

Détection multidomaine d'anomalies dans un réseau 5G

Thomas Hoger

LAAS - CNRS, Université de Toulouse, CNRS

Toulouse, France

thomas.hoger@laas.fr

Philippe Owezarski

LAAS - CNRS, Université de Toulouse, CNRS

Toulouse, France

owe@laas.fr

Abstract—Avec l'avènement de la 5G, les réseaux mobiles se dynamisent et vont donc présenter une plus large surface d'attaque. Pour sécuriser ces nouveaux systèmes, nous proposons une méthode de détection d'anomalies multidomaine qui se distingue par l'étude de la corrélation du trafic sur trois dimensions : temporel en analysant les séquences de messages, sémantique en abstrayant les paramètres que ces messages contiennent et topologique en les reliant sous forme de graphe. Contrairement aux approches traditionnelles qui se limitent à considérer ces domaines indépendamment, notre méthode étudie leurs corrélations pour obtenir une vision globale, cohérente et explicable des anomalies.

Index Terms—Réseaux du futur, détection d'anomalies, machine learning

I. INTRODUCTION

Les réseaux mobiles sont historiquement conçus comme des systèmes monolithiques où chaque fonction est exécutée sur un matériel dédié, communiquant avec ses intermédiaires par des canaux fixes et des piles protocolaires figées. Ces limites disparaissent en 5G avec la virtualisation des fonctions réseaux (NFV) qui permet de déployer des services à la demande sur n'importe quel type de matériel. La structure du réseau de cœur peut être définie logiciellement et la 5G passe alors à un système de client-serveur qui suit le principe REST. Les procédures permettant le bon fonctionnement du réseau deviennent donc des microservices déployables dynamiquement et n'importe quelle entité peut ensuite les solliciter par le biais de protocoles de haut niveau, souvent HTTP. Néanmoins l'aspect dynamique des services de la 5G et la complexification de ses protocoles augmentent grandement sa surface d'attaque. Ainsi, bien que la 5G partage les vulnérabilités d'un réseau classique, elle est maintenant aussi la cible de nouvelles attaques qui lui sont propres. Coldwell et al. ont notamment trouvé des vulnérabilités sur les paramètres des appels d'API [1] en profitant du manque d'authentification des fonctions dans le réseau de cœur. Amponis et al. mettent en lumière des attaques semblables sur PFCP, un protocole dédié à la 5G [2]. Garbelini et al. proposent quant à eux des attaques de déni de service sur des protocoles bas niveau [3]. Comme la détection de ces attaques nécessite une inspection détaillée des paquets, une analyse quantitative de flux comme celles réalisées par les IDS classiques ne suffit plus. Pour sécuriser la 5G, il nous faut donc concevoir des méthodes de détection qui sauront s'adapter à un système dynamique. Pour détecter une anomalie dans un

tel système, un humain s'appuie sur plusieurs éléments clés comme les informations sur un paramètre, aussi bien au niveau de son nom que de sa valeur. L'analyse des paramètres et de leur sémantique permet de remarquer les paquets avec des valeurs aberrantes ou impossibles. Cependant, il arrive que le contenu même du paramètre soit moins pertinent que son contexte comme dans le cas des adresses IP, hash ou divers identifiants. Il existe ici deux types de contextes que l'on peut observer : le contexte temporel et le contexte topologique. Le contexte temporel analyse les séquences pour révéler certaines anomalies, tel que les DoS par rejeu de messages légitimes. Le contexte topologique, quant à lui, observe les liens entre les différents acteurs, ce qui permet de détecter des attaques coordonnées comme des DDoS. Notre objectif est de nous inspirer de la façon dont un humain détecterait une anomalie, en intégrant trois dimensions à notre détection : la sémantique du contenu, le contexte topologique et le contexte temporel.

II. CADRE DE L'ÉTUDE

Le design dynamique de la 5G a pour but de permettre aux opérateurs réseaux de déployer de nouveaux services rapidement. Cela permet entre autres d'incorporer à son réseau des fonctions personnalisées correspondant chacune à des besoins spécifiques. Le nombre de cas d'utilisations et de fonctions associées ne va cesser de croître et il est donc nécessaire de définir des limites claires pour le cadre de notre étude. Pour cela, nous choisissons de nous intéresser seulement aux éléments implémentés par le projet Open Air Interface (OAI) [4] que nous utiliserons pour nos expérimentations.

A. Scénarios d'intrusion

Les attaques de l'état de l'art nécessitent en grande majorité d'avoir au préalable mis en place un point d'entrée dans le réseau 5G, que ce soit en compromettant une machine existante ou en intégrant un nouvel acteur hostile. Il existe cependant de nombreuses méthodes pour arriver à remplir ces conditions. Un attaquant peut par exemple profiter de vulnérabilités sur les slices [5] pour pivoter sur des machines d'un réseau auquel il n'avait auparavant pas accès. Comme les fonctions réseaux sont virtualisées, il est aussi possible de les atteindre via leur hôte [6]. Un attaquant pourrait, pour finir, profiter de la proximité entre les stations de base 5G (gNB) avec les utilisateurs pour accéder physiquement à l'une d'entre

elle et en prendre le contrôle. Nous faisons donc l'hypothèse préliminaire qu'un attaquant a réussi à s'introduire sur le réseau en prenant le contrôle d'un ou plusieurs équipements utilisateurs (UE), gNB ou fonctions du réseau de cœur (CN).

B. Chiffrement des messages

Pour faciliter notre étude nous adoptons le point de vu de l'opérateur administrant le réseau 5G et considérons que le trafic de contrôle qu'il intercepte est lisible en clair. En effet, même si la communication entre NFV est chiffré de point à point par le protocole TLS, l'opérateur a le contrôle de chaque machines du CN et peut donc déchiffrer les messages à sa guise. L'attaquant n'ayant quant à lui pas le contrôle du réseau, on considère qu'il n'est pas capable de déchiffrer le trafic récupéré par écoute passive. Nous limitons donc notre étude aux attaques nécessitant une participation active d'un attaquant.

C. Surfaces considérées

Nos analyses concernent aussi bien la couche applicative que des protocoles de bas niveaux. Au niveau applicatif, il est seulement possible de traiter les données utilisateur avec de la volumétrie. En effet, une fois la connexion avec l'UE établie, le réseau 5G sert de tunnel au trafic utilisateur, ce qui rend impossible de déchiffrer le contenu des échanges et donc de l'analyser en profondeur. Comme l'analyse de volumétrie est déjà largement prise en compte par les systèmes de détection d'intrusion (IDS) classiques, nous préférons consacrer notre étude de la couche applicative au trafic de contrôle dont le rôle est essentiel au bon fonctionnement de l'intégralité du réseau. Parmi les fonctions réseaux agissant sur le flux de contrôle nous choisissons de nous limiter dans un premier temps aux AMF, AUSF, NRF, SMF, UDM, PCF, UDR et UPF¹. Nous considérons que ces fonctions sont les éléments fondamentaux d'un réseau 5G et seront retrouvées dans toutes les implémentations quel que soit l'opérateur qui la met en place. Pour chacune, nous considérons l'ensemble des procédures supportées par OAI et détaillées dans leur documentation respective. Pour les niveaux réseau et liaison nous nous concentrons là aussi sur un sous ensemble des protocoles, ou versions de protocoles, spécifiques à la 5G. Parmi eux on retrouve notamment NGAP, NAS, RRC et RLC.

III. APPROCHE PROPOSÉE

Pour détecter des anomalies sur les trois domaines que nous considérons nous avons choisi de combiner successivement des modèles spécialisés. Nous avons préféré une analyse successive à une analyse parallèle car les premiers modèles de notre chaîne sont des auto encodeurs qui, en plus de détecter des anomalies, permettent d'abstraire les données qu'ils traitent. Ainsi, en passant par ces modèles, les informations sont enrichies et les corrélations sont accentuées. La chaîne de

¹Ces fonctions réseau sont respectivement responsables de la gestion de l'accès et de la mobilité, de l'authentification, de la gestion des informations du réseau, de la gestion des sessions, de la gestion des données d'abonnés, du contrôle des politiques, du stockage des données d'abonnés et du traitement du plan utilisateur.

traitement que nous avons conçue est présentée dans la figure 2.

A. Analyse sémantique

Plusieurs attaques 5G sur le CN n'ont besoin d'envoyer qu'un seul paquet pour être menées à bien. Elles ne pourront donc pas être détectées par des méthodes d'analyse quantitatives. Pour déterminer la normalité d'un paquet, il est donc fondamental d'inspecter ses paramètres et de comprendre leur nature. Cette compréhension demande de considérer conjointement la valeur et le nom des paramètres. Malheureusement, la notion de sémantique apparaît rarement dans l'état de l'art qui se concentre le plus souvent sur l'analyse des valeurs avec des modèles comme des CNN. Pour utiliser dans notre apprentissage des valeurs textuelles telles que les noms de paramètres, il est nécessaire de les encoder. Une approche possible serait d'utiliser un encodage one-hot qui transforme chaque paramètre différent en un vecteur unique et orthogonal. Cependant, il existe un grand nombre de noms de paramètres différents dans les CN 5G et certains, bien que partageant la même sémantique, présentent des variations morphologiques. C'est par exemple le cas des paramètres `nfType` et `targetNfType` qui, bien que légèrement différents, seraient intéressants à regrouper. Notre objectif est donc d'abstraire nos données textuelles en les projetant dans un espace vectoriel où leur proximité avec les autres points reflétera une similitude sémantique. La prise en compte de cette sémantique est possible grâce à des techniques de Natural Language Processing (NLP) tel que Word2Vec [7] et ses variantes. Ces méthodes apprennent la sémantique d'un mot à travers son contexte et représentent les similitudes par des proximités vectorielles. Cependant, les mots sont ici projetés indépendamment dans un espace vectoriel de même dimension que celui d'origine. En plus d'être difficilement scalable, ces méthodes peinent aussi à traiter les variations morphologiques ainsi que les nouveautés. Nous leur préférons donc FastText [8], une des variantes de Word2Vec, qui découpe les mots en tokens et résout les problèmes énoncés précédemment par une analyse plus fine. Nous considérerons aussi des modèles de transformer comme BERT [9] et ses variantes, qui bien que moins rapides que FastText, compensent par une meilleure compréhension des informations contextuelles et des relations sémantiques. Bien que ces méthodes soient applicables aux noms et valeurs textuelles, elles sont moins efficaces lorsqu'il s'agit de valeurs numériques. Dans ce cas, nous utiliserons un Gaussian Mixture Model (GMM) qui modélise les répartitions des valeurs par des distributions gaussiennes et permet de les regrouper en plusieurs catégories. Les GMM sont particulièrement efficaces pour approximer des densités et ont déjà été utilisés avec succès dans des scénarios de détection d'anomalies [10]. Pour pouvoir utiliser à la fois les résultats de GMM et du NLP, il faudra néanmoins passer par une couche "fully connected" qui harmonisera les dimensions de leur espace de projection.

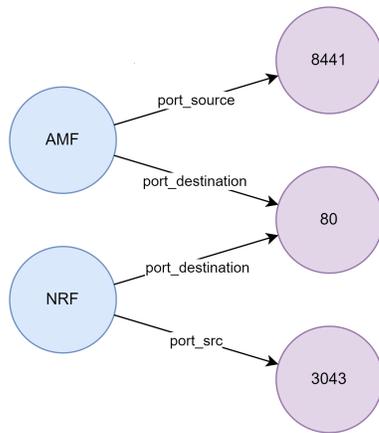


Fig. 1. Exemple de graphe généré par la réception de deux paquets destinés respectivement à un AMF et un NRF. Les NF, à gauche, sont liées par des arcs aux attributs que leur paquet contient. L'arc contient le nom de l'attribut tandis que sa valeur est dans le nœud cible.

B. Analyse topologique

Certains attributs, comme les adresses IP, les ports, les identifiants d'instance de NF ou les hachages, n'ont pas d'intérêt intrinsèque, mais doivent être considérés d'un point de vue relationnel. La forte présence d'une même IP source, quelle que soit sa valeur, pourrait par exemple être un indice d'une attaque de DDoS. Pour représenter ces relations, on peut modéliser les NF et leurs attributs par des nœuds dans un graphe. Le lien entre NF et attribut peut quant à lui être représenté par un arc. On obtient alors un graphe biparti dirigé et acyclique tel que présenté dans la figure 1. L'analyse topologique de ce graphe permet de comprendre la structure des échanges à grande échelle et ainsi de détecter des attaques coordonnées. Pour intégrer cette information dans la détection, nous avons décidé d'explorer les Graph Neural Networks (GNN), qui sont particulièrement adaptés pour capturer des informations topologiques. Il existe un grand nombre de techniques différentes, mais leur objectif est toujours de propager l'information sémantique d'un nœud vers ses voisins. Dans notre cas, il est crucial de prendre en compte les valeurs des arcs, ce qui nous a orienté vers les Message Passing Neural Networks (MPNN) [11], des GNN intégrant explicitement ces valeurs dans leur processus. Cette technique est le plus souvent utilisée sur des graphes statiques et il nous faut donc la limiter à un sous-ensemble du graphe pour éviter une explosion combinatoire. La profondeur de propagation est donc un hyperparamètre sur lequel nous réaliserons des études expérimentales pour en déterminer une valeur adéquate.

C. Analyse temporelle

Analyser les séquences de messages reçus permet de détecter les attaques de rejeu et de DoS. En effet, le trafic du plan de contrôle 5G, tel que défini par la norme 3GPP, suit des modèles d'échange séquentiels et toute déviation par rapport à ces schémas représente une anomalie. L'analyse topologique s'occupe déjà des corrélations entre les différents

acteurs, ce qui nous permet de nous concentrer spécifiquement sur les comportements indépendants des acteurs. Pour ce faire, les paquets destinés à une même entité sont regroupés en séquences représentant son activité individuelle. Ces séquences sont ensuite fournies à un réseau neuronal récurrent (RNN), spécialement conçu pour analyser les corrélations temporelles.

D. Explicabilité

Si notre détection se limite à classifier les messages sans fournir d'explications, l'information perd considérablement de sa valeur. Dans le cas des remédiations automatiques, cette perte n'est pas importante mais il arrive parfois que la nature d'une anomalie soit ambiguë et nécessite l'intervention d'un spécialiste. Ce dernier devra interpréter l'anomalie et il est donc fondamental de faciliter son travail. Notre approche répond intrinsèquement à ce besoin par son design modulaire qui permet de lever des alertes sur différents niveaux du pipeline.

IV. ETAT DE L'ART

Une première approche de détection considère les octets d'un paquet comme une image sur laquelle on utilise des réseaux de neurones convolutifs (CNN) pour détecter des variations structurelles [12] [13]. L'idée de mettre à profit la puissance intrinsèque des CNN qui ont déjà eu des résultats encourageants sur des problèmes ne relevant pas directement de la computer vision, comme par exemple la détection de malwares. Cependant, cette méthode se base principalement sur la disposition des octets, sans aucune garantie que ce format soit constant à travers les implémentations de la 5G. De plus, comme les CNN n'interprètent pas le contenu des données qu'ils traitent, ils ne peuvent pas évaluer l'impact qu'aura le changement d'une valeur ni établir de lien entre paramètres similaires. AutoGuard [14] et ADSeq-5GCN [15] utilisent quant à eux des réseaux de neurones récurrents (RNN) pour capturer les dépendances temporelles au sein de séquences de messages. Cependant ces travaux se concentrent exclusivement sur la forme des séquences et ignorent complètement le contenu des messages. De son côté, PROV5GC [16] utilise des graphes pour établir des liens entre les entités communicantes. Chaque nœud est un acteur différent et les arcs qui les relient représentent des échanges de messages. Le contenu des paquets est présent dans les arcs mais il est encapsulé dans un dictionnaire JSON, ce qui empêche de lier les paramètres entre eux. GSAD [17] fonctionne de la même manière mais considère la payload comme une suite d'octets qui sont encodés avant d'être insérés en tant que contenu des arcs de leur graphe. Dans les deux approches, la payload n'est pas interprétée et les relations établies se limitent alors aux acteurs communicants, sans prendre en compte le contenu des échanges. À notre connaissance, l'état de l'art ne propose aucune approche s'intéressant à la sémantique du contenu des paquets, et ne tente pas non plus de combiner simultanément les trois domaines que nous explorons.

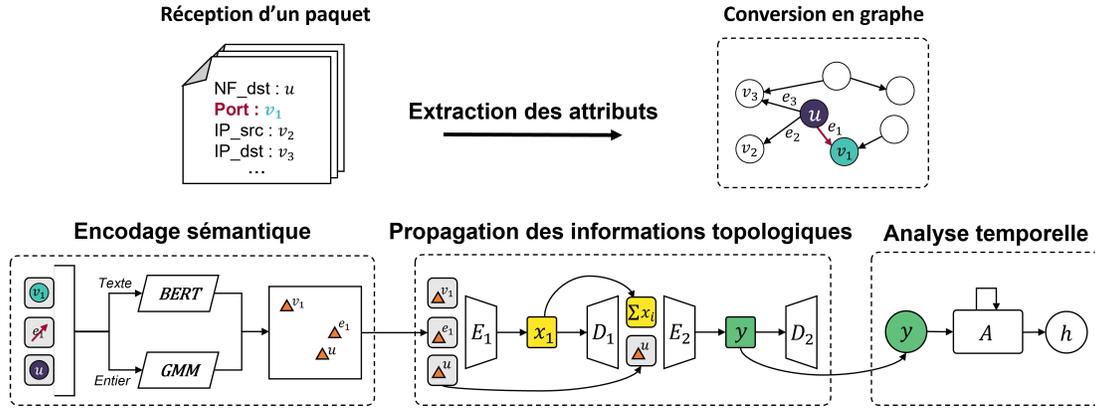


Fig. 2. Pipeline pour la détection d’anomalies multidomaines. Chaque paquet est ajouté dans un graphe en tant que nœud central u avec comme valeur le nom de l’entité réceptrice. On relie ensuite ce nœud central u à des nœuds successeurs v_i représentant chacun un attribut que le paquet contient. L’arc e_i contient le nom de l’attribut (par exemple “ip”) tandis que le nœud successeur v_i contient la valeur de l’attribut (par exemple “192.168.1.1”). Le contenu de ces différents nœuds et arcs est projeté dans un espace vectoriel par un encodeur dont la nature dépend du type de valeur rencontré (NLP pour le texte, GMM pour les entiers). Pour chaque successeur du nœud central, un triplet d’attributs encodés est transmis à un auto encodeur composé de E_1 et D_1 sous la forme (u, e_i, v_i) . Celui-ci se charge de condenser le triplet en un vecteur x_i unique, chacun représentant une partie spécifique du voisinage du nœud central. Ces condensats sont ensuite agrégés en un vecteur $\sum x_i$ et ré-encodés avec le nœud u . Le second auto encodeur composé de E_2 et D_2 produit ensuite une représentation y globale du nœud et de son voisinage. On donne enfin cette représentation à un RNN A qui analysera les séquences de messages.

V. PERSPECTIVES

La validation expérimentale de notre approche est une étape essentielle pour démontrer sa pertinence. Il est donc nécessaire d’avoir à disposition des données réalistes et adaptées aux besoins de notre étude. La conception d’un dataset ainsi que la génération automatique d’attaques sont donc les axes principaux que nous souhaitons explorer dans le futur.

A. Datasets

A ce jour, il existe deux principaux dataset d’attaques 5G. Le premier, 5GAD [1] met en place des attaques sur l’API REST sur une plateforme free5GC avec deux UEs et un gNB. Malheureusement, leur version de free5C est relativement ancienne et utilise le protocole HTTP au lieu d’HTTP2. De plus, leurs données bénignes représentent uniquement du trafic utilisateur (streaming youtube, téléchargement ftp, conférence teams) alors que nous avons dans notre cas besoin de trafic de contrôle. Le deuxième “5G Core PFCP Intrusion Detection Dataset” [18] à été réalisé avec Open5GC et UERANSIM. Leurs données incluent les 4 attaques qu’ils ont mises au point ainsi que des données qu’ils décrivent comme “normales”, mais nous n’avons pas trouvé d’informations supplémentaires concernant la nature de leur trafic bénin. Notre objectif étant de détecter des attaques sur plusieurs protocoles, il nous est nécessaire d’avoir des datasets représentant chacun d’entre eux et réalisés dans un même environnement. Or il n’existe pas à notre connaissance de dataset intégrant des attaques sur plusieurs protocoles différents. Il nous est donc nécessaire de réaliser notre propre dataset de trafic de contrôle applicatif et réseau. Pour ce faire, nous prévoyons d’utiliser la plateforme 5G du LAAS-CNRS qui met en place un réseau d’accès radio complet sur lequel est déployé le code du projet Open Air Interface [4]. Cette plateforme comprend trois serveurs DELL 7920, chacun doté de 2 processeurs à 18 cœurs et d’un noyau

optimisé pour la faible latence, qui servent respectivement de CN, gNB et d’UE. La plateforme inclut également trois USRP X310, chacun équipé de deux antennes log périodiques, ainsi que deux téléphones Google Pixel 6 agissant en tant qu’UE et disposant chacun de cartes SIM spéciales commercialisées par le projet Open Cells.

B. Génération automatique d’attaques bas niveau

À ce jour, les attaques sur la couche applicative nécessitent l’utilisation de paramètres précis et peuvent difficilement être automatisées. D’un autre côté, les attaques sur les couches de bas niveaux telles que proposées par Garbelini et al. [3] sont le plus souvent des injections de valeurs incorrectes dont le but est de provoquer un dysfonctionnement logiciel. Cette caractéristique se prête particulièrement bien à l’élaboration d’un modèle adverse. On pourrait avoir d’une part un générateur capable de produire des paquets malformés dans le but de déclencher des défaillances, et d’autre part, un détecteur conçu pour identifier et reconnaître ces attaques. En plus d’entraîner un outil de détection d’anomalies réseau. Cette approche offre aussi la possibilité de développer un générateur d’attaques artificielles qui pourraient être utilisées dans des datasets.

VI. CONCLUSION

L’évolution de la 5G nécessite de changer nos méthodes de détection d’anomalies. Nous avons identifié un manque de corrélation entre les différents niveau d’analyse dans les travaux de l’état de l’art et proposons donc un système de détection multidomaine basé sur l’analyse sémantique, séquentielle et temporelle. Nous proposons donc un système explicable par design et facilitant l’analyse humaine qui reste indispensable lors de l’utilisation d’un outil de détection d’anomalies. Le prochain objectif est de valider expérimentalement notre approche pour en démontrer la pertinence.

REMERCIEMENTS

Nous tenons à remercier le programme PEPR “Réseaux du Futur” de l’Agence Nationale de la Recherche (ANR) pour le soutien apporté à nos travaux dans le cadre du plan d’investissement France 2030. Nous remercions, en particulier, le projet NF-HiSec, financé sous la référence ANR-22-PEFT-0009, qui a joué un rôle essentiel dans la réalisation de ces travaux.

REFERENCES

- [1] C. Coldwell, D. Conger, E. Goodell, B. Jacobson, B. Petersen, D. Spencer, M. Anderson, and M. Sgambati, “Machine Learning 5G Attack Detection in Programmable Logic,” in *2022 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2022, pp. 1365–1370. [Online]. Available: <https://ieeexplore.ieee.org/document/10008647>
- [2] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, “Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 124, Dec. 2022. [Online]. Available: <https://jwcn-urasipjournals.springeropen.com/articles/10.1186/s13638-022-02204-5>
- [3] M. E. Garbelini, Z. Shang, S. Chattopadhyay, S. Sun, and E. Kurniawan, “5Ghoul: Unleashing Chaos on 5G Edge Devices,” Dec. 2023.
- [4] EURECOM, “Open Air Interface - Core Network 5G,” Nov. 2024. [Online]. Available: <https://gitlab.eurecom.fr/oai/cn5g>
- [5] A. Kumar and V. L. Thing, “Malicious Lateral Movement in 5G Core With Network Slicing And Its Detection,” in *2023 33rd International Telecommunication Networks and Applications Conference*, Nov. 2023, pp. 110–117. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10368559>
- [6] A. Tomar, D. Jeena, P. Mishra, and R. Bisht, “Docker Security: A Threat Model, Attack Taxonomy and Real-Time Attack Scenario of DoS,” in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Jan. 2020, pp. 150–155. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9058115>
- [7] T. Mikolov, K. Chen, G. Corrado, and J. Dean, “Efficient estimation of word representations in vector space.” [Online]. Available: <http://arxiv.org/abs/1301.3781>
- [8] P. Bojanowski, E. Grave, A. Joulin, and T. Mikolov, “Enriching word vectors with subword information.” [Online]. Available: <http://arxiv.org/abs/1607.04606>
- [9] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” May 2019. [Online]. Available: <http://arxiv.org/abs/1810.04805>
- [10] L. Leichtnam, E. Totel, N. Prigent, and L. Mé, “Sec2graph: Network Attack Detection Based on Novelty Detection on Graph Structured Data,” vol. 12223, Jun. 2020, p. 238. [Online]. Available: <https://inria.hal.science/hal-02950489>
- [11] J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, and G. E. Dahl, “Neural Message Passing for Quantum Chemistry,” Jun. 2017. [Online]. Available: <http://arxiv.org/abs/1704.01212>
- [12] R. Kale, K. W. Fok, and V. L. L. Thing, “Payload-based 5G Attack Detection,” in *2023 9th International Conference on Computer and Communications (ICCC)*, Dec. 2023, pp. 1262–1266. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10507422>
- [13] J. Lam and R. Abbas, “Machine Learning based Anomaly Detection for 5G Networks,” Mar. 2020. [Online]. Available: <http://arxiv.org/abs/2003.03474>
- [14] T. Madi, H. A. Alameddine, M. Pourzandi, A. Boukhtouta, M. Shoukry, and C. Assi, “AutoGuard: A Dual Intelligence Proactive Anomaly Detection at Application-Layer in 5G Networks,” in *Computer Security – ESORICS 2021*, E. Bertino, H. Shulman, and M. Waidner, Eds. Cham: Springer International Publishing, 2021, pp. 715–735.
- [15] Z. Tian, R. Patil, M. Gurusamy, and J. McCloud, “ADSeq-5GCN: Anomaly Detection from Network Traffic Sequences in 5G Core Network Control Plane,” in *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)*, Jun. 2023, pp. 75–82. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10147931>
- [16] H. S. Pacherkar and G. Yan, “PROV5GC: Hardening 5G Core Network Security with Attack Detection and Attribution Based on Provenance Graphs,” in *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec ’24. New York, NY, USA: Association for Computing Machinery, May 2024, pp. 254–264. [Online]. Available: <https://dl.acm.org/doi/10.1145/3643833.3656129>
- [17] M. Wang, P. Li, Z. Cheng, W. Liu, L. Nie, H. Bao, Q. Liu, and K. Zhang, “Unsupervised Graph-Sequence Anomaly Detection for 5G Core Network Control Plane Traffic,” in *2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS)*, Dec. 2023, pp. 1645–1652. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10475915>
- [18] G. Amponis, P. Radoglou-Grammatikis, G. Nakas, S. Goudos, V. Argyriou, T. Lagkas, and P. Sarigiannidis, “5G Core PFCP Intrusion Detection Dataset,” in *2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, Jun. 2023, pp. 1–4. [Online]. Available: <https://ieeexplore.ieee.org/document/10176693>