https://people.cispa.io/cas.cremers/scyther/

[5]https://spinroot.com/spin/whatispin.html

formais para protocolos (ou esquemas) e sistemas (ou outras soluções) estão relacionados com cenários de aplicação específicos em 5G. Por exemplo, pode-se observar aplicações na agricultura inteligente [21], saúde inteligente [22], Indústria 4.0 [23] e transporte e rede elétrica inteligente [24].

Além do uso de métodos formais para analisar soluções específicas em 5G, em alguns estudos, estes métodos servem como base para o desenvolvimento de soluções para aumentar a segurança na rede. Por exemplo, Kang e Cho [25] propuseram um arcabouço baseado em verificação automática de modelos (*model checking*) para a segurança em SDN. É possível observar também a relevância de analisar ameaças à rede 5G, como, por exemplo, a propagação de *malware* [26]. A verificação formal de políticas de segurança usando lógica é outro exemplo de uso de métodos formais como base para o desenvolvimento de soluções [27].

Soluções com foco mais amplo na segurança de redes 5G também podem ser desenvolvidas utilizando métodos formais. Por exemplo, Li *et al.* [28] apresentaram uma abordagem para a análise de segurança baseada em modelos formais. Os autores utilizaram redes de Petri coloridas hierárquicas para desenvolver um modelo de topologia da rede. Foram considerados os seguintes componentes: UE (geração de mensagens, envio e recebimento de dados e resposta à instrução), a rede de acesso (troca de informações entre UE e 5G *core*) e o 5G *core* (controle de dados, gerenciamento e suporte a NS). Na abordagem proposta, simulações são aplicadas por meio deste tipo de modelo hierárquico. Além do modelo hierárquico, os autores desenvolveram um modelo de redes de Petri estocástica e cadeias de Markov para analisar a confiabilidade da rede 5G. Nos dois tipos de análise, são consideradas possíveis vulnerabilidades relacionadas com ameaças tais como comprometimento de integridade de dados, controle ilegal de funções e consumo malicioso de fatias de rede.

V. Desafios e Oportunidades

Na aplicação de métodos formais para aumentar a confiança (em termos de segurança) de redes 5G, um dos desafios é a escolha adequada em como representar os componentes de rede, componentes específicos de cenários de aplicação, possíveis ataques e estratégias para mitigações. Portanto, o nível de abstração de modelos depende do tipo de análise, cenários de ataque e mitigação a serem analisados. As redes 5G são compostas por vários elementos, tais como equipamento de usuário, rede de acesso, rede portadora (*bearer network*) e *core* 5G. Por exemplo, o *core* 5G está também relacionado com várias funções de rede virtualizadas, como é o caso da *Authentication Server Function* (AUSF).

A análise de propriedades de segurança de soluções específicas (*e.g.*, protocolos) é uma atividade comum e reconhecida pela comunidade como relevante. Entretanto, a modelagem e análise formal de cenários de aplicação 5G, quando integradas a elementos de rede, é ainda um desafio na área [28]. Cada cenário de aplicação possui propósitos (*e.g.*, saúde inteligente) e contextos específicos (*e.g.*, sala de operações remotas). Isto implica que cada cenário de aplicação possui ameaças específicas à segurança. Por exemplo, um adversário com controle indevido de equipamentos em uma sala de operações remotas pode colocar a integridade física de um paciente em risco. Este tipo de cenário deve ser considerado em análises formais de segurança em redes 5G. Dado que software é uma parte expressiva da rede, a superfície de ataques em cenários de aplicação habilitados por 5G é bastante ampliada.

Em vários cenários de uso de 5G, a aplicação de técnicas de *machine learning* pode auxiliar no aumento de confiança na rede [29], como é o caso dos sistemas de detecção de intrusão. Em muitos estudos científicos, estes sistemas são usados para a detecção, e, consequentemente, a mitigação de várias ameaças. Neste caso, um problema relevante está relacionado com a confiança em sistemas 5G baseados em inteligência artificial. A aplicação de métodos formais é uma oportunidade de pesquisa interessante para aumentar a confiança nesses sistemas. Porém, vários desafios são identificados ao aplicar métodos formais, tais como:

1) a representação de modelos de *machine learning* tradicionais como parte de sistemas habilitados por redes 5G;
2) a representação de modelos de *deep learning* como parte de sistemas habilitados por redes 5G; e
3) a análise formal de propriedades (incluindo segurança) deste tipo de modelo.

Seshia et al. [31] apresentam cinco desafios relevantes: modelagem do ambiente, especificação formal, modelagem de sistemas de aprendizado, motores formais escaláveis e *correct-by-construction design*. Pode-se observar que, mesmo a linha de pesquisa geral sobre a aplicação de métodos formais em sistemas baseados em inteligência artificial, é bastante recente [30]. No trabalho apresentado por Nauman *et al* [30], modelos de redes de Petri coloridas são usados para analisar o comportamento de modelos de árvores de decisão no contexto de aplicações educacionais.

Além disso, deve-se observar os desafios específicos conhecidos para métodos formais. Em modelos baseados em estados (*e.g.*, redes de Petri coloridas), o problema de explosão de espaço de estados deve ser considerado durante a modelagem e análises de propriedades de segurança em 5G [32]. Neste contexto, técnicas para a redução de espaço de estados podem auxiliar na mitigação deste problema.

Com base nas discussões apresentadas neste artigo, é possível destacar outras oportunidades de pesquisa. Na maioria das pesquisas, a aplicação de métodos formais possui foco na análise de soluções específicas. Portanto, existe a oportunidade de mais pesquisas relacionadas com a identificação de vulnerabilidades e ameaças ao considerar componentes de rede, componentes específicos de cenários de aplicação, possíveis ataques e mitigações. Além disso, existem vários cenários de aplicação que ainda não foram considerados. Exemplos incluem educação inteligente, serviços públicos e cidades inteligentes.

De fato, estes (e outros) cenários podem ser explorados no mesmo contexto do trabalho apresentado por Li *et al.* [28]. Este tipo de trabalho indica a relevância de não somente utilizar métodos formais para analisar propriedades de segurança de soluções específicas, mas também analisar vulnerabilidades e ameaças em cenários de aplicação habilitados por redes 5G. Entretanto, outros métodos formais e tipos de análises

podem ser experimentadas, como, por exemplo, a verificação automática de modelos.

Outra oportunidade de pesquisa está relacionada com a aplicação de métodos formais para a análise de conformidade com políticas de segurança, como, por exemplo, a metodologia proposta por Unal et al. [27]. Considerando, por exemplo, a vertical de aplicação cidades inteligentes, é possível utilizar rastros de execução do sistema para verificar formalmente a conformidade com estratégias de mitigação de DDoS. Neste tipo de ataque, pode-se utilizar dispositivos infectados tais como *drones* (*firmware* malicioso) para congestionar a rede. Um exemplo de política de segurança é a verificação de integridade e autenticidade de atualizações de *firmware*.

VI. Conclusões

A aplicação de métodos formais no contexto de segurança cibernética de sistemas 5G é uma área que possui vários desafios e oportunidades de pesquisa. Na maioria dos estudos disponíveis na literatura científica, o foco está na análise formal de soluções específicas, como, por exemplo, protocolos ou esquemas de segurança. Portanto, vários cenários de aplicação 5G ainda não foram explorados na literatura científica. Neste contexto, é possível considerar a modelagem e análise de componentes de rede 5G, componentes específicos de cenários de aplicação, possíveis ataques cibernéticos e estratégias de mitigações. Em trabalhos futuros, a aplicação de métodos formais, tais como, redes de Petri coloridas e redes de Petri estocásticas, será investigada considerando vários cenários de aplicação 5G.

Agradecimentos

Os autores agradecem aos 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] 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.

[3] 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.

[4] 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.

[5] K. Hofer-Schmitz e B. Stojanović, "Towards formal verification of IoT protocols: A Review," *Computer Networks*, v. 174, pp. 107233, 2020.

[6] A. Kunnappilly, P. Backeman e C. Seceleanu. "From UML Modeling to UPPAAL Model checking of 5G Dynamic Service Orchestration," *Conference on the Engineering of Computer Based Systems*, 2021.

[7] B. Stojanović, K. Hofer-Schmitz, K. Nahrgang, H. Vallant e C. Derler, "Formal Modeling: A Step Forward to Cyber Secure Connected Car Systems," *Towards Connected and Autonomous Vehicle Highways*, 2020.

[8] 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*, 2017.

[9] D. Basin, C. Cremers, J. Dreier e R. Sasse, "Tamarin: Verification of Large-Scale, Real-World, Cryptographic Protocols," *IEEE Security & Privacy*, v. 20, pp. 24–32, 2022.

[10] M. Houmer, M. Ouaissa e M. Ouaissa, "Secure Authentication Scheme for 5G-based V2X Communications," *Procedia Computer Science*, v. 198, pp. 276–281, 2022.

[11] Z. Yan, C. Gu e H. Huang, "Analysis for Threat Models and Improvement Scheme of 5G AKA Protocol Based on Petri-net," *International Conference on Communication Technology*, 2021.

[12] A. Peltonen, R. Sasse e D. Basin, "A comprehensive formal analysis of 5G handover," *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021.

[13] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse e V. Stettler, "A Formal Analysis of 5G Authentication," *ACM SIGSAC Conference on Computer and Communications Security*, 2018.

[14] K. Hofer-Schmitz, "A Formal Analysis of EnOcean's Teach-in and Authentication," *International Conference on Availability, Reliability and Security*, 2021.

[15] G. Akman, P. Ginzboorg, M. T. Damir e V. Niemi, "Privacy-Enhanced AKMA for Multi-Access Edge Computing Mobility," *Computers*, v. 12, pp. 2, 2023.

[16] Z. Ding, Y. Hu, W. Luo, Z. Huang, L. Zhang e Z. Qin, "Security Analysis of Embedded SIM Remote Provisioning Protocol Using SPIN," *International Conference on Communication and Network Security*, 2022.

[17] J. Zhang, L. Yang, W. Cao e Q. Wang, "Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif," *IEEE Access*, v. 8, pp. 23674–23688, 2020.

[18] J. Kim, D. Duguma, Gerbi P. V. Astillo, Hoon-Yong Park, B. Kim, I. You e V. Sharma, "A Formally Verified Security Scheme for Inter-gNB-DU Handover in 5G Vehicle-to-Everything," *IEEE Access*, v. 9, pp. 119100–119117, 2021.

[19] V. O. Nyangaresi, "Provably Secure Protocol for 5G HetNets," *IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems*, 2021.

[20] Z. Ding, Y. Hu, W. Luo, Z. Huang, J. Xue e Z. Qin, "Formal Analysis and Verification of Embedded SIM Session Key Agreement Protocol," *International Conference on Electronic Information Technology and Computer Engineering*, 2021.

[21] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, M. A. Chaudhary, "Robust Multi-Gateway Authentication Scheme for Agriculture Wireless Sensor Network in Society 5.0 Smart Communities," *Agriculture*, v. 11, pp. 1020, 2021.

[22] T.-W. Lin e C.-L. Hsu, "FAIDM for Medical Privacy Protection in 5G Telemedicine Systems," *Applied Sciences*, v. 11, pp. 1155, 2021.

[23] G. Marchetto, R. Sisto, J. Yusupov e A. Ksentinit, "Formally verified latency-aware VNF placement in industrial Internet of things," *IEEE International Workshop on Factory Communication Systems*, 2018.

[24] W. Hou, Y. Sun, D. Li, Z. Guan e J. Liu, "Lightweight and Privacy-Preserving Charging Reservation Authentication Protocol for 5G-V2G," *IEEE Transactions on Vehicular Technology*, v. 11, pp. 1-13, 2023.

[25] M. Kang and J. J. Cho, "Verification Framework for Software-Defined Networking," *International Conference on Advanced Communication Technology*, 2022.

[26] B. U. Kazi e G. Wainer, "Formal modeling and simulation to analyze the dynamics of malware propagation in networks using cell-DEVS," *Communications & Networking Symposium*, 2017.

[27] D. Unal, M. Hammoudeh e M. S. Kiraz, "Policy specification and verification for blockchain and smart contracts in 5G networks," *ICT Express*, v. 6, pp. 43-47, 2020.

[28] X. Li, X. Hu, R. Zhang, C. Zhou, Q. Yin e L. Yang, "A Model-Driven Security Analysis Approach for 5G Communications in Industrial Systems," *IEEE Transactions on Wireless Communications*, v. 22, pp. 889-902, 2023.

[29] A. Afaq, N. Haider, M. Z. Baig, K.l S. Khan, M. Imran e I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Networks*, v. 123, pp. 102667, 2021.

[30] M. Nauman, N. Akhtar, A. Alhudhaif e A. Alothaim, "Guaranteeing Correctness of Machine Learning Based Decision Making at Higher Educational Institutions," *IEEE Access*, v. 9, pp. 92864–92880, 2021.

[31] S. A. Seshia, D. Sadigh e S. S. Sastry, "Toward Verified Artificial Intelligence," *Communications of the ACM*, v. 65, pp. 46–55, 2022.

[32] E. M. Clarke, W. Klieber, M. Nováček e P. Zuliani, "Model Checking and the State Explosion Problem," *Tools for Practical Software Verification*, 2012.