IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Survey On Intrusion Detection And Prevention In 5g Network

[1]Abhilash L Bhat [0000-0002-6465-6266], [2]Dr. Deepa S R [0000-0002-2071-9050]

[1]Assistant Professor, [2]Professor and Head

[1]Department of Computer Science and Engineering, [2]Department of Computer Science and Design

[1 2]K. S Institute of Technology, Bengaluru

Abstract: The deployment of 5G networks introduces a new era of communication technologies, provides higher data speeds, reduction in latency and enhanced connectivity. However, these advancements also increase significant concerns regarding security, especially with the increased attack surface and complexity inherent in 5G's architecture. Intrusion Detection and Prevention Systems (IDPS) are essential for safeguarding 5G networks against malicious threats and ensuring the integrity and availability of services. This paper surveys the state-of-the-art techniques for detecting and preventing in 5G environments, including both traditional and modern approaches. We discuss the role of machine learning and artificial intelligence in enhancing the detection capabilities of IDPS, as well as the challenges posed by the dynamic, distributed nature of 5G networks. Additionally, we explore the integration of IDPS with emerging 5G technologies such as network slicing, edge computing, and the Internet of Things (IoT), highlighting the potential for more adaptive and scalable security solutions. The paper also reviews key issues like real-time processing, scalability, and the need for privacy-preserving methods in intrusion detection. Finally, we identify research gaps and propose directions for future work to enhance the resilience of 5G networks.

Index Terms - 5G Network, Intrusion Detection and Prevention Systems (IDPS), Network Security, Cybersecurity in 5G, Machine Learning (ML)

I. INTRODUCTION

The fifth-generation (5G) cellular network is poised to revolutionize global connectivity by providing ultra-fast data rates, ultra-reliable low-latency communication (URLLC), and massive connectivity to billions of devices. As 5G networks extend beyond traditional mobile phones to include IoT devices, smart cities, and critical infrastructures, the complexity of securing these networks becomes increasingly challenging. Unlike previous generations of mobile networks, 5G relies on a distributed architecture that incorporates network slicing, edge computing, and cloud technologies. These innovations promise significant performance benefits, but they also create new vulnerabilities that malicious actors can exploit.

Intrusion Detection and Prevention Systems (IDPS) are vital for detecting, preventing, and responding to cyberattacks targeting 5G networks. IDPS traditionally rely on signature-based or anomaly-based detection techniques; however, with the advanced nature of attacks and the evolving 5G architecture, traditional methods are often insufficient. The dynamic nature of 5G networks, coupled with the massive volume of connected devices and high-speed traffic, demands more sophisticated solutions. Recent advances in machine learning, artificial intelligence, and deep learning offer promising techniques to enhance the accuracy and efficiency of intrusion detection. Moreover, integrating IDPS with emerging 5G technologies such as network slicing and edge computing introduces new challenges in real-time processing and scalability, as well as concerns related to privacy and data protection.

This survey paper aims to explore the current landscape of intrusion detection and prevention techniques tailored for 5G networks. We examine existing approaches, highlight their advantages and limitations, and discuss future directions to strengthen the security posture of 5G infrastructure.

II. LITERATURE REVIEW

Razvan Bocu and MaksimIavich [1] proposes a real-time IDS/IPS framework tailored for 5G and beyond networks built on software-defined networking (SDN). The system combines entropy-based anomaly detection with a CNN classifier to identify and respond to both known and unknown threats in real time. It is validated using both synthetic and real telecom traffic, achieving millisecond-level response times and demonstrating its feasibility for deployment in high-speed, large-scale network environments.
Neha Yadav et al [2] presents a deep learning-based intrusion detection system designed for IoT environments connected via 5G networks. It combines an autoencoder for feature reduction and a deep neural network for classification, trained on the UNSW-NB15 dataset. The system achieves high accuracy in detecting abnormal traffic, making it suitable for securing large-scale, data-intensive 5G-IoT deployments.
Ishtiaque Mahmood et al [3] investigates the effectiveness of machine learning algorithms for detecting intrusions in 5G networks. Using a large-scale dataset with millions of records, the authors evaluate models like Decision Tree, Random Forest, Naive Bayes, and Linear Regression. The results show that ML models, especially Decision Trees, can achieve very high accuracy in identifying malicious traffic, making them a practical solution for improving 5G network security.
Nimeshkumar Patel [4] introduces an AI-driven intrusion detection and prevention system designed for real-time application in 5G networks. It evaluates multiple models—including TCN, SVM, CatBoost, and LightGBM—using a real-time dataset collected from a telecom provider. The TCN model achieves the best performance, demonstrating the potential of deep learning for accurate and adaptive security in complex, high-speed 5G environments.
Diana Pineda Andrade et al [5] presents a DDoS detection and mitigation framework tailored for 5G networks using P4 programmable switches and SDN. It enables deep inspection of GTP-U encapsulated traffic—a key challenge in 5G—by extracting flow-level statistics and applying machine learning classifiers. Tested in a realistic 5G testbed, the system significantly reduces detection time and enables dynamic mitigation, demonstrating its effectiveness in handling internal DDoS threats.
Shivank Malik and Samaresh Bera [6] explores how integrating virtualized security functions like IDS and IPS affects the performance of 5G networks when deployed on general-purpose hardware. Using a softwarized 5G setup with open-source tools, the study evaluates key quality-of-service metrics such as throughput and latency under different traffic conditions. The results highlight that passive monitoring (IDS) introduces minimal overhead, while active filtering (IPS) can impact performance under load. The research provides practical insights into deploying security as a virtualized service within 5G infrastructures.

Hyun-Jin Kim et al [7] proposes a domain adaptation-based anomaly detection system for 5G networks, addressing the challenge of deploying machine learning models in environments with limited labeled data. It uses a stacked denoising autoencoder and adversarial training with a gradient reversal layer to adapt between different datasets. The model successfully detects anomalies in target domains despite being trained on different source data, making it effective for real-world deployment in diverse 5G environments.

Vinay Kumar Gugueoth [8] introduces a comprehensive framework for detecting and preventing multiple types of security attacks in 5G networks. It combines an advanced convolutional neural network (CD-GELU-CNN) for accurate attack detection, a quantum-inspired encryption scheme (FMLRQC) for secure data transmission, and a traffic management module (HDFS-ECH-KMeans) for handling large-scale network traffic. The system aims to provide robust multi-attack detection and end-to-end data protection in high-performance 5G environments.

Renato S. Silva et al [9] presents REPEL, a game-theoretic strategy designed to defend the 5G control plane from DDoS signalling attacks that target virtualized core components like the vMME. Instead of relying on detection-based blocking, REPEL uses dynamic resource allocation and strategic scaling of virtual network functions to absorb and mitigate the impact of signalling floods. The system is tested in a cloud-native 5G environment and demonstrates effective protection while maintaining service availability for legitimate users.
Matteo Varotto et al [10] introduces a novel method for detecting jamming attacks in private 5G networks using a one-class classification approach based on a Generalized Likelihood Ratio Test (GLRT). The system employs a convolutional neural network trained solely on legitimate signal data, enabling it to identify unknown jamming patterns without needing attack samples. Validated using software-defined radios, the model achieves high detection accuracy, making it suitable for physical-layer threat detection in mission-critical 5G deployments.
Mehrnoosh Monshizadeh et al [11] proposes a scalable and adaptive architecture for detecting and mitigating unsafe traffic in software-defined mobile networks, which are core to 5G infrastructure. The system leverages Detection-as-a-Service (DaaS) nodes combined with real-time traffic clustering and SDN-based flow control to proactively stop malicious traffic before it reaches the network controller. Demonstrated using OpenStack and Open vSwitch, the architecture highlights the potential of modular, programmable defenses in dynamic 5G environments.

M Awais Javed and Sohaib khan Niazi [12] provides a conceptual analysis of key security vulnerabilities in 5G networks, focusing on DoS/DDoS attacks and authentication challenges across RF, IP, and SDN layers. It outlines inherited weaknesses from LTE-A and discusses emerging threats unique to 5G's flexible architecture. The authors propose architectural improvements such as dual-homed switching, secure context information (SCI), and RF fingerprinting to enhance resilience. While theoretical, the paper offers a comprehensive view of layered 5G security threats and potential countermeasures.

Bruno Sousa et al [13] proposes MONDEO-Tactics5G, a multistage botnet detection and mitigation framework designed for 5G and 6G networks. The system analyzes DNS and HTTP traffic to detect malware-infected devices and command-and-control domains without requiring any software on end-user devices. It uses a phased approach including whitelisting, query rate analysis, DGA detection, and machine learning. Upon detection, it applies mitigation tactics like quarantining or blackholing infected nodes. The framework is designed to be integrated with 5G core functions and emphasizes proactive, network-level botnet defence.

REZA PARSAMEHR et al [14] presents IDLP, a two-phase intrusion detection and prevention system aimed at combating pollution attacks in mobile small cells that use network coding—an emerging component in 5G networks. The system detects maliciously altered packets using homomorphic MACs and then locates the attacker via SDN-assisted analysis of coded packet reports. IDLP is designed to minimize overhead while maintaining high detection accuracy and improving network reliability in bandwidth-constrained and decentralized environments.

Table 1: Comparative Analysis of all methods

Title	Methodology	Strengths	Limitations/Challenges
[1]	The authors developed a CNN-based real-time IDS/IPS system integrated with SDN and NFV. It uses entropy-based pre-processing for anomaly detection and is deployed in a virtualized 5G network environment for efficient, parallel traffic analysis.	Real-time detection with millisecond latency, low false alarm rate (0.81%), scalable architecture, and the ability to detect unknown (zero-day) attacks. Validated on real 5G telecom data.	Lacks post-quantum encryption support; relies on strong infrastructure for real-time processing; generalization across diverse datasets needs improvement.
[2]	The authors propose a novel intrusion detection framework combining Autoencoder (AE) and Deep Neural Network (DNN) models. They use the UNSW-NB15 dataset to train	Achieves 99.76% accuracy, Utilizes a benchmark dataset (UNSW-NB15) relevant to modern threats. Employs deep learning (AE + DNN) for high precision and	Does not deeply explore multi-class attack categorization. Performance may vary in real-world environments with more diverse or unseen attack patterns. The

	and evaluate their system. The approach involves: 1) Preprocessing and feature selection using Pearson correlation, 2) Transforming categorical data with one-hot encoding 3) Applying autoencoder for feature reduction 4) Using a customized DNN for final classification. Ensemble ML models like XGBoost and Random Forest were also tested for comparison.	low false positives.	model is resource-intensive, requiring high computational power (tested on high-end hardware). Limited explanation on real-time deployment challenges such as latency, adaptation, or dynamic updates in evolving networks.
[3]	The authors propose a machine learning-based IDS model using a large-scale 5G network dataset. The methodology includes: 1) Data preprocessing and transformation 2) Feature selection using a correlation matrix 3) Applying and evaluating four ML algorithms: Gaussian Naive Bayes, Decision Tree, Random Forest Regression, and Linear Regression.	Comprehensive comparative analysis of multiple ML algorithms. Decision Tree model achieved 99.99% accuracy, Uses a large, realistic dataset sourced from Kaggle. Includes both binary and multi-class classification considerations. Offers insights into processing time and practical deployment scenarios.	No real-time testing; the IDS is evaluated only on historical data. No deep learning models were tested or compared. Processing time for Random Forest was higher, which may limit real-time feasibility. Limited exploration of dataset imbalance or noise issues.
[4]	The system uses a multi-model machine learning approach, including SVM, CatBoost, LightGBM, and Temporal Convolutional Networks (TCN). Preprocessing included feature selection (via ANOVA and correlation), encoding, and normalization. Models were evaluated using accuracy, precision, recall, and F1-score.	Real-time dataset from an active telecom environment ensures practical relevance. TCN model captures temporal patterns effectively, ideal for evolving 5G traffic. Comprehensive comparative analysis with multiple models.	Requires significant computing resources, limiting deployment in lightweight environments. Focuses mostly on binary classification (benign vs. malicious), not multi-class attack types. Dataset is limited to one telecom provider, which may affect generalizability.
[5]	The proposed approach combines Software-Defined Networking (SDN) and P4 programmable switches to analyze GTP traffic in real time. A flow-based IDS system is developed using a P4 switch (Stratum) and an ONOS controller. The system extracts flow-level statistics from GTP packets, which are then processed by Machine Learning (ML) models (Logistic Regression and Naive Bayes) to classify traffic as benign or malicious.	Uses realistic 5G standalone testbed with live GTP traffic. Employs programmable switches (P4) to inspect GTP headers, enabling accurate flow-level detection. Significantly reduces detection time (e.g., from 81s to 20s for SYN flood) compared to OpenFlow-based SDN methods. Implements real-time mitigation without disrupting ongoing flows. Supports modular ONOS controller workflow, enhancing scalability.	Approach may not detect non-volume-based attacks, focusing mainly on DDoS floods. Effectiveness depends on the accuracy of initial flow statistics and assumptions about GTP parsing. Limited discussion on false positives/negatives and system behavior under high false alert rates. Resource and scalability overhead for maintaining flow tables in large deployments not thoroughly analyzed.

[6]	The authors implement a virtualized 5G network using Open5GS and UERANSIM, where the User Plane Function (UPF) is configured to act as IDS or IPS alongside NAT. Tools like Snort are used for traffic inspection. Synthetic TCP and UDP traffic are generated using D-ITG, and the network is evaluated under two configurations: IDS-NAT (passive monitoring) and IPS-NAT (inline filtering).	Practical implementation using widely available open-source tools and realistic virtual environments. Evaluation covers multiple QoS metrics under different traffic scenarios. Shows that IDS-NAT can support high-performance applications with minimal overhead.	Performance is hardware-dependent; results may not generalize to all systems. IPS-NAT introduces noticeable overhead under high packet loads due to NFQ bottlenecks. Only Snort is evaluated; no comparative testing with other tools like Suricata. No real attack scenarios are tested—only synthetic traffic is used. Focuses on binary IDS/IPS action (alert or drop); lacks nuanced policy enforcement or adaptive rules.
[7]	The authors design a Domain-Adaptive Anomaly Detection (DAAD) system that uses a Stacked Denoising Autoencoder (SDA) for feature extraction and a dual-classifier setup (class classifier + domain classifier) for binary classification and domain adaptation. The architecture uses Gradient Reversal Layer (GRL) to train classifiers via adversarial learning. Performance is validated using the NSL-KDD (source) and UNSW-NB15 (target) datasets to simulate domain shift.	Effectively addresses the domain shift problem using unsupervised domain adaptation. Demonstrates strong performance with 84.55% accuracy and 85.37 F1-score on a target dataset. Avoids the need for large labeled datasets in the deployment environment. Adopts adversarial training techniques (inspired by GANs) for better generalization.	Focused on binary classification (normal vs. abnormal), no multi-class attack detection. High model complexity with manual hyper parameter tuning required. Doesn't directly integrate into a live 5G edge network—purely theoretical/prototype stage.
[8]	The model includes three major components: 1. CD-GELU-CNN: An enhanced CNN model using a novel activation function to classify attacked vs. non-attacked data with improved accuracy. 2. FMLRQC: A quantum-inspired cryptographic mechanism for secure data transmission. 3. HDFS-ECH-KMeans: A load-balancing algorithm combining Hadoop Distributed File System and Entropy-based clustering to handle large volumes of traffic efficiently. The system processes real-time data logs (5G AD 2022), applies vectorization using a custom BERT variant, and verifies classification using multiple datasets (5G NIDD and 5G SliciNdd).	Highly accurate model with reported performance of 98.50% accuracy, outperforming existing CNN and DL models. Capable of detecting multiple attack types simultaneously. Integrates advanced quantum cryptography (FMLRQC) for enhanced data protection. The HDFS-ECH-KMeans module effectively handles traffic congestion and latency issues. Combines multiple datasets and feature composition techniques for comprehensive IDS training.	The framework is complex and computationally heavy, requiring substantial resources. Results are based on public datasets, not tested on live production 5G traffic. No real-world deployment or latency benchmarking in an actual telecom network. Quantum cryptography implementation (FMLRQC) is conceptual and not validated against adversarial attacks in practice. Explainability and interpretability of deep models like CD-GELU-CNN are not discussed.

[9]	The authors propose REPEL, a game-theoretic, insurance-based resource scaling strategy that uses virtualized network functions to dynamically scale the control plane. Key components include: 1. Game-theory model to predict attacker/defender behaviors. 2. A queuing model to simulate overload and evaluate attack impacts. 3. Testbed implementation using OpenStack and OpenAirInterface to simulate attack scenarios and measure system response. 4. vMME load balancing based on relative capacity (weight factor) to attract or deflect signalling traffic dynamically.	Provides a scalable and proactive solution using cloud-native principles. Effectively mitigates attacks without disrupting legitimate traffic. Reduces signalling loss by 20% when adding vMMEs during attack. Combines experimental validation and mathematical modeling for accuracy. Models attacker/defender interactions using Nash equilibrium, giving strategic insight into optimal countermeasures.	Assumes cloud resources are available, which may not hold in large-scale or persistent attacks. Requires preallocated standby capacity, which may be idle during normal operation. Does not explore detection methods in detail—relies on external IDS triggers. No real-time data labeling or filtering to block malicious flows. Complex deployment may limit adoption in resource-constrained environments.
[10]	The authors implement a Convolutional Neural Network (CNN) designed to function as a Generalized Likelihood Ratio Test (GLRT). The model is trained using a real dataset of legitimate IQ (in-phase quadrature) signal samples and an artificial jamming dataset. A baseline Convolutional Autoencoder (CAE) model is also implemented for comparison. All testing was done using Software-Defined Radios (SDRs) in a lab-based private 5G setup, with performance evaluated using false alarm (FA) and misdetection (MD) rates under multiple jamming scenarios (uniform, Gaussian, frame-based).	Demonstrates effective detection of previously unseen jamming attacks. CNN-based GLRT model significantly outperforms autoencoder baseline. Uses realistic lab environment with SDR-based 5G components. Does not require real attack data for training, increasing robustness.	Focuses on physical-layer jamming only, not higher-layer or multi-vector threats. Lab-based validation may not reflect performance in large-scale live 5G networks. Effectiveness depends on quality of artificial training data. Performance varies with sample window size, requiring fine-tuning. Does not consider adversarial learning or robustness against crafted attacks.
[11]	The authors propose an adaptive detection and prevention architecture that uses: Detection-as-a-Service (DaaS) nodes for anomaly detection. A clustering mechanism to group traffic based on features for load balancing. A layered structure with application, management, and data planes. Real-time SDN flow control to	Adaptive and scalable for SDN-based 5G environments. Supports load balancing through traffic clustering. Programmable and modular, integrating well with existing SDN controllers. Provides real-time mitigation via flow rule updates. Proof-of-concept validated through demonstrations on real platforms	Focuses on proof-of-concept; no quantitative performance evaluation (e.g., accuracy or latency). Attack types and detection algorithms used in DaaS are not deeply detailed. Scalability in large, production-grade 5G networks remains untested.

	block, forward, or modify traffic based on DaaS feedback. The system is demonstrated using OpenStack, OpenvSwitch, and a floodlight controller in two scenarios: full-packet and sampled traffic processing.		
[12]	SDN-based authentication, and Dual-Homed Switching Network (DSN) which integrates LTE-A with Wi-Fi for redundancy and load reduction. Adoption of SCI (Secure Context Information) and RF fingerprinting as future security solutions.	Provides a comprehensive overview of 5G security from RF to SDN. Introduces DSN concept to enhance redundancy and load balancing. Identifies RF-level attack vectors in LTE-A channels relevant for 5G. Recommends SDN-integrated SOCs and advanced context-based authentication. Bridges practical attack examples with architectural solutions.	No experimental or empirical validation; entirely theoretical. Solutions like DSN and SCI are proposals, not tested implementations. Scalability and overhead of proposed mitigations (e.g., SCI) not quantified. Heavy reliance on SDN and NFV may itself introduce centralization risks. Focus is mostly on infrastructure-level threats, with limited focus on end-user devices and applications.
[13]	The authors introduce MONDEO-Tactics5G, a multistage botnet detection and mitigation system designed to integrate with 5G infrastructures. The system is split into: 1. Detection using a four-phase pipeline: Whitelisting/Blacklisting, DNS Query Rate Analysis, Domain Generation Algorithm (DGA) detection, and Machine Learning. 2. Tactics for mitigation: quarantining infected devices, blackholing C2 servers, and CAPTCHA verification. It uses real DNS and HTTP traffic, lab-simulated malware (FluBot samples), and microservice-based architecture integrated into core 5G elements like UPF and PCF.	Supports real-time traffic analysis using DNS and HTTP inspection. Designed to integrate seamlessly with 5G core functions. Tactics are optimized based on utility functions, balancing security and user experience. Includes a statistical model-checking evaluation of tactic effectiveness using the PRISM model.	Primarily evaluated on FluBot; generalization to other malware needs validation. No live deployment in commercial 5G networks. Tactic scalability (e.g., CAPTCHA at scale) may pose implementation challenges. Some tactics like quarantining risk disrupting legitimate users if detection accuracy is low. Heavy reliance on DNS-based behavior; may miss botnets using encrypted or alternative channels.
[14]	The proposed IDLP (Intrusion Detection and Location-aware Prevention) mechanism operates in two phases: 1. Detection Phase: Uses a null space-based homomorphic MAC scheme to verify packet integrity. Applied to relay and	Efficient in detecting and preventing pollution attacks. Reduces computational and communication overhead by limiting full-node monitoring. Accurately locates attacker for proactive mitigation using SDN.	Evaluation is simulation-based, not deployed in live networks. Relies on SDN controller and trust in Hotspots, which may be single points of failure. Attack scope is limited to pollution attacks, not broader threat vectors.

	destination nodes only, avoiding unnecessary resource usage. 2. Locating Phase: Once a pollution attack is detected, all devices in the affected Mobile Small Cell (MSC) generate expanded coded packets and reports to help an SDN Controller identify the malicious node's location and apply mitigation (e.g., blocking access). The mechanism is implemented in Kodo and evaluated against a previous IDPS scheme.	Demonstrates higher decoding success rate and lower delay than prior work. Validated through real implementation using Kodo and MATLAB on simulated topologies.	Assumes secure and tamper-proof key distribution via a central KDC. Some overhead is still present due to tag generation and verification steps.

III. CONCLUSION

This paper surveys various works carried on Intrusion detection and prevention in 5G network in various domains such as Artificial Intelligence and Machine Learning, IoT and others and founds that each field ha stheir own advantages and drawbacks.

The rapid adoption of 5G networks introduces significant security challenges, particularly in intrusion detection and prevention. This paper has provided a comprehensive survey of existing techniques, highlighting traditional and modern approaches, including machine learning-based methods, deep packet inspection, anomaly detection, and blockchain-enabled security frameworks. While traditional intrusion detection systems (IDS) and intrusion prevention systems (IPS) remain relevant, they face scalability and adaptability challenges in the dynamic 5G environment.

Recent technologies, such as Artificial Intelligence (AI) and software-defined networking (SDN), offer promising solutions for real-time threat detection and mitigation. However, challenges related to high-speed data processing, encrypted traffic analysis, and false positive reduction must be addressed to enhance the efficiency of 5G security mechanisms. Future research should focus on developing lightweight, adaptive, and decentralized security solutions that can keep pace with evolving cyber threats.

In conclusion, while 5G networks present new security vulnerabilities, ongoing advancements in intrusion detection and prevention technologies offer hope for robust and resilient defense mechanisms. A combination of AI-driven security, blockchain-based trust models, and intelligent network monitoring will be crucial in safeguarding next-generation mobile networks from sophisticated cyber threats.

IV. REFERENCES

[1] Razvan Bocu, Maksim Iavich, "Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks" Symmetry 2023, 15, 110. https://doi.org/10.3390/sym15010110

[2] Neha Yadav, Sagar Pande, Aditya Khamparia, Deepak Gupta, "Intrusion Detection System on IoT with 5G Network Using Deep Learning" Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 9304689

[3] Ishtiaque Mahmood, Tahir Alyas, Sagheer Abbas, Tariq Shahzad, Qaiser Abbas, Khmaies Ouahada, "Intrusion Detection in 5G Cellular Network Using Machine Learning" Computer Systems Science and Engineering DOI: 10.32604/csse.2023.033842

[4] Nimeshkumar Patel "AI-Powered Intrusion Detection and Prevention Systems in 5G Networks" Proceedings of the Nineth International Conference on Communication and Electronics Systems (ICCES-2024) IEEE Xplore Part Number: CFP24AWO-ART; ISBN: 979-8-3503-7797-2

[5] Diana Pineda Andrade, Kemal Akkaya, Alexander Perez-Pons, Selcuk Uluagac, Abdulhadi Sahin, "DDoS Attack Detection and Mitigation in 5G Networks using P4 and SDN" 2024 IEEE 49th Conference on Local Computer Networks (LCN) DOI: 10.1109/LCN60385.2024.10639648

[6] Shivank Malik, Samaresh Bera, “Security-as-a-Function in 5G Network: Implementation and Performance Evaluation” 2024 International Conference on Signal Processing and Communications (SPCOM) | 979-8-3503-5045-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/SPCOM60851.2024.10631599

[7] Hyun-Jin Kim, Jonghoon Lee, Cheolhee Park, Jong-Geun Park, “Network Anomaly Detection based on Domain Adaptation for 5G Network Security” 2022 13th International Conference on Information and Communication Technology Convergence (ICTC) | 978-1-6654-9939-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICTC55196.2022.9952454

[8] Vinay Kumar Gugueoth, “Enhanced Security Attack Detection and Prevention in 5G Networks using CD-GELU-CNN and FMLRQC with HDFS-ECH-KMEANS” 2024 8th International Conference on Computer, Software and Modeling (ICCSM) | 979-8-3503-6713-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCSM63823.2024.00015

[9] Renato S. Silva , Carlos Colman-Meixner Thierno Diallo, Borja O. Garcia , Rafael S. Guimarães ,LuísF.M.deMoraes , Magnos Martinello, “REPEL: A Strategic Approach for Defending 5G Control Plane From DDoS Signalling Attacks” IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 18, NO. 3, SEPTEMBER 2021

[10] Matteo Varotto, Stefan Valentin, Francesco Ardizzon, Samuele Marzotto, Stefano Tomasin, “One-Class Classification as GLRT for Jamming Detection in Private 5G Networks” 2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC) | 979-8-3503-9318-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/SPAWC60668.2024.10694335

[11] Mehrnoosh Monshizadeh, Vikramajeet Khatri , Raimo Kantola , “An Adaptive Detection and Prevention Architecture for Unsafe Traffic in SDN Enabled Mobile Networks” 2017 IFIP/IEEE International Symposium on Integrated Network Management (IM2017):

[12] M Awais Javed, Sohaib khan Niazi, “5G Security Artifacts (DoS / DDoS and Authentication)” 2019 International Conference on Communication Technologies (ComTech 2019), 987-1-5386-5106-3/19/$31.00 ©2019 IEEE

[13] Bruno Sousaa, Duarte Diasa, Nuno Antunesa, Javier Cámarab, Ryan Wagnerc, Bradley Schmerlc, David Garlanc, Pedro Fidalgod, “MONDEO-Tactics5G: Multistage botnet detection and tactics for 5G/6G networks” https://doi.org/10.1016/j.cose.2024.103768

[14] REZA PARSAMEHR, JONATHAN RODRIGUEZ, GEORGIOS MANTAS, JOSÉ-FERNÁN MARTÍNEZ-ORTEGA, “IDLP: An Efficient Intrusion Detection and Location-Aware Prevention Mechanism for Network Coding-Enabled Mobile Small Cells” DOI: 10.1109/ACCESS.2020.2977428