World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

[redacted]

Extensive Review of Security and Privacy Issues in Heterogeneous Networks

Mmasi Patience Robai *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Kenya.

World Journal of Advanced Research and Reviews, 2024, 23(01), 2955–2984

Publication history: Received on 18 June 2024; revised on 28 July 2024; accepted on 30 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2308

Abstract

This paper studies advanced network security, privacy, and performance issues for Heterogeneous Networks (HetNets), which combine multiple types of cells to enhance wireless communication coverage and capacity. The coexistence of heterogeneous network elements inherently leads to considerable issues in terms of security, privacy, and performance. Previous research has primarily addressed security issues using common cryptographic techniques including data encryption with AES, secure key exchange with RSA, and handoff security with mutual authentication. Data anonymization methods and regulatory compliance have been used to address privacy concerns. Allocating resources and managing interference are some of the tactics that have been used in performance optimization. Although the current solutions offer a solid base, they frequently have issues with computational overhead, scalability, and continuous maintenance needs. Performance optimization solutions might not sufficiently handle dynamic network conditions, and privacy protections might not be sufficient to mitigate sophisticated data harvesting operations. This study evaluates existing HetNets solutions using a thorough evaluation and analytical technique. It assesses how well they handle issues with security, privacy, and performance, points out any shortcomings, and suggests areas for further investigation. Our analysis emphasizes the need for improved security mechanisms, including quantum-resistant cryptography, AI-driven threat detection, and technologies that improve privacy, such as differential privacy and homomorphic encryption. Innovative resource management and optimization strategies catered to HetNets' dynamic nature are needed to address performance issues. The necessity of developing new security, privacy, and performance solutions to guarantee the stability and dependability of HetNets is emphasized by this study. Stakeholders can promote the broad adoption and smooth integration of HetNet technology by tackling these obstacles. To sum up, this study offers a thorough analysis of the HetNets' architectural, security, privacy, and performance issues. It lists existing remedies, analyses their drawbacks, and suggests new lines of inquiry for future development to advance the area and improve HetNets' operational capabilities.

Keywords: Heterogeneous Networks; Small Cells; Authentication; Encryption; Network Resilience; Machine Learning for Security.

1 Introduction

Wireless networks have evolved from the 1G to the current Fifth Generation (5G) and beyond due to the constant need for fast wireless communication and the rapid expansion of mobile devices [1]-[3]. Data rates, latency, and capacity have all significantly improved with each new iteration. However, due to the growth of connected devices and data traffic, traditional network architectures—which are mostly focused on homogenous networking and macro cells—are finding it increasingly difficult to handle the explosive increase in capacity demand [4]-[6]. This challenge has spurred the deployment of Heterogeneous Networks (HetNets). According to [7], particularly in the context of 5G and beyond, heterogeneous networks (HetNets) integrate numerous information and communication technologies (ICTs) to deliver high-quality service for a variety of consumers. These networks offer distributed communication modes through device-to-device (D2D) characteristics and cutting-edge technology like massive MIMO and interference cancellation. These

* Corresponding author: Mmasi Patience Robai

systems combine different ICTs to improve QoS (quality of service) for different user classes, especially concerning 5G and beyond [8]. These networks may comprise gateway devices to enable smooth network connectivity as well as other data networks, including those that use the Time Slotted Channel Hopping (TSCH) and Carrier Sense Multiple Access (CSMA) protocols [9]. Because of their intricate structures and content, heterogeneous networks present both opportunities and difficulties for creating specialized machine learning solutions to solve a range of problems in complex systems [10]. These networks may also include techniques like utilizing several connection channels, such Multiprotocol Border Gateway Protocol (MP-BGP) and OpenFlow, to synchronize messages across distinct domain devices [11]. The heterogeneous networks seek to raise the flexibility and universality of communication systems while lowering costs, minimizing delays, and increasing data transmission efficiency [12], [13] . These HetNets have substantial obstacles when it comes to privacy, security, and performance enhancement.

HetNets' security issues are increased by the integration of many technologies and devices, leaving networks vulnerable to dangers including data interception, eavesdropping, and illegal access [14]-[15]. These flaws erode user confidence in the network architecture in addition to compromising data integrity and secrecy. These security issues must be resolved to protect sensitive data and guarantee the dependable operation of vital services, including public safety communications, healthcare applications, and financial transactions [16], [17]. HetNets' massive gathering, transfer, and processing of personal data raises privacy issues [18], [19]. The interchange of data between devices over heterogeneous network elements increases the danger of privacy violations and data breaches. Maintaining user privacy rights and adhering to legal obligations (such as the GDPR) depend on having strong privacy safeguards. HetNets can reduce these risks and increase user confidence in the secure handling of their personal data by putting in place privacy-enhancing technologies and strict data protection policies [20]. The intricate interactions between various network components and technologies, which affect data throughput, latency, and reliability, are the source of performance problems in HetNets. Managing smooth handovers and optimizing resource allocation become essential when HetNets include numerous small cells, macro cells, and other network parts [21]-[24]. This is necessary to guarantee constant service quality over a range of user densities and traffic patterns. Performance on traditional centralized networks is frequently compromised during hours of high demand due to inefficiencies in managing network load and resource allocation. HetNets use technologies like dynamic spectrum allocation and network slicing to optimize resource utilization and boost spectral efficiency to overcome these issues [25]-[30]. HetNets' integration of edge computing allows for reduced latency and localized data processing, which is beneficial for latency-sensitive applications like autonomous vehicles and real-time video streaming [31].

With an emphasis on the privacy, security, and performance in heterogeneous networks, this research significantly focuses on:

- Thorough examination of the privacy problems and the solutions in heterogeneous networks.
- Assessment of heterogeneous networks security risks and practical solutions.
- Analysis of the performance issues and the existing solutions in heterogeneous networks.
- Identification of research gaps and future research scopes.

2 Hetnets Architecture

The term heterogeneous networks describe the inter-working of different radio network layers (the macro cell layer and one or more small cell layers). HetNets increase network capacity by adding more cell sites; i.e., radio access networks, macro sites, in-building wireless and small cell deployments. As shown in Figure 1, HetNets use a combination of macro, pico, and femto cells to offer network densification. HetNets appear as one ubiquitous, seamless network that incorporates different access technologies like 4G, 5G, and Wi-Fi [32]. Heterogeneous networks are distinguished by a variety of nodes and edges, providing a more thorough depiction of the connections between various entities. These networks are essential for many applications because they allow data from different platforms and data sources to be combined [33].

HetNets not only significantly improve network coverage, they can also reduce power consumption and improve overall spectral efficiency [34]. HetNets offer relief and optimally benefit operators and users alike, but only if their installation is close to where additional capacity is required (i.e., close to the people) and a higher Signal-to-Interference-and-Noise-Ratio (SINR) can be achieved compared to the existing (macro-cell) deployment [35], [36]. A high SINR results in high additional indoor capacity created by the new base stations [37]. By combining lower-power small cells (femto, pico, and micro cells) with higher-power macro cells, HetNets offer advantages such as lower costs, more efficiency and better coverage.

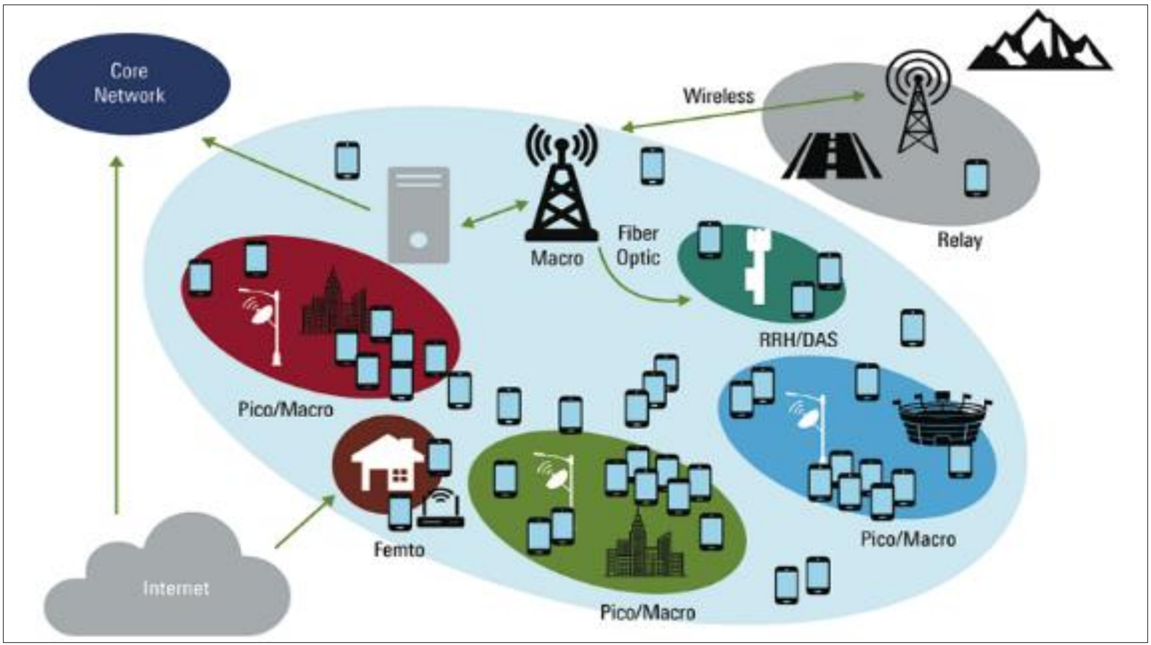

Figure 1 Heterogenous Network

Nevertheless, issues with energy management and interference arise when dense HetNets are deployed [38]. However, the implementation of dense HetNets has several challenges, including severe interference, inadequate energy management, and a lack of adaptability and flexibility. As the authors in [39] explain, Heterogeneous C-RANs (H-CRANs) [40] present a promising alternative for achieving high energy and spectrum efficiency [41], [42]. While MEC can offer substantial computing resources for low-latency applications, H-CRANs can also offer wide coverage and good energy efficiency. By merging these two essential technologies, 5G will provide additional applications. Considering the computational and storage resources in the BBU pools as well as the deployment of the RRHs, H-CRAN may be connected with MEC to facilitate the MEC system's installation [43], [44].

2.1 Elements of HetNets

The following are the basic building blocks of heterogeneous networks:

a). Macro cells: As in other cellular networks, a high-power base station (BS) is used to cover a wide area in a macro cell network [45]. The Base Station is always located at a high location, like the top of a mountain or tower, from where it can offer a clear view of the surrounding structures and barriers, and therefore it has a long transmission distance and a vast coverage area, with a cell radius ranging from 1 km to 25 km [7]. Macro cells are also characterized by:

Large Coverage Area: They are made to cover a wide geographic area with a high degree of coverage. Their diameter usually spans several kilometres, which makes them perfect for providing wide-area cellular service in rural, suburban, and urban settings [46].

High Transmit Power: Compared to small cells, macro cells operate at higher transmit power levels because of their broader coverage footprint [47]. They can span greater distances and more successfully through walls and other obstructions.

Lower Frequencies: Mainly utilized for 2G, 3G, and lower-frequency 4G LTE deployments, macro cells operate in lower frequency bands, usually below 6 GHz. These frequencies provide superior long-distance propagation characteristics as well as improved obstacle penetration [48], [49].

Capacity Handling: High amounts of data traffic and numerous simultaneous connections can be handled by macro cells. Within their service region, they act as the main infrastructure that facilitates data downloads, video streaming, and phone conversations for a large number of users [50].

Network Backbone: Macro cells frequently act as the network's anchor points or backbone in HetNets. They offer basic coverage and capacity, which are supplemented by smaller cells (such as Wi-Fi access points and small cells) that improve coverage and capacity in certain places, including inside or busy areas [51].

b). Small Cells: Small cells come in a variety of shapes and sizes. Their range, power, and capacity for handling many users all differ. They almost always contain LTE and Wi-Fi, the carrier's two key 3G technologies. They also have a backhaul link to the cellular network and a power source [52]. Femtocells, picocells, and microcells are the small cell types that supplement the core cellular coverage that microcells provide in HetNets. Femtocells are the smallest units and the macrocells are the largest, covering tens of Kilometers. To address network capacity and coverage challenges, mobile operators provide targeted cellular coverage in smaller regions through the use of femtocells, picocells, and microcells. Femtocells cover up to 10 meters, picocells cover up to 200 meters, while the macrocells cover up to 2 Km [53].

i) Femtocells: these are affordable base stations that increase coverage over time and offer high bit rates in demanding settings like indoors [54], [55]. They are the smallest of the small cells and mobile operators frequently employ them to improve signals. Customers can directly handle them and they are simple to install and run. With a maximum range of ten meters, femtocells are a component of a mobile operator's core network. They are often referred to as "coverage" or "signal booster,". Femtocells are typically sold as plug-and-play products that need to be plugged into a power outlet and connected to a LAN or WiFi router at home for consumers to use them. They can use a gateway to connect to the mobile operator's main network once they are online. As shown in Figure 2, femtocells give mobile consumers coverage and extra capacity, just like other tiny cells do [56].

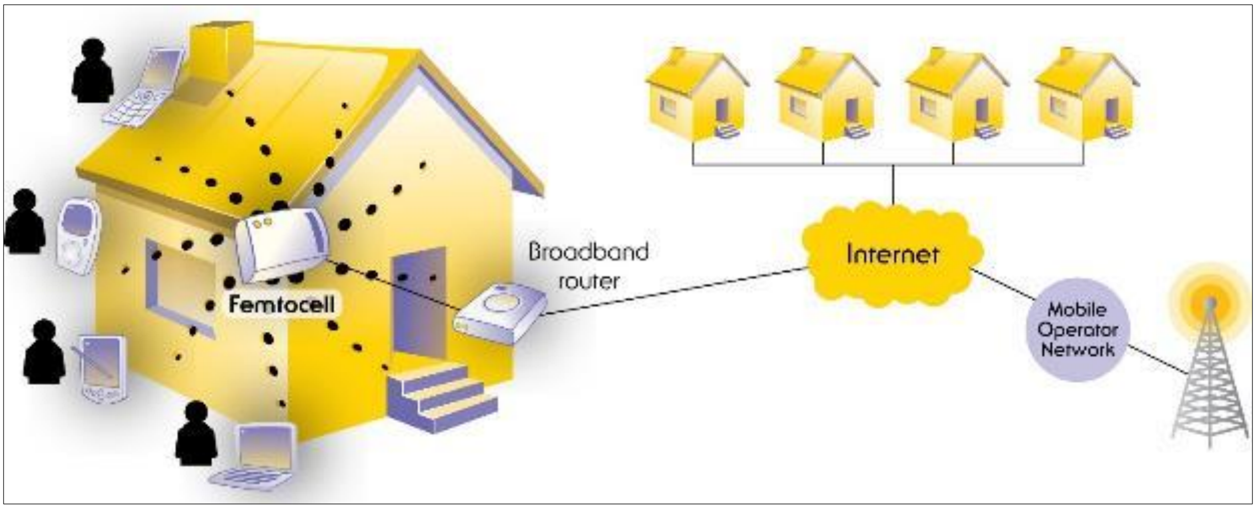

Figure 2 Femtocell

Femtocells are characterized by:

Small Coverage Area: Femtocells improve indoor cellular connectivity in regions with inadequate macrocell signals by providing small, often tens to hundred-meter coverage zones [57]. They provide steady signal strength and little interference for customers in the vicinity while relieving network congestion by unloading capacity from the macro network.

Low Transmit Power: Femtocells are compact, and therefore they minimize interference with nearby cells by operating at far lower power levels than standard macrocells [58]. Because of the low transmit power, customers can optimize their tailored deployment while also improving indoor coverage and consuming less energy.

Self-Organizing Networks (SON): These networks handle planning, configuration, and optimization autonomously, reducing the need for human interaction [59]. Since users frequently deploy femtocells without doing conventional RF planning, SON guarantees plug-and-play functionality.

Licensed and Unlicensed Spectrum: Femtocells can function in licensed or unlicensed spectrum, each with its own set of implications. Licensed bands follow rules, work with macrocells, and offer exclusive usage of particular frequencies within predetermined geographic zones [60]. Conversely, unlicensed frequencies (like Wi-Fi) are accessible to the general public, enabling femtocells to supplement current cellular networks. Femtocells operate in both spectrums, which balances capacity, cost [61], and coverage.

Subscriber Initiated Deployment: By enabling end users to build femtocells on their own in their homes or businesses, Subscriber Initiated Deployment (SID) improves interior mobile coverage without requiring direct MNO involvement [62]. By using a plug-and-play setup, this method streamlines activation and enhances voice and data connectivity in places where macrocell signals are poor.

ii) Picocell: This refers to a tiny cellular base station that usually covers a limited area. As show in Figure 3, a picocell can be found in place of an office, a store, a train station, a stock market, or, more recently, an airplane. Picocells are commonly used in cellular networks to increase network capacity in locations with high phone usage density, like train stations or stadiums, or to extend coverage to indoor regions where external signals are not as strong. In locations that are costly or challenging to access with the more conventional macrocell method, picocells offer coverage and capacity [63].

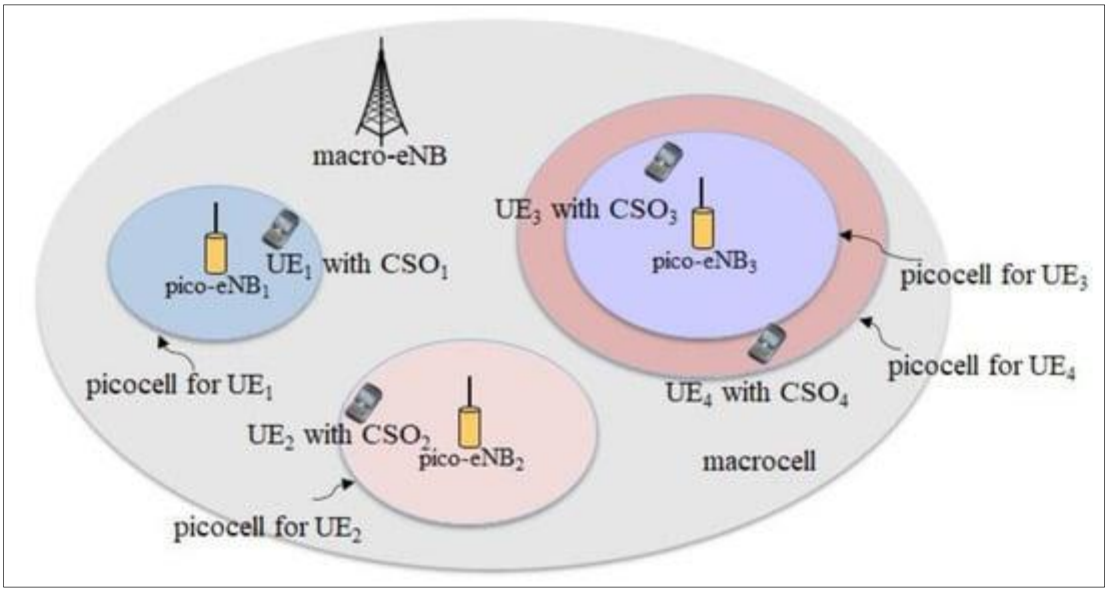

Figure 3 Picocell

Picocells are characterized by:

Coverage Area: Picocells have a limited coverage area; usually, they may cover up to 820 feet (250 meters) [64]. In locations like workplaces, retail centers, railroad stations, and stock markets, they are frequently used indoors. Nevertheless, they can also be utilized outside.

User Capacity: A picocell can accommodate up to 64 people at once. They offer targeted coverage where it's most required, however not as much as macrocells [65].

Deployment Locations: Picocells are installed within buildings as well as on utility poles, streetlights, and the sides of buildings [66]. Because of their small size, carriers can improve signal strength in places with spotty or non-existent coverage.

Backhaul: Depends on the wireless carrier or operator; often uses hybrid fiber-coaxial (HFC) technology [67] (e.g., DOCSIS 3.0/3.1).

iii). Microcells: Usually larger than a femtocell but smaller than a macro cell, this type of small-scale cellular base station is used in telecommunications networks to offer localized coverage over a relatively small geographic area [68]. They can go the furthest, around two kilometers, of any species. In addition to macrocells, microcells can expand the mobile network's coverage and capacity. Microcells have a range of up to 2 kilometers, which makes them a viable option for places like major rail stations. They can also take care of short-term capacity requirements for big public events like concerts and sporting events. In any mobile network, macrocells continue to offer the primary network coverage, but microcells can be added to the main network to cover gaps in capacity and coverage [69].

Microcells are characterized by:

- Coverage Area: Microcells have a specific coverage area, which may include transportation hubs or shopping malls [70]. Usually, their range reaches several hundred meters.
- Indoor Coverage: In areas where outdoor signals might not be as strong, they are utilized to increase mobile network coverage indoors.
- Network Capacity: Microcells expand the capacity of the network in places where phone usage is high. In comparison to larger base stations (macrocells), they can manage fewer simultaneous sessions [71].
- Cost-Effectiveness: Because microcells consume less power and have a smaller coverage area than typical macrocells, their deployment is more economical [72].
- Frequency Reuse: Reusing the same frequencies within a certain geographic area allows microcells to maximize available spectrum and improve overall network efficiency [73].
- Backhaul: Depends on the wireless carrier or operator; often uses hybrid fiber-coaxial (HFC) technology (e.g., DOCSIS 3.0/3.1).

Table 1 presents a summary of the various networks within hetnets.

Table 1 Characteristics of the HetNet Elements

Cell Type	Coverage Area	Height	Use Cases	Deployment Locations	Backhaul
Macrocell	Large (Tens of Kilometres)	>100 ft	Wide coverage, rural areas	Outdoor (cell towers)	Fiber-based or wireless microwave
Microcell	Small (Hundreds of Meters)	>100 ft	Urban areas, high traffic	Outdoor (streetlights, utility poles) or indoor	Fiber-based or hybrid fiber-coaxial
Picocell	Very Small (Tens of meters)	>100 ft	Densely populated areas, hotspots	Indoor (offices, malls) or outdoor	Fiber-based or hybrid fiber-coaxial
Femtocell	Extremely Small (Meters)	>100 ft	Residential or small office coverage	Indoor (homes, small offices)	Broadband internet (DSL, cable)

2.2 HetNets Variations

The following are the variants of hetnets:

2.2.1 Single-Radio Access Technology (RAT) Multi-Tier Network Components

Single RAT Multitier Network Component refers to a network architecture [74] within Heterogeneous Networks (HetNets) that utilizes a single Radio Access Technology (RAT) across multiple tiers or layers. This approach aims to simplify network management by standardizing the RAT used throughout different network components [75].

They are characterized by:

- *Dual-Band Deployment*: Small cells are deployed in both the mm-wave and sub-6GHz frequency bands via single RAT multitier networks [76]. Large route loss and directional antennas are obstacles faced by mm-wave small cells; the sub-6GHz spectrum helps with initial access operations.
- *Optimizing Coverage*: Dual-band small cell deployment aids in improving coverage. mm-wave cells have a high bandwidth, however beamforming is needed to compensate for route loss [77]. By aiding in early access, the sub-6GHz frequency enhances coverage.
- *Load balancing*: Biases are applied to tier and RAT selection to balance loads. These biases affect user throughput, cell load, and the distribution of the signal-to-interference plus noise ratio (SINR) [78]. Either user downlink throughput or SINR coverage are maximized by optimal biases.

- *Cell Density Considerations*: Dual-band small cells are essential, particularly when placed sparingly or during periods of high traffic density [79]. Through the management of overloading and outage possibilities, they improve system performance.

2.2.2 Multi-Radio Access Technology Multi-Tier Network Components

Multi-RAT Multi-Tier Component refers to the many components and architecture of a communications network that include different radio access technologies (RATs) and coverage tiers. This covers several base station tiers (such as macrocells, microcells, and small cells), Wi-Fi networks, small cells (like femtocells and picocells), and several generations of cellular technologies (including LTE and 5G). Together, these parts give wireless communication networks better capacity, efficiency, and coverage [80], [81].

They are characterized by:

- *Heterogeneity*: To maximize coverage and capacity in a variety of settings and user densities, these networks combine several radio access technologies (RATs) and cell types, such as LTE, 5G, Wi-Fi, and tiny cells [82].
- Coverage and Capacity Optimization: To optimize traffic management and user experience, they deploy different tiers of cells (macrocells, microcells, and small cells) to give seamless coverage over varying distances and areas [83].
- *Interference Management*: To reduce interference between various RATs and cells and improve spectral efficiency and network performance, sophisticated techniques including adaptive beamforming and interference coordination are used [84].
- *Flexibility and Scalability*: Because these networks are built for modular deployment and scalability, operators can gradually increase capacity and coverage without having to completely rebuild their infrastructure [85].
- Optimized Resource Allocation: They dynamically allocate resources (like spectrum and power) based on real-time network conditions [86] and user demand, ensuring efficient use of network resources and minimizing operational costs [87].

Table 2 below provides the comparisons between single rat multi-tier and multi-rat multi-tier.

Table 2 Comparison between single rat multi-tier and multi-rat multi-tier

Aspect	**Single rat mlti-tier**	**Multi rat multi-tier**
Elements	Consists of multiple tiers (e.g., macrocells, small cells) using the same radio access technology (RAT)	Involves multiple tiers using different RATs (e.g., LTE, Wi-Fi, 5G-NR)
Link	Homogeneous link properties within each tier	Heterogeneous link properties due to different RATs
Opportunistic Use	Limited to the same RAT	Opportunistically utilizes overlapping RATs
Service Management	Simplified due to uniform RATs	Complex due to diverse RATs
Quality of Service	Easier to manage QoS within a single RAT	Complex due to diverse RATs
Application Areas	Well-suited for Homogeneous Services	Enables diverse applications and improved connectivity
Examples	LTE-only multi-tier network	5G-NR + Wi-Fi multi-tier network

3 Security challenges in HetNets

A HetNet is a type of network architecture that integrates different types of cells, i.e. macrocells and small cells (microcells, picocells, and femtocells) to improve coverage, capacity, and user experience [88]. The integration of this range of tools often brings about several security issues. These issues need to be resolved. The heterogeneous character of the network itself is one of the main security issues with HetNets. In contrast to conventional homogenous networks, which usually depend on standardized protocols and infrastructure [89], HetNets integrates many technologies and interfaces. The complexity of maintaining security policies and configurations across many network nodes is increased by this variety [90], which also increases the attack surface.

3.1 Interference

Due to the presence of different cell types, such as femtocells and macrocells, interference provides a significant difficulty in heterogeneous networks (HetNets), resulting in inter-cell interference (ICI) concerns that affect user throughput and Quality of Service [91]. When considering co-channel HetNet deployment—where the macrocells and small cells share the same frequency spectrum—interference management emerges as one of the most significant issues [92], [93]. There are overlapping coverage areas, and therefore the cells operating nearby may cause interference. Controlling interference becomes essential to prevent signals from one cell from severely impairing the functionality of nearby cells [94]. HetNet interference can result in eavesdropping attacks against mobile users, jeopardizing their secrecy rate. By using interference as a covert channel, attackers might evade conventional security measures and send malicious signals or intercept confidential information [95]. The risk of eavesdropping and unlawful data interception is increased when signals are weaker owing to interference, endangering user privacy and organizational security. Interference increases the risk to device security and operational integrity in HetNets integrating IoT devices, which could allow attackers to take advantage of weaknesses and compromise more extensive network infrastructure [96].

3.2 Virtual Resource Security

Due to the complexity of virtualization, virtual resource allocation in HetNets presents difficulties and may result in security risks and vulnerabilities. Research that is now available mostly concentrates on optimizing network services without sufficiently addressing virtual resource security issues, which could lead to problems with performance and information leakage [97]. Although virtualization technology in 5G HetNets allows for flexible resource allocation, the additional complexity [98] and layers between systems provide security problems [99]. These difficulties show up as four primary categories of security threats: attacks on physical linkages, attacks among virtual elements, attacks among physical elements, and physical elements attacking virtual elements. Physical components could undermine the management of virtual nodes, opening the door to manipulation or sniffer assaults. On the other hand, susceptible physical nodes may be attacked by virtual nodes, which could result in denial-of-service (DoS) assaults. Virtual nodes that share physical resources may establish hidden channels that are vulnerable to side-channel attacks [100]-[104]. Finally, weaknesses in substrate linkages are brought to light by physical link attacks, like as man-in-the-middle attacks. To provide secure operations in 5G HetNets, it is imperative to design strong virtualized resource allocation frameworks that prioritize security. To comprehend the possible dangers associated with security threats targeting virtual resource allocation, it is necessary to model and categorize them [105]. Virtual resources in HetNets are so diverse and complicated, therefore securing them raises considerable issues. Several entities share resources like bandwidth, processing power, and storage by using virtualization techniques like Software-Defined Networking and Network Function Virtualization. Strict isolation measures are also required due to the increased danger of unwanted access, data leakage, and interference between virtual instances. The security of virtual resources can be jeopardized by exploiting flaws in virtualization technologies like hypervisors and virtual switches [106].

3.3 End-to-End Communication Security

Communication networks' end-to-end (E2E) security faces several challenges. A significant concern is the susceptibility to single points of failure, wherein the compromise of a solitary component may compromise the security of the entire network, hence enabling potential exploitation by malicious actors [107]-[110]. Identity privacy leakage is a serious issue as well since insufficient security measures could expose private user data, which could result in privacy violations and illegal access to personal information [111]. Furthermore, the scalability and adaptability of many current E2E security solutions are limited by their lack of generality across various network domains and technologies. To maintain high-security standards, smooth coordination of intricate operations such as user equipment registration, key management, authentication protocols, and session key generation is necessary for ensuring secure E2E connections [112]. Also, maintaining both security integrity and communication speed requires careful design and optimization to strike a balance between strong security measures and optimal performance efficiency [113]-[116].

3.4 Edge Security Risks

The HetNet's edge interfaces with numerous networks, making it susceptible to attacks. Edge computing is distributed and integrates a variety of network technologies [117]-[119]. Due to their lack of security features and irregular update schedules, edge devices, which are frequently placed at network edges for better performance, are susceptible to attacks including malware penetration and denial-of-service attacks. HetNets have been viewed as a viable solution to satisfy the rapidly growing needs of mobile services and applications. To cache multimedia material for mobile users, numerous caching-enabled small-cell-based stations (SBSs) are deployed within the coverage of a macro-cell base station (MBS). However, because untrusted SBSs pose security risks, the proprietors of these SBSs may get unauthorized access to the cached material, compromising the privacy of its users [120]- [122]. Because different network types and vendors have inconsistent protocols and configurations, heterogeneous networks make security management more difficult. These concerns are made worse by the growth of IoT devices, which increase the attack surface by adding more devices that can be remotely exploited and used with default credentials [123]. To offer complete protection against ever-evolving threats in HetNets, addressing these difficulties requires strong measures including intrusion detection systems, network segmentation, strong encryption, and collaborative vendor adherence to security regulations [124].

4 Privacy challenges in HetNets

HetNets presents privacy issues because of the intricate and multifaceted architecture, which combines several network domains and access methods [125]. As people interact via more channels and gadgets, issues including data security, location privacy, and regulatory compliance come to light. Because HetNets are scattered, it is more difficult to protect user data across different network domains [126]-[128]. To properly protect user information, strong privacy controls and adherence to regulatory frameworks are necessary.

4.1 Insecure Access Points

Significant privacy difficulties are introduced by the complicated network topology of HetNets, which has a variety of base station (BS) types and elaborate network topologies. This heterogeneous environment's insecure access points put user privacy and data security at risk and could compromise sensitive data. The existence of highly concentrated base stations and diverse access technologies exacerbate security weaknesses in many network segments, raising the probability of intrusions that may jeopardize user data and network stability [129] . An important security risk is presented by the existence of insecure access points, particularly in public hotspots where users value convenience over security. The vulnerability of untrusted small-cell-based stations (SBSs) in HetNets can result in unauthorized access and privacy breaches of cached multimedia material due to the exponential proliferation of mobile services and applications [130].

4.2 Privacy Preservation in Handover Authentication

Privacy preservation in handover authentication in HetNets, such as 5G HetNets and integrated terrestrial-satellite networks (ITSN), is a crucial concern due to the increasing risk during user mobility support and network densification [131]-[134]. The intricacy emerges from the requirement to preserve service continuity while shielding private user data—like location—during handovers. The need for standardized and compatible authentication frameworks arises from the added complexity of privacy protection measures caused by interoperability among BSs from different operators or technologies [135]. User tracking, identity disclosure, location privacy, contextual data, and the trade-off between privacy and authentication delays also contribute to the complexity of this problem.

5 Performance challenges in HetNets

HetNets integrate several access points and a variety of network technologies to improve coverage and capacity [136]. This represents a paradigm shift in wireless communication systems. Despite offering considerable advantages including increased spectral efficiency and better user experience, the implementation of HetNets presents several performance issues. These comprise problems with mobility management, resource allocation, interference control, and providing quality of service (QoS) across diverse network parts [137]. For HetNets to fulfil the ever-increasing needs for flawless connectivity and high-speed data services in contemporary wireless communications, these obstacles must be overcome.

5.1 Interference Management

HetNets have special requirements and characteristics, and therefore authentication presents a serious security risk [138]-[140]. Ensuring End-to-End (E2E) communication security is critical in the context of Large-Scale HetNets (LS-HetNets), as current research highlights problems such as identity privacy leakage and single points of failure [141]. HetNets pose a complex challenge in terms of securing access control and secure authentication across heterogeneous network parts like Wi-Fi access points, macro cells, small cells, and Internet of Things devices. The administration of user identities and access privileges is made more difficult by the possibility that multiple authentication procedures and protocols be used by each type of network element. Network compromises, illegal access, and data breaches can result from improperly configured access control settings or weak authentication procedures [142]-[146]. It is essential to integrate safe and easy authentication methods throughout HetNets to stop unwanted access attempts and safeguard private information sent over the network. Furthermore, HetNets' subset of vehicular networks has difficulties with authentication because of their great mobility and variety of security approaches. The dynamic structure, which causes devices to connect and disengage frequently as they travel between various network nodes, makes it more difficult to maintain continuous access control and authentication [147]. Since HetNets integrate several devices, interference results from multiple networks coexisting on the same frequencies and overlapping coverage areas. The user experience and overall network efficiency are ultimately jeopardized by this interference, which results in lower throughput, higher packet loss rates, and increased delay. We examine a co-channel HetNet deployment scenario, as seen in the figure below, where Q number of small cells, each consisting of a low power transmitter, are superimposed on a macro cell M with high power base station. It is expected that every base station and user equipment has Nt and Nr antennas configured, correspondingly. High cross-tier and co-tier interference coexist because all cells inside the macro cell coverage reuse the same frequency band and because cell coordination was not initially anticipated [148]. Figure 4 gives an illustration of interference in HetNets.

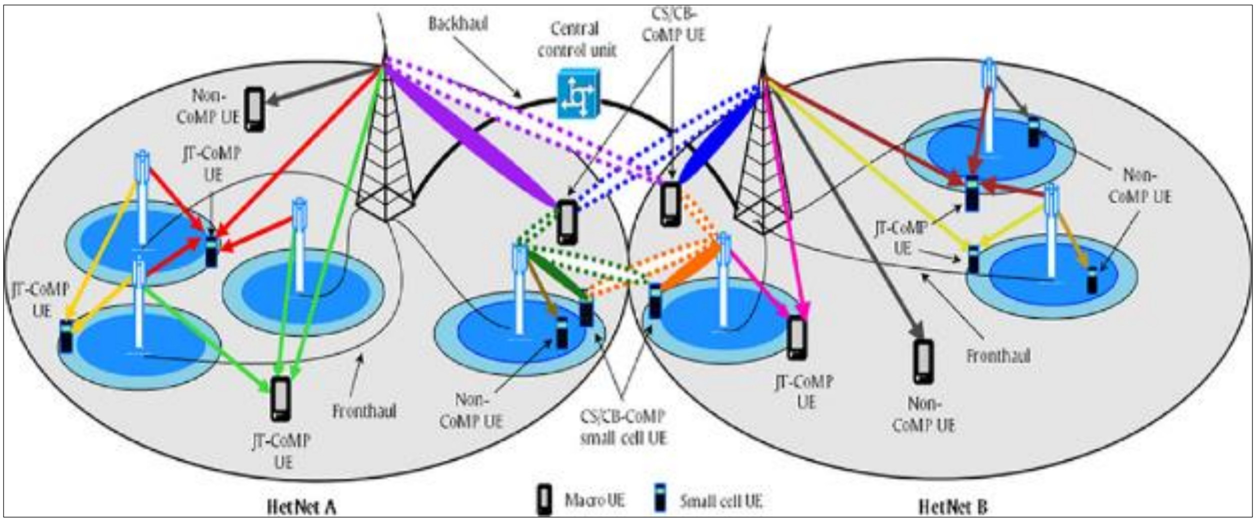

Figure 4 Interference in HetNets

The performance of HetNets is largely dependent on interference levels. Uplink transmission power control (PC) is crucial to reducing interference and improving system performance in 5G relay-based HetNets because interference from co-channel User Equipment (UEs) and Relay Nodes (RNs) can severely reduce the User Equipment (UE) signal [149], [150]. Furthermore, co-tier interference is introduced by the deployment of femtocells in HetNets, which affects the performance of different 5G applications.

5.2 Mobility Management

Because small cells are deployed in Heterogeneous Networks (HetNets), managing mobility presents a major challenge that necessitates effective mobility solutions and more handovers [151]. The different cell sizes and coverage areas in HetNets make handover and mobility management difficult. HetNets' mobility management can degrade performance [152] by complicating resource allocation, adding to signaling overhead, and generating disruptions during network handovers. Transitions between distinct network types, such as cellular to Wi-Fi, may result in poor connectivity and reduced service quality, whereas frequent mobility may put stress on network nodes and complicate general network administration. Efficient changeover techniques and protocols are necessary for seamless mobility between different cell types (such as switching from a macro cell to a small cell) to retain connectivity without experiencing service interruptions or quality deterioration [153]-[155]. HetNets have distinct mobility and connection problems from a variety of mobile user types, including pedestrians, vehicular users, and high-speed users. High-speed users may encounter a higher rate of Radio Link Failure (RLF) because of their rapid movement and the short amount of time the network has to create and sustain connections, whereas pedestrian users may suffer Handover Ping-Pong (HOPP) because of their slower speed. There are several reasons why an incorrect cell handover occurs in HetNets including insufficient signal strength, network congestion, interference from nearby cells, etc [156], [157]. Figure 5 below shows several mobile user types and associated difficulties in the context of a 5G HetNet.

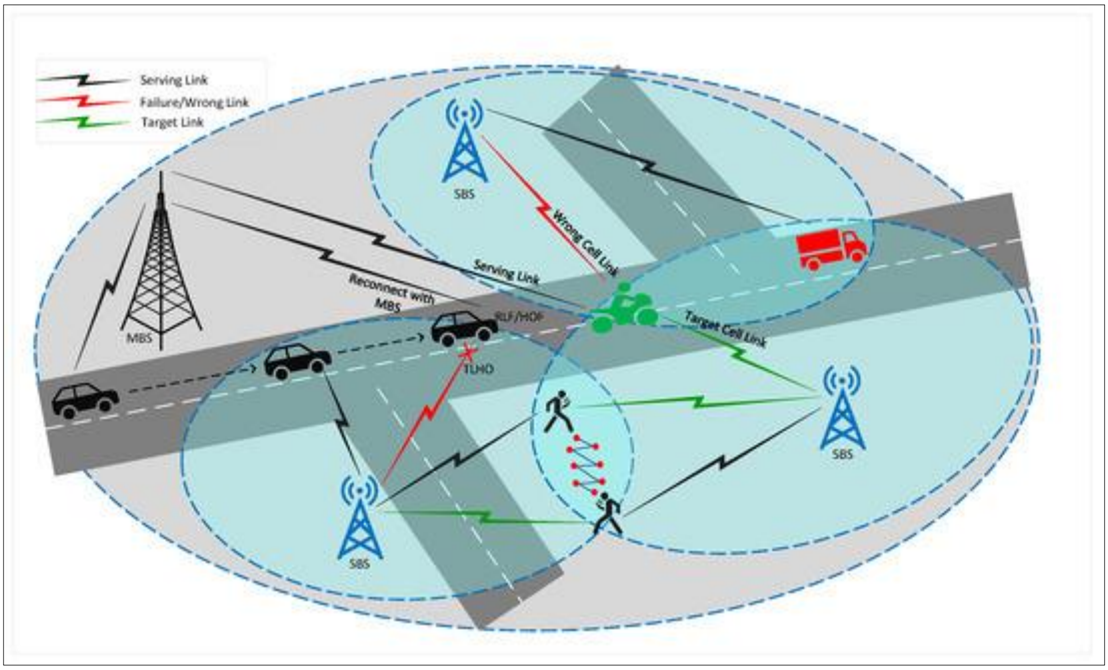

Figure 5 Mobility users and their related issues in a HetNet

5.3 Resource Allocation and Load Balancing

Resource Allocation [158] and Load Balancing: Because of the intricate interference scenarios and the growing number of base stations and users in HetNets, resource allocation, and load balancing provide substantial hurdles [159]. It is difficult to allocate resources (such as frequency spectrum, time slots, and transmit power) among different types of cells in an efficient manner to manage diverse and dynamic traffic loads. HetNets are designed to increase network capacity and support more users; however, this makes quality of service (QoS) challenging to achieve. Furthermore, resource allocation in high mobility networks is further complicated by the mobility feature, which renders standard optimization solvers unfeasible [160]-[163]. Insufficient resource distribution can result in underuse or congestion of network resources, which lowers service quality and creates inefficiencies. Similar to this, ineffective load balancing can cause an uneven traffic distribution, which can cause bottlenecks [164] and higher latency in specific network regions. Because they result in lost connections, sluggish speeds, and inconsistent performance throughout the heterogeneous network environment, these problems can have a substantial negative effect on user experience.

5.4 Heterogenous Deployment and Management

It is difficult to integrate different technologies and devices. Mobility and changeover problems impede the growing need for high-speed data transmission and low latency, while the swift expansion of data traffic and mobile devices demands dependable services during mobility [20], [165]. HetNet deployment and management require a variety of hardware, software, and settings for various cell types. It can be difficult to configure heterogeneous networks, effectively coordinate these components, and guarantee that different pieces of equipment and protocols work together [166].

5.5 Interoperability and Standards

There are many different types of devices, protocols, and systems in heterogeneous networks (HetNets), interoperability and standards which provide considerable issues. The variances in standard quality, implementation variances, and operational context variations are the sources of the complexity [167], [168]. Interoperability in the Internet of Things (IoT) space is further complicated by integrating sensors and devices with different standards and protocols from different vendors [169], [170].

6 Discussion

6.1 Current Solutions to Security Challenges in HetNets

Current solutions to security challenges in Heterogeneous Networks (HetNets) include advanced encryption protocols, multi-factor authentication, and network slicing. Encryption protocols such as AES and RSA ensure data confidentiality and integrity across diverse network components. Multi-factor authentication enhances access control by requiring multiple forms of verification, reducing the risk of unauthorized access. Network slicing isolates different network segments, allowing customized security measures for each slice and minimizing the impact of potential breaches. Additionally, machine learning algorithms are employed for real-time threat detection and mitigation, adapting to evolving security threats and ensuring robust protection for HetNets. In the following sub-sections, the current solutions to each of the issues in HetNets are described.

6.1.1 Interference

The authors in [171] proposes an approach that focuses on using estimated interference levels to inform the implementation of interference mitigation measures in HetNets. These tactics, which include the best pilot-based vector perturbation precoding, are meant to reduce interference as much as possible while maximizing network efficiency. This method shapes transmitted signals in wireless communication networks by using pilot signals and precoding, which lowers interference and improves signal quality at receivers. To optimize signal transmission based on estimated channel information, the procedure uses pilot signals for channel estimation and designs a precoding matrix (MMSE precoding matrix in multi-user systems). This method efficiently reduces interference from other signals or devices, increasing the total capacity of the system and the quality of the signals received by HetNets. By minimizing interference between cells and antennas through optimal signal shaping based on pilot signals and channel predictions, PB-VPP in HetNets enhances network performance. According to [172], PB-VPP facilitates dependable data transmissions that are essential for availability and confidentiality in HetNets, and this improves signal integrity. The effective use of resources by PB-VPP increases network resilience by reducing vulnerabilities and supporting protection against assaults such as jamming. When combined with strong security protocols, PB-VPP improves overall defenses against online threats and guarantees safe network operations in a variety of scenarios.

6.1.2 Virtual Resource Security

Resource management in virtual networks is essential, especially when it comes to preventing Distributed Denial-of-Service (DDoS) attacks. Load-balancing strategies are used in Software-Defined Networking (SDN) to efficiently counter DDoS attacks [173]-[176]. An optimization-driven approach to resource allocation is presented for 5G mobile networks to protect against malicious co-residency and defeat DDoS attacks to enhance security. This all-encompassing resource allocation architecture strengthens the network's overall security posture and preserves the integrity of the network, guaranteeing strong protection in virtualized environments [99]. Using a comprehensive approach, the VRA-RL secAwa framework tackles the problem of virtual resource security in HetNets [131]. To ensure that only authorized entities can use resources, it uses capability-based access control mechanisms to provide access to virtual resources based on assigned permissions, prohibiting unauthorized access. Based on network conditions and real-time security measurements, reinforcement learning (RL) optimization dynamically modifies resource allocation algorithms to maximize efficiency while reducing security concerns. By giving security requirements first priority when allocating resources, security-aware resource allocation reduces vulnerability to threats. The framework keeps an eye out for irregularities in the network environment and uses automated reactions to quickly neutralize threats that are detected. Network operators can share information and coordinate responses by collaborating on security management, and uniform policy enforcement across heterogeneous networks guarantees consistent security standards. By combining access control, dynamic optimization, threat detection, policy enforcement, and cooperative defensive mechanisms within HetNets, VRA-RL secAwa improves virtual resource security overall.

6.1.3 End-to-End Communication Security

Sec-E2E, a decentralized secure end-to-end communication architecture for LS-HetNets that makes use of blockchain technology, as proposed in [111]. Through the use of BAN-Logic, Scyther, and Tamarin-prover, their framework's security was assessed, and the satisfaction of crucial security properties such as mutual authentication, privacy preservation, session key secrecy, attack resistance, and forward/backward security was confirmed. To securely store and exchange security parameters for confirming anonymous UE certificates—which are essential for user equipment (UE) authentication at Secure Networks (SN) levels—Sec-E2E uses blockchain. The benefits of the blockchain include openness, minimal maintenance costs, tamper resistance, and the removal of single points of failure [177]-[182]. Sec-E2E is a consortium blockchain that is administered by nodes from various network domains. It enables global scalability and dependable information exchange across large geographic areas by allowing new nodes to join depending on authorization. The framework limits the percentage of bad miners to reduce the dangers of node compromise while adhering to consensus procedures such as Practical Byzantine Fault Tolerance (PBFT). Furthermore, implementing an off-chain storage system with smart contracts maximizes blockchain performance to successfully satisfy the needs of LS-HetNets.

6.1.4 Edge Security Risks

the development of the secure edge caching framework takes into consideration the layered aspects of multimedia; the essential base layer subfiles of the contents are given by the trustworthy MBS, while the enhancement layer subfiles are cached on the untrusted SBSs. Additionally, the edge caching problem of SBSs is formulated as a non-convex 0–1 integer programming problem based on the caching capacities of SBSs and the dynamic content needs of mobile users. The ADMM is used to find the best edge caching method for each SBS in order to fix the issue. The outcomes of the simulation demonstrate how well the suggested strategy reduces content transmission latency while safeguarding each piece of material's security. In subsequent research, we will examine the cooperative caching between mobile devices and SBSs.

6.2 **Current Solutions to Privacy Challenges in HetNets**

The current solutions to privacy challenges in Heterogeneous Networks (HetNets) include advanced data anonymization techniques, secure multi-party computation (SMPC), and robust privacy policies. Data anonymization ensures that personally identifiable information (PII) is obscured, protecting user identity while maintaining data utility for analytics. SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private, ensuring sensitive data is not exposed during processing. Implementing strict privacy policies and compliance with regulations like GDPR further safeguard user data. Additionally, differential privacy techniques are used to add noise to data, balancing the trade-off between data utility and privacy, ensuring that individual data cannot be easily re-identified in large datasets.

6.2.1 Insecure Access Points

To cache multimedia material for mobile users, numerous caching-enabled small-cell-based stations (SBSs) are deployed within the coverage of a macro-cell base station (MBS) in HetNets. However, because untrusted SBSs pose security risks, the proprietors of these SBSs may get unauthorized access to the cached material, compromising the privacy of its users. According to [120], by dividing content caching duties according to trust levels, the secure edge caching strategy solves security issues in heterogeneous networks. By letting untrusted small-cell base stations (SBSs) cache enhancement layer subfiles while trusted macro-cell base stations (MBS) handle crucial base layer subfiles of multimedia content directly, it protects the privacy and security of material. This division improves overall security by lowering the possibility that SBS owners may gain unwanted access to cached content. The plan uses a distributed alternate direction method of multipliers (ADMM) to optimize SBS caching algorithms, guaranteeing mobile users receive enhancement layer subfiles effectively and securely. Through efficient caching environment management in heterogeneous networks, the scheme reduces security risks related to untrusted SBSs and protects user privacy when accessing multimedia content.

6.2.2 Privacy Preservation in Handover Authentication

Using SDN and user capability integration, Cao suggested a unique handover authentication mechanism with user anonymity and traceability for 5G HetNets. The approach enables direct mutual authentication and key agreement between User Equipment (UE) and Base Stations (BS) in 5G HetNets without requiring communication with any other parties, greatly streamlining the authentication handover process. Security analysis techniques, such as the BAN logic and the formal verification tool Scyther have been used to show that the architecture can provide strong security. The outcomes of the performance analysis further demonstrate that the scheme's computational and communication costs are significantly lower than those of the conventional handover scheme and other comparable

According to [126], strong privacy features are offered by XAuth on heterogeneous networks (HetNets). By preserving the identity of User Equipment (UE) during authentication, it protects user privacy and guarantees anonymity for the user. Additionally, the protocol includes conditional privacy preservation, which permits information to be disclosed selectively in response to certain conditions. This ensures the required authentication while protecting user privacy. With forward secrecy, XAuth further improves privacy by guaranteeing that previous conversations are safe even if long-term keys are later compromised. It also provides backward secrecy, which safeguards session keys from the past and future in the event that a current session key is compromised, preserving the confidentiality of network interactions across time.

6.3 Current Solutions to Performance Challenges in HetNets

The existing solutions to performance challenges in heterogeneous networks include dynamic resource allocation, load balancing, and edge computing. Dynamic resource allocation optimizes the distribution of network resources based on real-time demand, ensuring efficient utilization and reducing bottlenecks. Load balancing techniques distribute traffic evenly across the network, preventing overload on any single node and enhancing overall performance. Edge computing brings data processing closer to the source of data generation, reducing latency and improving response times. Additionally, advanced interference management strategies and the use of software-defined networking (SDN) enable more flexible and adaptive network configurations, further enhancing the performance and reliability of HetNets.

6.3.1 Interference Management

Interference management in HetNets is crucial for maintaining network performance and reliability. Techniques such as interference coordination, power control, and spectrum allocation are employed to mitigate interference. Interference coordination, including coordinated multipoint transmission (CoMP) and enhanced inter-cell interference coordination (eICIC), allows cells to work together, reducing cross-cell interference. Power control dynamically adjusts the transmission power of devices to minimize interference while maintaining communication quality. Spectrum allocation strategies, such as dynamic spectrum access and cognitive radio, enable more efficient use of available frequencies, reducing the likelihood of interference. Additionally, advanced signal processing techniques and machine learning algorithms are increasingly used to predict and adapt to interference patterns, ensuring optimal network performance in diverse and dense environments typical of HetNets.

Spectrum Sharing (Load-Based Shared Spectrum Pool): Mobile Network Operators share spectrum, working together to use a shared pool of resources for their small and macro cell networks. To effectively manage their network resources and meet the growing demand for data services, operators share the available spectrum bands. Operators can increase network capacity, optimize resource allocation, and boost overall performance by sharing spectrum [183]-[185]. The shared spectrum pool is distributed using a load-based methodology, in which each operator's traffic load is taken into account while allocating resources. By coordinating the use of spectrum resources, spectrum sharing seeks to lessen interference across operators, improving user experiences and increasing average data speeds [186], [187]. Because spectrum sharing makes it possible to manipulate interference effectively and maximizes network performance [188], it is essential for interference control in heterogeneous networks (HetNets). Several spectrum-sharing algorithms have been developed by research to manage interference in next-generation networks, such as 6G [189], [190]. Furthermore, research has investigated joint multi-domain resource-aided interference management strategies, demonstrating enhanced throughput and decreased outage probability (Ding et al,) by employing beam and power domains to control co-frequency interference in satellite-ground integrated networks. Moreover, spectrum leasing becomes more advantageous when interference levels are higher, while spectrum sharing proves advantageous for higher data rates under lower interference conditions. Spectrum trading between Mobile Network Operators (MNOs) has also been studied in the context of 5G and beyond to reduce interoperator interference [191], [192].

Spectrum Leasing (Load-Based Leased Spectrum Pool): This method gives dedicated access to particular frequency bands for a predetermined amount of time by having one operator lease spectrum resources to the other [193]. The lessee can use the leased spectrum only for network operations under this arrangement, which gives the leasing operator dedicated access to specific frequency bands. The lease usually specifies details like the length of the lease, the spectrum bands that are allotted, and any associated expenses or fees. Operators can manage network resources more flexibly by renting spectrum, which allows them to meet short-term capacity or coverage demands without committing to anything long-term. With the help of spectrum leasing, operators may increase network efficiency [194], maximize their use of spectrum, and improve subscriber experience. Spectrum leasing is an essential technique for managing interference to improve both the overall performance of the network and spectrum efficiency [195], [196]. Numerous scholarly articles offer valuable perspectives on diverse methods of mitigating interference within these types of networks. In comparison to spectrum sharing, the use of spectrum leasing, as discussed in [197], can be useful in situations when there is greater levels of interference. Furthermore, research such as [4] suggests strategies for reusing spectrum that employ a Stackelberg game technique to lessen cross-tier interference, hence enhancing spectral efficiency in HetNets. According to [198], by lowering interference in primary networks, novel interference management strategies like interference alignment, can optimize spectrum allocation, hence improving network performance and utility.

6.3.2 Mobility Management

Mobility management in heterogeneous networks is essential for ensuring seamless connectivity and optimal performance as users move across different network cells. Key solutions include handover mechanisms, context-aware mobility management, and the use of software-defined networking (SDN). Handover mechanisms, such as hard and soft handovers, allow devices to switch between cells without interrupting ongoing connections. Context-aware mobility management leverages information about user location, speed, and network conditions to make more intelligent handover decisions. SDN enables centralized control of the network, allowing for dynamic and flexible management of mobility. Additionally, the integration of machine learning algorithms helps predict user movement patterns and preemptively adjust network resources, ensuring continuous and efficient connectivity in the heterogeneous and dynamic environments characteristic of HetNets.

Autonomous Mobility Management Control Approaches: HetNets' autonomous mobility management makes use of tile coding function approximation and reinforcement learning [199], [200]. This aims at minimizing needless handovers and failures, improving user equipment (UE) mobility robustness, and optimizing changeover control rules. Through interaction with the environment, the reinforcement learning framework develops the best handover control strategy on its own. When compared to deep Q-learning using neural networks, tile coding ensures higher convergence and computing efficiency [201] by handling the enormous state and action space efficiently. The strategy's key goals are to achieve almost zero handover failure rates, maintain high throughput, low latency, and lower operational expenses. Through sophisticated mobility management control, it establishes smooth communications between the UE and the base station. By integrating Device-to-Device (D2D) communication in HetNets using frameworks such as E-MIS-D2D, the D2D mobility experience is improved, the packet loss ratio is decreased, and the evolved Node B (eNB)'s average throughput, latency, bandwidth utilization, and load rate are all improved [202]. In addition, the integration of Multi-Access Edge Computing (MEC) technology and identity-location separation mechanisms into mobility management resolves problems with handover signal interactions, anchor points, and signaling overhead, leading to better performance than that of conventional cellular handover mechanisms [203]. To provide smooth communication during user mobility in HetNets, auto-tuning optimization techniques based on user speed and received signal reference power aid in lowering the frequency of handovers and handover failure ratios [204].

Context-aware Mobility Management Strategies: This entails leveraging inter-cell coordination and reinforcement learning techniques to enhance user equipment (UE) throughput and handover performance [205], [206]. To schedule user equipment based on their velocities and historical rates exchanged throughout tiers, macro and pico base stations cooperatively study their long-term traffic loads and ideal cell range expansion. To choose the best neighbor cells for handovers, the system takes into account variables including velocity, historical data, and traffic loads [207]. This guarantees smooth connections between the UE and the base station [208]. By resolving the issues raised by HetNets, this method improves small-cell network performance and fairness.

6.3.3 Resource Allocation and Load Balancing

Resource allocation and load balancing in heterogeneous networks are critical for optimizing network performance and ensuring equitable distribution of resources among diverse network elements. Dynamic resource allocation techniques adjust the distribution of bandwidth, power, and other resources based on real-time demand and network conditions, ensuring efficient utilization and minimizing congestion. Load balancing algorithms distribute network traffic evenly across various nodes and cells, preventing any single component from becoming overwhelmed. Techniques such as cell range expansion, carrier aggregation, and small cell deployment help manage load distribution effectively. Additionally, software-defined networking (SDN) and network function virtualization (NFV) provide centralized and programmable control over the network, enabling adaptive and scalable resource management. By balancing load and efficiently allocating resources, HetNets can maintain high performance and quality of service, even in densely populated and highly dynamic environments.

Dynamic Spectrum Management (DSM): This approach allows for the effective distribution and use of spectrum resources among various network technologies. To meet bandwidth demands, networks opportunistically access unused spectrum bands through dynamic spectrum access (DSA) [209]. Through Dynamic Spectrum Management, cognitive radio approaches enable networks to adaptively modify transmission parameters in response to current interference levels and spectrum availability. This increases overall network efficiency and lessens the impact of spectrum shortages [210].

Coordinated Multipoint (CoMP) transmission and Reception Technique: Through the coordination of transmissions and receptions across several base stations or access points, CoMP maximizes network capacity, improves coverage, and maximizes spectral efficiency [211], [212]. By enabling numerous cells to serve a user simultaneously, this technology lowers interference and guarantees flawless connectivity even when users travel between various network locations. CoMP approaches maximize resource consumption while preserving quality of service (QoS) [213] by dynamically allocating resources depending on real-time conditions, such as user location and network load [214].

Dynamic Load Balancing Techniques and Algorithms: With the help of these algorithms, traffic should be intelligently distributed among various cells or network technologies according to user requests and current network conditions [215], [216]. Through constant monitoring of variables including data traffic load, signal strength, and cell congestion, dynamic load balancing guarantees that users are assigned to the best available network resources [217]. This method reduces network congestion and boosts user data rates, which not only optimizes resource usage but also improves the overall quality of service.

Traffic Offloading Techniques: Traffic offloading techniques are crucial tactics for load balancing to maximize resource utilization and improve network performance [218], [219]. Among these methods is WiFi offloading, which uses WiFi's faster data rates to transfer mobile data traffic to WiFi networks when there are hotspots nearby, relieving cellular network congestion [220]. Small cell offloading is the process of increasing capacity and enhancing local service quality in crowded or underserved locations by placing femtocells and picocells. Using unlicensed spectrum resources such as LTE-U/LAA, dynamic spectrum offloading helps to relieve congestion on licensed bands while meeting the increasing demand for data [221].

6.3.4 Heterogenous Deployment and Management

Heterogeneous deployment and management in HetNets involve integrating various types of network nodes, such as macro cells, micro cells, pico cells, and femto cells, to provide seamless and efficient connectivity. This multi-layered network architecture aims to enhance coverage, capacity, and overall performance. Effective management requires advanced coordination and control mechanisms, including centralized and distributed approaches, to handle the complexity and diversity of the network elements. Techniques like self-organizing networks (SON) enable automated configuration, optimization, and healing of the network, reducing operational costs and enhancing reliability. Additionally, software-defined networking (SDN) and network function virtualization (NFV) offer flexible and scalable management solutions, allowing for dynamic adjustments and efficient resource utilization. By leveraging these technologies, HetNets can achieve robust, adaptive, and high-performing network environments that meet the demands of diverse applications and user scenarios.

Multi-Technology Coordination and Optimization: This involves putting into practice rules and algorithms that facilitate the effective coordination and optimization of various network technologies within HetNets [222], [223]. It comprises dynamic resource allocation techniques that modify frequency, power, and bandwidth usage for various technologies like WiFi, LTE, and tiny cells. Operators can maximize user experience and improve network efficiency by dynamically balancing resources and traffic [224], [225].

Self-Organizing Networks (SON): SON capabilities are being used to automate HetNet-wide network configuration, optimization, and healing procedures [226]-[228]. SON automatically monitors network performance, finds problems, and takes immediate corrective action using network intelligence and algorithms [229]. By doing this, operational overhead is decreased, network dependability is increased, and consistent service quality [230] is guaranteed across diverse deployments.

Cloud Radio Access Networks (Cloud-RAN): This entails leveraging and virtualizing network functions by utilizing Cloud-RAN designs and network function virtualization (NFV). By separating the baseband processing operations from the remote radio heads (RRHs), cloud-RAN enables centralized radio resource management and control across various network technologies [231]-[234]. NFV also makes it possible to virtualize network functions, which makes it easier to scale and deliver services across HetNets in a flexible manner [235]. This architecture facilitates the agile deployment of new services in diverse contexts while also enhancing resource consumption [236] and streamlining management.

6.3.5 Interoperability Standards Solutions

Interoperability standards solutions in heterogeneous networks are crucial for ensuring seamless communication and integration among diverse network elements and technologies. Standards such as 3GPP, IEEE, and IETF define protocols and interfaces that enable different network components—ranging from macro cells to small cells and various wireless technologies like Wi-Fi and LTE—to work together harmoniously. These standards facilitate compatibility and interoperability, ensuring devices and infrastructure from different vendors can communicate effectively. Interoperability is further enhanced through the use of software-defined networking (SDN) and network function virtualization (NFV), which provide a programmable and flexible framework for managing network resources and services. By adhering to these standards, HetNets can achieve unified operation, simplify network management, and support seamless user experiences across different network layers and technologies.

Agreements and Standardization Organizations: Interoperability standards are defined in large part by standards organizations like the Institute of Electrical and Electronics Engineers (IEEE) for WiFi and LAN standards and 3rd Generation Partnership Project (3GPP) for cellular networks [237]-[239]. They create and disseminate specifications that guarantee various network technologies can interact with one another in HetNets in an efficient manner [240]. Aligning implementations with these standards is facilitated by agreements and collaborations amongst various industry stakeholders, such as network operators, equipment manufacturers, and technology suppliers. This collaboration guarantees seamless device and network interoperability across many vendors.

Technological Solutions: Interworking gateways: These are hardware and software elements that help various network technologies communicate with one another. An interworking gateway, for instance, can facilitate a smooth transition between WiFi and cellular networks, guaranteeing continuous service when a user moves across coverage regions [241]. HetNet components can have dynamic resource [242] allocation and management like virtualization techniques and SDN concepts. This adaptability can improve interoperability by adjusting network configurations according to user needs and real-time situations [243].

7 Research gaps

Important research gaps have surfaced during this investigation, highlighting important chances for innovation in HetNets. The need for integrated frameworks that address security, privacy, and performance issues holistically has been identified as a major gap. The way these components are currently approached often leads to fragmented solutions that do not properly balance trade-offs or work in concert. An integrated framework would allow architects to create HetNets with all-encompassing protections and optimizations, guaranteeing that improvements in one area don't jeopardize other areas. Furthermore, HetNets' dynamic structure [244] poses a significant difficulty.

Because of the constant changes in user needs, environmental factors, and technology improvements, these networks require adaptive solutions that can be adjusted in real-time. This comprises self-optimizing settings [245], dynamic resource allocation [246], and proactive security measures [247] to foresee and thwart incoming threats. Collaboration amongst network engineering, data science, cybersecurity, and privacy advocacy [248] is necessary to achieve this adaptability and create flexible solutions that grow with HetNets. Closing these gaps would improve the security, privacy, and performance of HetNets while also promoting robust, effective networks that can easily accommodate a wide range of applications and user requirements. By giving integrated frameworks and adaptive solutions priority, we may further enhance the capabilities of HetNets and make a substantial contribution to the advancement of contemporary telecommunications infrastructure.

8 Future research scopes

The development of enhanced security measures specifically designed for HetNets is important due to the constantly changing landscape of cybersecurity threats. To proactively detect and neutralize new threats and weaknesses, proactive defensive tactics are essential. This entails putting strong encryption protocols [249] in place to secure data transmission across heterogeneous network elements, utilizing machine learning and artificial intelligence to detect anomalies in network behavior [250], and integrating threat intelligence frameworks to keep up with changing cyber threats.

When it comes to HetNets, where private and sensitive data is transferred between various network nodes and interfaces, protecting user privacy [251] while preserving service quality is critical. Strong privacy solutions ought to include privacy-enhancing technologies (PETs) including homomorphic encryption [252], anonymization, and differential privacy. These technologies support the anonymization of user data, restrict data gathering to what is required, and impose stringent access controls to stop illegal data breaches. Furthermore, maintaining legal obligations in data handling methods inside HetNets and fostering user trust depend on compliance with privacy legislation and standards (e.g., GDPR, CCPA) [253].

In the future, research on improved performance for dynamic HetNet systems should concentrate on creating novel methods for managing QoS and allocating resources. This entails investigating novel dynamic spectrum allocation algorithms, adaptive modulation methods, and sophisticated load balancing schemes that can instantly react to changing user demands and network conditions. Efficiency and customer experience will also be improved by incorporating machine learning techniques to forecast traffic trends and optimize network configurations. By putting an emphasis on network slicing technologies, operators will be able to adjust service settings and resource allocation to meet the demands of individual applications, guaranteeing reliable performance across a range of HetNet use cases.

9 Conclusion

HetNets, offer a variety of network topologies that combine many technologies to satisfy the increasing demands of contemporary connectivity. They represent a dynamic and expanding paradigm in the field of telecommunications. The basic features of HetNets have been covered in this manuscript, along with their architecture, and the numerous obstacles they must overcome. This study has examined the security, privacy, and performance opportunities and problems presented by heterogeneous networks (HetNets). According to the study, HetNets have inherent vulnerabilities because of their diverse network elements and interfaces. The solutions discussed in this article, while promising, have limits when it comes to their ability to adapt to changing threats and dynamic network conditions. The vast transmission of personal data within HetNets has raised serious privacy concerns, highlighting the need for more privacy-preserving methods. While network performance and user experience have improved, further innovations are needed to realize the full potential of these complex systems and their adoption must be accompanied by robust measures to address security, privacy, and performance concerns.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Solyman AA, Yahya K. Evolution of wireless communication networks: from 1G to 6G and future perspective. International journal of electrical and computer engineering. 2022 Aug 1;12(4):3943.

[2] Alsharif MH, Nordin R. Evolution towards fifth generation (5G) wireless networks: Current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. Telecommunication Systems. 2017 Apr;64:617-37.

[3] Salih AA, Zeebaree SR, Abdulraheem AS, Zebari RR, Sadeeq MA, Ahmed OM. Evolution of mobile wireless communication to 5G revolution. Technology Reports of Kansai University. 2020 Jun;62(5):2139-51.

[4] Aldmour I. Wireless broadband tools and their evolution towards 5G networks. Wireless Personal Communications. 2017 Aug;95(4):4185-210.

[5] Adebusola JA, Ariyo AA, Elisha OA, Olubunmi AM, Julius OO. An overview of 5G technology. In2020 international conference in mathematics, computer engineering and computer science (ICMCECS) 2020 Mar 18 (pp. 1-4). IEEE.

[6] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[7] Alotaibi S. HetNet Characteristics and Models in 5G Networks. International Journal of Computer Science & Network Security. 2022;22(4):27-32.

[8] Alhammadi A, Ismail ZH, Shayea I, Shamsan ZA, Alsagabi M, Al-Sowayan S, Saad SA, Alnakhli M. SOMNet: Self-Optimizing mobility management for resilient 5G heterogeneous networks. Engineering Science and Technology, an International Journal. 2024 Apr 1;52:101671.

[9] Vujicic Z, Santos MC, Méndez R, Klaiqi B, Rodriguez J, Gelabert X, Rahman MA, Gaudino R. Towards Virtualized Optical-Wireless Heterogeneous Networks. IEEE access. 2024 Jun 20.

[10] Tashan W, Shayea I, Aldirmaz-Colak S, El-Saleh AA, Arslan H. Optimal handover optimization in future mobile heterogeneous network using integrated weighted and fuzzy logic models. IEEE Access. 2024 Apr 18.

[11] Urooj S, Arunachalam R, Alawad MA, Tripathi KN, Sukumaran D, Ilango P. An effective model for network selection and resource allocation in 5G heterogeneous network using hybrid heuristic-assisted multi-objective function. Expert Systems with Applications. 2024 Aug 15;248:123307.

[12] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[13] Gures E, Shayea I, Alhammadi A, Ergen M, Mohamad H. A comprehensive survey on mobility management in 5G heterogeneous networks: Architectures, challenges and solutions. IEEE Access. 2020 Oct 13;8:195883-913.

[14] Alruhaili T, Aldabbagh G. A Survey on Het-Nets: Challenges and Solutions for Enhanced Capacity and Energy Efficiency. Solid State Technology. 2020 Jul 30;63(1):1556-69.

[15] Wani AR, Gupta SK, Khanam Z, Rashid M, Alshamrani SS, Baz M. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. IET Intelligent Transport Systems. 2023 Nov;17(11):2171-89.

[16] Sharma A, Balasubramanian V, Jolfaei A. Security challenges and solutions for 5G HetNet. In2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) 2020 Dec 29 (pp. 1318-1323). IEEE.

[17] Singh PK, Singh R, Nandi SK, Ghafoor KZ, Nandi S. Seamless v2i communication in hetnet: State-of-the-art and future research directions. Connected vehicles in the internet of things: Concepts, technologies and frameworks for the IoV. 2020:37-83.

[18] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[19] Rashid A, Sharma D, Lone TA, Gupta S, Gupta SK. Secure communication in UAV assisted HetNets: a proposed model. InSecurity, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS 2019, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12 2019 (pp. 427-440). Springer International Publishing.

[20] Rehman AU, Roslee MB, Jun Jiat T. A survey of handover management in mobile HetNets: current challenges and future directions. Applied Sciences. 2023 Mar 6;13(5):3367.

[21] Sultan J, Mohsen MS, Al-Thobhani NS, Jabbar WA. Performance of hard handover in 5G heterogeneous networks. In2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA) 2021 Aug 10 (pp. 1-7). IEEE.

[22] Sönmez Ş, Shayea I, Khan SA, Alhammadi A. Handover management for next-generation wireless networks: A brief overview. 2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW). 2020 Oct 1;1:35-40.

[23] Khan SA, Shayea I, Ergen M, El-Saleh AA, Roslee M. An improved handover decision algorithm for 5G heterogeneous networks. In2021 IEEE 15th Malaysia International Conference on Communication (MICC) 2021 Dec 1 (pp. 25-30). IEEE.

[24] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[25] Nam YH, Ng BL, Han J, Zhang J. Evolution of HetNet Technologies in LTE-Advanced Standards. Heterogeneous Cellular Networks. 2013 May 17:287-311.

[26] Ahmad WS, Radzi NA, Samidi FS, Ismail A, Abdullah F, Jamaludin MZ, Zakaria M. 5G technology: Towards dynamic spectrum sharing using cognitive radio networks. IEEE access. 2020 Jan 13;8:14460-88.

[27] Sundan AP, Jha RK, Gupta A. Energy and spectral efficiency optimization using probabilistic based spectrum slicing (PBSS) in different zones of 5G wireless communication network. Telecommunication Systems. 2020 Jan;73(1):59-73.

[28] Nadeem L, Amin Y, Loo J, Azam MA, Chai KK. Efficient resource allocation using distributed edge computing in D2D based 5G-HCN with network slicing. IEEE Access. 2021 Sep 22;9:134148-62.

[29] Agarwal B, Togou MA, Marco M, Muntean GM. A comprehensive survey on radio resource management in 5G HetNets: Current solutions, future trends and open issues. IEEE Communications Surveys & Tutorials. 2022 Sep 20;24(4):2495-534.

[30] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[31] Zheng J, Gao L, Wang H, Li X, Xu P, Wang L, Jiang B, Yang X. Joint downlink and uplink edge computing offloading in ultra-dense HetNets. Mobile Networks and Applications. 2019 Oct;24:1452-60.

[32] Bennis M, Simsek M, Czylwik A, Saad W, Valentin S, Debbah M. When cellular meets WiFi in wireless small cell networks. IEEE communications magazine. 2013 Jun 10;51(6):44-50.

[33] Sun Y, Han J. Mining heterogeneous information networks: a structural analysis approach. ACM SIGKDD explorations newsletter. 2013 Apr 30;14(2):20-8.

[34] Balachandran M, Vali Mohamad NM. Joint power optimization and scaled beamforming approach in B5G network based massive MIMO enabled HetNet with full-duplex small cells. Peer-to-Peer Networking and Applications. 2021 Jan;14:333-48.

[35] Faruk N, Abdulkarim A, Surajudeen-Bakinde NT, Popoola SI. Energy efficiency of backhauling options for future heterogeneous networks. Advances on Computational Intelligence in Energy: The Applications of Nature-Inspired Metaheuristic Algorithms in Energy. 2019:169-94.

[36] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[37] Mahbub M, Shubair RM. Contemporary advances in multi-access edge computing: A survey of fundamentals, architecture, technologies, deployment cases, security, challenges, and directions. Journal of Network and Computer Applications. 2023 Aug 26:103726.

[38] Xu Y, Gui G, Gacanin H, Adachi F. A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges. IEEE Communications Surveys & Tutorials. 2021 Feb 17;23(2):668-95.

[39] Ejaz W, Sharma SK, Saadat S, Naeem M, Anpalagan A, Chughtai NA. A comprehensive survey on resource allocation for CRAN in 5G and beyond networks. Journal of Network and Computer Applications. 2020 Jun 15;160:102638.

[40] Alhumaima RS, Khan M, Al-Raweshidy HS. Component and parameterised power model for cloud radio access network. IET Communications. 2016 May;10(7):745-52.

[41] Ranjbar M, Tran N, Karacolak T, Pham KD. On the Energy Efficiency and Spectral Efficiency Trade-Off of Multi-User Full-Duplex Cognitive Radio Networks under Imperfect Spectrum Sensing. InAIAA SCITECH 2024 Forum 2024 (p. 1736).

[42] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[43] Esmat HH, Elmesalawy MM, Abdelhakam MM, Elhattab MK. Joint radio resource and power allocation using Nash bargaining game for H-CRAN with nonideal fronthaul links. Transactions on Emerging Telecommunications Technologies. 2018 Sep;29(9):e3449.

[44] Zhang J, Yan Z, Fei S, Wang M, Li T, Wang H. Is Today's End-to-End Communication Security Enough for 5G and Its Beyond?. IEEE Network. 2021 Oct 18;36(1):105-12.

[45] Yaqoob M, Gemikonakli O, Ever E. Modelling heterogeneous future wireless cellular networks: An analytical study for interaction of 5G femtocells and macro-cells. Future Generation Computer Systems. 2021 Jan 1;114:82-95.

[46] Simsek M, Bennis M, Guvenc I. Mobility management in HetNets: a learning-based perspective. EURASIP Journal on Wireless Communications and Networking. 2015 Dec;2015:1-3.

[47] Wang YC, Lee S. Small-cell planning in LTE HetNet to improve energy efficiency. International Journal of Communication Systems. 2018 Mar 25;31(5):e3492.

[48] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[49] Merwaday A, Güvenç I. Optimisation of FeICIC for energy efficiency and spectrum efficiency in LTE-advanced HetNets. Electronics Letters. 2016 May;52(11):982-4.

[50] Jon JH, Jong C, Ryu KS, Kim W. Enhanced uplink handover scheme for improvement of energy efficiency and QoS in LTE-A/5G HetNet with ultra-dense small cells. Wireless Networks. 2024 Apr;30(3):1321-38.

[51] Ever E, Al-Turjman FM, Zahmatkesh H, Riza M. Modelling green HetNets in dynamic ultra large-scale applications: A case-study for femtocells in smart-cities. Computer Networks. 2017 Dec 9;128:78-93.

[52] Noohani MZ, Magsi KU. A review of 5G technology: Architecture, security and wide applications. International Research Journal of Engineering and Technology (IRJET). 2020 May;7(05):3440-71.

[53] Bhosle AS. Emerging trends in small-cell technology. In2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE) 2017 Apr 27 (pp. 1-4). IEEE.

[54] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[55] Ghosh A, Cottatellucci L, Altman E. Nash equilibrium for femto-cell power allocation in HetNets with channel uncertainty. In2015 IEEE Global Communications Conference (GLOBECOM) 2015 Dec 6 (pp. 1-7). IEEE.

[56] Sambanthan P, Muthu T. Role of Femtocell Networks beyond 4G. In2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA) 2018 Jul 6 (pp. 1-5). IEEE.

[57] Molisch AF, Tufvesson F. Propagation channel models for next-generation wireless communications systems. IEICE Transactions on Communications. 2014 Oct 1;97(10):2022-34.

[58] Al-omari MS, Alomari MA, Ramli AR, Sali A, Azmir RS, Yusoff MH. Effects of femtocell ultradense deployment on downlink performance in LTE heterogeneous networks. Wireless Communications and Mobile Computing. 2021;2021(1):2735935.

[59] Bayazeed A, Khorzom K, Aljnidi M. A survey of self-coordination in self-organizing network. Computer networks. 2021 Sep 4;196:108222.

[60] Zinno S, Di Stasi G, Avallone S, Ventre G. On a fair coexistence of LTE and Wi-Fi in the unlicensed spectrum: A Survey. computer communications. 2018 Jan 1;115:35-50.

[61] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[62] Rao SP, Bakas A. Authenticating Mobile Users to Public Internet Commodity Services Using SIM Technology. InProceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks 2023 May 29 (pp. 151-162).

[63] Fall M, Balboul Y, Fattah M, Mazer S, El Bekkali M, Kora AD. Towards sustainable 5G networks: A proposed coordination solution for macro and pico cells to optimize energy efficiency. IEEE Access. 2023 May 19;11:50794-804.

[64] Al-Turjman F, Ever E, Zahmatkesh H. Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview. IEEE Communications Surveys & Tutorials. 2018 Aug 10;21(1):28-65.

[65] Zhu Y, Zhang Z, Marzi Z, Nelson C, Madhow U, Zhao BY, Zheng H. Demystifying 60GHz outdoor picocells. InProceedings of the 20th annual international conference on Mobile computing and networking 2014 Sep 7 (pp. 5-16).

[66] Georlette V, Moeyaert V, Bette S, Point N. Outdoor optical wireless communication: potentials, standardization and challenges for Smart Cities. In2020 29th wireless and optical communications conference (WOCC) 2020 May 1 (pp. 1-6). IEEE.

[67] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[68] Soh YS, Quek TQ, Kountouris M, Shin H. Energy efficient heterogeneous cellular networks. IEEE Journal on selected areas in communications. 2013 Apr 16;31(5):840-50.

[69] Haneda K, Zhang J, Tan L, Liu G, Zheng Y, Asplund H, Li J, Wang Y, Steer D, Li C, Balercia T. 5G 3GPP-like channel models for outdoor urban microcellular and macrocellular environments. In2016 IEEE 83rd vehicular technology conference (VTC spring) 2016 May 15 (pp. 1-7). IEEE.

[70] Hossain MI, Alzarrad MA, Wolfe K, Miah S. Small-Cell Installation in Transportation Infrastructure—A Literature Review. FHWA-ICT-20-003. 2020.

[71] Ismaiil KA, Assaf B, Ghantous M, Nahas M. Reducing power consumption of cellular networks by using various cell types and cell zooming. InThe Third International Conference on e-Technologies and Networks for Development (ICeND2014) 2014 Apr 29 (pp. 33-38). IEEE.

[72] López-Pérez D, Ding M, Claussen H, Jafari AH. Towards 1 Gbps/UE in cellular systems: Understanding ultra-dense small cell deployments. IEEE Communications Surveys & Tutorials. 2015 Jun 17;17(4):2078-101.

[73] Yunas SF, Valkama M, Niemelä J. Spectral and energy efficiency of ultra-dense networks under different deployment strategies. IEEE Communications Magazine. 2015 Jan 16;53(1):90-100.

[74] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[75] Himayat N, Yeh SP, Panah AY, Talwar S, Gerasimenko M, Andreev S, Koucheryavy Y. Multi-radio heterogeneous networks: Architectures and performance. In2014 International Conference on Computing, Networking and Communications (ICNC) 2014 Feb 3 (pp. 252-258). IEEE.

[76] Ghatak G, De Domenico A, Coupechoux M. Coverage analysis and load balancing in HetNets with millimeter wave multi-RAT small cells. IEEE Transactions on Wireless Communications. 2018 Feb 26;17(5):3154-69.

[77] Xiao Z, Zhu L, Liu Y, Yi P, Zhang R, Xia XG, Schober R. A survey on millimeter-wave beamforming enabled UAV communications and networking. IEEE Communications Surveys & Tutorials. 2021 Nov 2;24(1):557-610.

[78] Paul ES, Browne W, Mendl MT, Caplen G, Trevarthen A, Held S, Nicol CJ. Assessing animal welfare: a triangulation of preference, judgement bias and other candidate welfare indicators. Animal Behaviour. 2022 Apr 1;186:151-77.

[79] Aboagye S, Saeidi MA, Tabassum H, Tayyar Y, Hossain E, Yang HC, Alouini MS. Multi-band wireless communication networks: Fundamentals, challenges, and resource allocation. IEEE Transactions on Communications. 2024 Feb 16.

[80] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[81] Marvi M, Aijaz A, Khurram M. Toward a Unified Framework for Analysis of Multi-RAT Heterogeneous Wireless Networks. Wireless Communications and Mobile Computing. 2019;2019(1):6918637.

[82] Vahid S, Tafazolli R, Filo M. Small cells for 5G mobile networks. Fundamentals of 5G Mobile Networks. 2015 May 8:63-104.

[83] Yang Y, Li Y, Li K, Zhao S, Chen R, Wang J, Ci S. DECCO: Deep-learning enabled coverage and capacity optimization for massive MIMO systems. IEEE Access. 2018 Apr 20;6:23361-71.

[84] Chen Z, Li H, Cui G, Rangaswamy M. Adaptive transmit and receive beamforming for interference mitigation. IEEE Signal Processing Letters. 2014 Jan 9;21(2):235-9.

[85] Feng B, Zhou H, Zhang H, Li G, Li H, Yu S, Chao HC. HetNet: A flexible architecture for heterogeneous satellite-terrestrial networks. IEEE network. 2017 Sep 11;31(6):86-92.

[86] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[87] Chaieb C, Mlika Z, Abdelkefi F, Ajib W. On the optimization of user association and resource allocation in HetNets with mm-wave base stations. IEEE Systems Journal. 2020 Jun 16;14(3):3957-67.

[88] Ali M, Mumtaz S, Qaisar S, Naeem M. Smart heterogeneous networks: a 5G paradigm. Telecommunication Systems. 2017 Oct;66:311-30.

[89] Shi D, Lü L, Chen G. Totally homogeneous networks. National science review. 2019 Sep;6(5):962-9.

[90] Khan AF, Nanda P. Hybrid blockchain-based Authentication Handover and Flow Rule Validation for Secure Software Defined 5G HetNets. In2022 International Wireless Communications and Mobile Computing (IWCMC) 2022 May 30 (pp. 223-230). IEEE.

[91] Palanisamy P. Downlink Intercell Interference Behavior in Heterogeneous Networks. In2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) 2023 Apr 5 (pp. 1-8). IEEE.

[92] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[93] Marabissi D, Fantacci R, Marabissi D, Fantacci R. Heterogeneous networks. Cognitive Interference Management in Heterogeneous Networks. 2015:3-16.

[94] Palanisamy P. Downlink Intercell Interference Behavior in Heterogeneous Networks. In2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) 2023 Apr 5 (pp. 1-8). IEEE.

[95] Iqbal MU, Ansari EA, Akhtar S. Interference mitigation in HetNets to improve the QoS using Q-learning. IEEE Access. 2021 Feb 19;9:32405-24.

[96] Fang D, Qian Y, Hu RQ. Security analysis for interference management in heterogeneous networks. Ad Hoc Networks. 2019 Mar 1;84:1-8.

[97] Cao J, Ma M, Fu Y, Li H, Zhang Y. CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets. IEEE transactions on dependable and secure computing. 2019 May 14;18(3):1182-95.

[98] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[99] Sattar D. Mitigating Security Problems in Virtualized Networks Through Resource Management (Doctoral dissertation, Carleton University).

[100] Ghelani D, Maral V, Mehetre DC. Efficient network security virtualization scheme. InInnovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017 2019 (pp. 51-58). Springer Singapore.

[101] Bazm MM, Lacoste M, Südholt M, Menaud JM. Side-channels beyond the cloud edge: New isolation threats and solutions. In2017 1st Cyber Security in Networking Conference (CSNet) 2017 Oct 18 (pp. 1-8). IEEE.

[102] Yang C, Guo Y, Hu H, Liu W, Wang Y. An effective and scalable VM migration strategy to mitigate cross-VM side-channel attacks in cloud. China Communications. 2019 Apr 22;16(4):151-71.

[103] Ometov A, Levina A, Borisenko P, Mostovoy R, Orsino A, Andreev S. Mobile social networking under side-channel attacks: Practical security challenges. IEEE Access. 2017 Feb 17;5:2591-601.

[104] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[105] Cao H, Wu S, Hu Y, Tian F, Yang L. Secure virtual resource allocation in heterogeneous networks for intelligent transportation. In2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) 2020 May 25 (pp. 1-5). IEEE.

[106] Firoozjaei MD, Jeong JP, Ko H, Kim H. Security challenges with network functions virtualization. Future Generation Computer Systems. 2017 Feb 1;67:315-24.

[107] Dui H, Zhang H, Dong X, Zhang S. Cascading failure and resilience optimization of unmanned vehicle distribution networks in IoT. Reliability Engineering & System Safety. 2024 Jun 1;246:110071.

[108] Artime O, Grassia M, De Domenico M, Gleeson JP, Makse HA, Mangioni G, Perc M, Radicchi F. Robustness and resilience of complex networks. Nature Reviews Physics. 2024 Feb;6(2):114-31.

[109] Weedage L, Magalhães SR, Stegehuis C, Bayhan S. On the resilience of cellular networks: how can national roaming help?. IEEE Transactions on Network and Service Management. 2024 Jan 10.

[110] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[111] Fei S, Yan Z, Xie H, Liu G. Sec-E2E: End-to-End Communication Security in LS-HetNets Based on Blockchain. IEEE Transactions on Network Science and Engineering. 2023 Aug 23.

[112] Sheron PF, Sridhar KP, Baskar S, Shakeel PM. A decentralized scalable security framework for end-to-end authentication of future IoT communication. Transactions on Emerging Telecommunications Technologies. 2020 Dec;31(12):e3815.

[113] Fadlullah ZM, Mao B, Kato N. Balancing QoS and security in the edge: Existing practices, challenges, and 6G opportunities with machine learning. IEEE Communications Surveys & Tutorials. 2022 Jul 18;24(4):2419-48.

[114] Haus M, Waqas M, Ding AY, Li Y, Tarkoma S, Ott J. Security and privacy in device-to-device (D2D) communication: A review. IEEE Communications Surveys & Tutorials. 2017 Jan 9;19(2):1054-79.

[115] Hu W, Chang CH, Sengupta A, Bhunia S, Kastner R, Li H. An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2020 Dec 29;40(6):1010-38.

[116] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[117] Pham QV, Fang F, Ha VN, Piran MJ, Le M, Le LB, Hwang WJ, Ding Z. A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. IEEE access. 2020 Jun 10;8:116974-7017.

[118] Zhao Y, Wang W, Li Y, Meixner CC, Tornatore M, Zhang J. Edge computing and networking: A survey on infrastructures and applications. IEEE Access. 2019 Jul 9;7:101213-30.

[119] Yang R, Yu FR, Si P, Yang Z, Zhang Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials. 2019 Jan 23;21(2):1508-32.

[120] Xu Q, Su Z, Wang Y, Zhang K. Secure edge caching for layered multimedia contents in heterogeneous networks. In2019 IEEE Global Communications Conference (GLOBECOM) 2019 Dec 9 (pp. 1-6). IEEE.

[121] Wang Y, Su Z, Ni J, Zhang N, Shen X. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. IEEE Communications Surveys & Tutorials. 2021 Dec 1;24(1):160-209.

[122] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[123] Ryu JW, Pham QV, Luan HN, Hwang WJ, Kim JD, Lee JT. Multi-access edge computing empowered heterogeneous networks: A novel architecture and potential works. Symmetry. 2019 Jul 1;11(7):842.

[124] Wang B, Chen W, Wang J, Zhang B, Zhang Z, Qiu X. Cooperative tracking control of multiagent systems: A heterogeneous coupling network and intermittent communication framework. IEEE transactions on cybernetics. 2018 Aug 26;49(12):4308-20.

[125] Wijesinghe KI, Lokuliyana S. Addressing IoT Security and Privacy Challenges. In2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) 2023 Jul 24 (pp. 2303-2307). IEEE.

[126] Wang M, Zhao D, Yan Z, Wang H, Li T. XAuth: Secure and privacy-preserving cross-domain handover authentication for 5G HetNets. IEEE Internet of Things Journal. 2022 Nov 18;10(7):5962-76.

[127] Qiu T, Chen N, Li K, Qiao D, Fu Z. Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks. 2017 Feb 1;55:143-52.

[128] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[129] Mishra N, Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access. 2021 Apr 15;9:59353-77.

[130] Bansal G, Chamola V. Lightweight authentication protocol for inter base station communication in heterogeneous networks. InIEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2020 Jul 6 (pp. 871-876). IEEE.

[131] Cao H, Aujla GS, Garg S, Kaddoum G, Yang L. Embedding security awareness for virtual resource allocation in 5g hetnets using reinforcement learning. IEEE Communications Standards Magazine. 2021 Jun 25;5(2):20-7.

[132] Zhang Y, Deng RH, Bertino E, Zheng D. Robust and universal seamless handover authentication in 5G HetNets. IEEE Transactions on Dependable and Secure Computing. 2019 Jul 9;18(2):858-74.

[133] Li K, Cui Q, Zhu Z, Ni W, Tao X. Lightweight, privacy-preserving handover authentication for integrated terrestrial-satellite networks. InICC 2022-IEEE International Conference on Communications 2022 May 16 (pp. 25-31). IEEE.

[134] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[135] Ozhelvaci A, Ma M. A group authentication scheme with privacy-preserving for D2D communications in 5G HetNets. InProceedings of the 2nd International Electronics Communication Conference 2020 Jul 8 (pp. 170-175).

[136] Andrews JG, Singh S, Ye Q, Lin X, Dhillon HS. An overview of load balancing in HetNets: Old myths and open problems. IEEE Wireless Communications. 2014 Apr;21(2):18-25.

[137] Qi W. A Study about Heterogeneous Network Issues Management based on Enhanced Inter-cell Interference Coordination and Machine Learning Algorithms (Doctoral dissertation, University of Sheffield).

[138] Lone TA, Rashid A, Gupta S, Gupta SK, Rao DS, Najim M, Srivastava A, Kumar A, Umrao LS, Singhal A. Securing communication by attribute-based authentication in HetNet used for medical applications. EURASIP Journal on Wireless Communications and Networking. 2020 Dec;2020:1-21.

[139] Duan X, Wang X. Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer. In2016 IEEE International Conference on Communications (ICC) 2016 May 22 (pp. 1-6). IEEE.

[140] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[141] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[142] Khan A, Ahmad A, Ahmed M, Sessa J, Anisetti M. Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems. 2022 Oct;8(5):3919-41.

[143] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications. 2011 Jan 1;34(1):1-1.

[144] Marali M, Sudarsan SD, Gogioneni A. Cyber security threats in industrial control systems and protection. In2019 International Conference on Advances in Computing and Communication Engineering (ICACCE) 2019 Apr 4 (pp. 1-7). IEEE.

[145] Rao PM, Deebak BD. A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks. 2023 Jul 1;146:103159.

[146] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[147] Ozhelvaci A, Ma M. Secure and efficient vertical handover authentication for 5G HetNets. In2018 IEEE international conference on information communication and signal processing (ICICSP) 2018 Sep 28 (pp. 27-32). IEEE.

[148] Gulia S, Ahmad A, Singh S, Gupta MD. Interference management in backhaul constrained 5G HetNets through coordinated multipoint. Computers and Electrical Engineering. 2022 May 1;100:107982.

[149] Sun K, Wu J, Huang W, Zhang H, Hsieh HY, Leung VC. Uplink performance improvement for downlink-uplink decoupled HetNets with non-uniform user distribution. IEEE Transactions on Vehicular Technology. 2020 May 11;69(7):7518-30.

[150] Siddiqui MU, Qamar F, Ahmed F, Nguyen QN, Hassan R. Interference management in 5G and beyond network: Requirements, challenges and future directions. IEEE Access. 2021 Apr 15;9:68932-65.

[151] Ullah Y, Roslee MB, Mitani SM, Khan SA, Jusoh MH. A survey on handover and mobility management in 5G HetNets: current state, challenges, and future directions. Sensors. 2023 May 25;23(11):5081.

[152] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[153] Saad WK, Shayea I, Hamza BJ, Azizan A, Ergen M, Alhammadi A. Performance evaluation of mobility robustness optimization (MRO) in 5G network with various mobility speed scenarios. IEEE Access. 2022 May 9;10:60955-71.

[154] Abdah H, Barraca JP, Aguiar RL. QoS-aware service continuity in the virtualized edge. IEEE Access. 2019 Apr 17;7:51570-88.

[155] Deng H, Peng C, Fida A, Meng J, Hu YC. Mobility support in cellular networks: A measurement study on its configurations and implications. InProceedings of the Internet Measurement Conference 2018 2018 Oct 31 (pp. 147-160).

[156] Khan SA, Shayea I, Ergen M, Mohamad H. Handover management over dual connectivity in 5G technology with future ultra-dense mobile heterogeneous networks: A review. Engineering Science and Technology, an International Journal. 2022 Nov 1;35:101172.

[157] Alotaibi S. Key challenges of mobility management and handover process In 5G HetNets. International Journal of Computer Science & Network Security. 2022;22(4):139-46.

[158] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[159] Chen Z, Wang F, Zhu X, Zhang Y, Yu G, Liu Y. Deep reinforce learning and meta-learning based resource allocation in cellular heterogeneous networks. In2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI) 2023 May 26 (pp. 378-383). IEEE.

[160] Wang L, Jiao L, Li J, Gedeon J, Mühlhäuser M. MOERA: Mobility-agnostic online resource allocation for edge computing. IEEE Transactions on Mobile Computing. 2018 Aug 28;18(8):1843-56.

[161] Shi Y, Lian L, Shi Y, Wang Z, Zhou Y, Fu L, Bai L, Zhang J, Zhang W. Machine learning for large-scale optimization in 6g wireless networks. IEEE Communications Surveys & Tutorials. 2023 Aug 1.

[162] Lai P, He Q, Cui G, Chen F, Grundy J, Abdelrazek M, Hosking J, Yang Y. Cost-effective user allocation in 5G NOMA-based mobile edge computing systems. IEEE Transactions on Mobile Computing. 2021 May 4;21(12):4263-78.

[163] Knopp S, Biesinger B, Prandtstetter M. Mobility offer allocations in corporate settings. EURO Journal on Computational Optimization. 2021 Jan 1;9:100010.

[164] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[165] Paiva S, Ahad MA, Tripathi G, Feroz N, Casalino G. Enabling technologies for urban smart mobility: Recent trends, opportunities and challenges. Sensors. 2021 Mar 18;21(6):2143.

[166] Hamdi R, Said AB, Baccour E, Erbad A, Mohamed A, Hamdi M, Guizani M. Optimal resource management for hierarchical federated learning over HetNets with wireless energy transfer. IEEE Internet of Things Journal. 2023 May 1;10(19):16945-58.

[167] Stamou A, Dimitriou N, Kontovasilis K, Papavassiliou S. Context-aware handover management for HetNets: Performance evaluation models and comparative assessment of alternative context acquisition strategies. Computer Networks. 2020 Jul 20;176:107272.

[168] Ibrahim M, Hashmi US, Nabeel M, Imran A, Ekin S. Embracing complexity: Agent-based modeling for HetNets design and optimization via concurrent reinforcement learning algorithms. IEEE Transactions on Network and Service Management. 2021 Oct 19;18(4):4042-62.

[169] Popp L, Schaller M. Towards IoT Standards Interoperability: A Tool-Assisted Approach. InInnovation Through Information Systems: Volume I: A Collection of Latest Research on Domain Issues 2021 (pp. 514-518). Springer International Publishing.

[170] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[171] Alruwaili O, Logeshwaran J, Natarajan Y, Alrowaily MA, Patel SK, Armghan A. Incremental RBF-based cross-tier interference mitigation for resource-constrained dense IoT networks in 5G communication system. Heliyon. 2024 Jun 12.

[172] Omri T, Bouallegue R. Multi-RAT integration in Heterogeneous Vehicular Communication Networks (HVCNets). In2023 International Wireless Communications and Mobile Computing (IWCMC) 2023 Jun 19 (pp. 751-756). IEEE.

[173] Belgaum MR, Musa S, Alam MM, Su'ud MM. A systematic review of load balancing techniques in software-defined networking. IEEE Access. 2020 May 20;8:98612-36.

[174] ZHANG Y, Hongwei DI. Security in Software-Defined Networks Against Denial-of-Service Attacks Based on Increased Load Balancing Efficiency. International Journal of Advanced Computer Science & Applications. 2023 Nov 1;14(11).

[175] Hamdan M, Hassan E, Abdelaziz A, Elhigazi A, Mohammed B, Khan S, Vasilakos AV, Marsono MN. A comprehensive survey of load balancing techniques in software-defined network. Journal of Network and Computer Applications. 2021 Jan 15;174:102856.

[176] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[177] Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022 Nov 21;14(11):341.

[178] Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, Alazab M. Blockchain for industry 4.0: A comprehensive review. Ieee Access. 2020 Apr 17;8:79764-800.

[179] Upadhyay N. Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management. 2020 Oct 1;54:102120.

[180] Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. International journal of web and grid services. 2018;14(4):352-75.

[181] Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A survey on the adoption of blockchain in iot: Challenges and solutions. Blockchain: Research and Applications. 2021 Jun 1;2(2):100006.

[182] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[183] Jorswieck EA, Badia L, Fahldieck T, Karipidis E, Luo J. Spectrum sharing improves the network efficiency for cellular operators. IEEE Communications Magazine. 2014 Mar 14;52(3):129-36.

[184] Yu R, Ding J, Huang X, Zhou MT, Gjessing S, Zhang Y. Optimal resource sharing in 5G-enabled vehicular networks: A matrix game approach. IEEE Transactions on Vehicular Technology. 2016 Mar 1;65(10):7844-56.

[185] Zhang H, Jiang C, Beaulieu NC, Chu X, Wen X, Tao M. Resource allocation in spectrum-sharing OFDMA femtocells with heterogeneous services. IEEE Transactions on Communications. 2014 Jun 4;62(7):2366-77.

[186] Tehrani RH, Vahid S, Triantafyllopoulou D, Lee H, Moessner K. Licensed spectrum sharing schemes for mobile operators: A survey and outlook. IEEE Communications Surveys & Tutorials. 2016 Jun 27;18(4):2591-623.

[187] Sharma SK, Bogale TE, Le LB, Chatzinotas S, Wang X, Ottersten B. Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges. IEEE Communications Surveys & Tutorials. 2017 Nov 15;20(1):674-707.

[188] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[189] Yang P, Kong L, Chen G. Spectrum sharing for 5G/6G URLLC: Research frontiers and standards. IEEE communications standards magazine. 2021 Apr 20;5(2):120-5.

[190] Qamar F, Siddiqui MU, Hindia MN, Hassan R, Nguyen QN. Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks. Electronics. 2020 Sep 1;9(9):1416.

[191] Saha RK. On exploiting millimeter-wave spectrum trading in countrywide mobile network operators for high spectral and energy efficiencies in 5G/6G era. Sensors. 2020 Jun 20;20(12):3495.

[192] Jeon J, Ford RD, Ratnam VV, Cho J, Zhang J. Coordinated dynamic spectrum sharing for 5G and beyond cellular networks. IEEE Access. 2019 Aug 9;7:111592-604.

[193] Khurshid HA, Aziz Bhatti F, Mehmood K, Jangsher S, Habib A. Traffic Load-Based Spectrum Trading between Two Mobile Network Operators in HetNets Using Interference Management Technique. Wireless Communications and Mobile Computing. 2022;2022(1):4080110.

[194] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[195] Gavili A, ShahbazPanahi S. Optimal spectrum leasing and resource sharing in two-way relay networks. IEEE Transactions on Signal Processing. 2014 Jul 15;62(19):5030-45.

[196] Bastami AH. NOMA-based spectrum leasing in cognitive radio network: Power optimization and performance analysis. IEEE Transactions on Communications. 2021 Mar 30;69(7):4821-31.

[197] Han K, Liu D, Chen Y, Chai KK. Spectrum reuse scheme in two-tier HetNets: A Stackelberg game approach. In2015 IEEE International Conference on Computer and Communications (ICCC) 2015 Oct 10 (pp. 404-409). IEEE.

[198] Nair GR, Moorthy YK, Pillai SS. A novel interference reduction technique in game theory based dynamic spectrum leasing scheme. In2016 International Conference on Emerging Technological Trends (ICETT) 2016 Oct 21 (pp. 1-8). IEEE.

[199] Liu Q, Kwong CF, Zhou S, Ye T, Li L, Ardakani SP. Autonomous mobility management for 5G ultra-dense HetNets via reinforcement learning with tile coding function approximation. IEEE Access. 2021 Jul 8;9:97942-52.

[200] Lee Y, Masood A, Noh W, Cho S. DQN based user association control in hierarchical mobile edge computing systems for mobile IoT services. Future Generation Computer Systems. 2022 Dec 1;137:53-69.

[201] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[202] Xu YH, Liu ML, Xie JW, Zhou J. Media independent mobility management for D2D communications over heterogeneous networks (HetNets). Wireless Personal Communications. 2021 Oct;120(4):2693-710.

[203] Zhang L, Niu J, Wang Y, Chen G, Gu T, Li Y. Energy-efficient task offloading in RIS-aided HetNets with wireless backhaul. IEEE Communications Letters. 2023 Jul 27.

[204] Saad WK, Shayea I, Hamza BJ, Mohamad H, Daradkeh YI, Jabbar WA. Handover parameters optimisation techniques in 5G networks. Sensors. 2021 Jul 31;21(15):5202.

[205] Mukhtar M, Yunus F, Alqahtani A, Arif M, Brezulianu A, Geman O. The Challenges and Compatibility of Mobility Management Solutions for Future Networks. Applied Sciences. 2022 Nov 15;12(22):11605.

[206] Hapanchak VS, Costa A, Pereira J, Nicolau MJ. An intelligent path management in heterogeneous vehicular networks. Vehicular Communications. 2024 Feb 1;45:100690.

[207] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Ma J, Honi DG, Aldarwish AJ, Abduljaleel IQ. Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes. Applied Sciences. 2022 Dec 11;12(24):12688.

[208] Niasar FA, Aghdam MJ, Nabipour M, Momen A. Mobility management in HetNets consider on QOS and improve Throughput. In2021 IEEE 11th annual computing and communication workshop and conference (CCWC) 2021 Jan 27 (pp. 1354-1359). IEEE.

[209] Gayatri T, Sharma VK, Anveshkumar N. A survey on conceptualization of cognitive radio and dynamic spectrum access for next generation wireless communications. Journal of Applied Science and Computations (JASC). 2019 Feb;6(2):744-51.

[210] Yilmazel R, Inanç N. A novel approach for channel allocation in OFDM based cognitive radio technology. Wireless Personal Communications. 2021 Sep;120(1):307-21.

[211] Irram F, Ali M, Maqbool Z, Qamar F, Rodrigues JJ. Coordinated multi-point transmission in 5G and beyond heterogeneous networks. In2020 IEEE 23rd international multitopic conference (INMIC) 2020 Nov 5 (pp. 1-6). IEEE.

[212] Qamar F, Dimyati KB, Hindia MN, Noordin KA, Al-Samman AM. A comprehensive review on coordinated multi-point operation for LTE-A. Computer Networks. 2017 Aug 4;123:19-37.

[213] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[214] Zhao J, Yang L, Xia M, Motani M. Unified analysis of coordinated multipoint transmissions in mmWave cellular networks. IEEE Internet of Things Journal. 2021 Dec 9;9(14):12166-80.

[215] Kanellopoulos D, Sharma VK. Dynamic load balancing techniques in the IoT: A review. Symmetry. 2022 Dec 2;14(12):2554.

[216] Shafiq DA, Jhanjhi NZ, Abdullah A. Load balancing techniques in cloud computing environment: A review. Journal of King Saud University-Computer and Information Sciences. 2022 Jul 1;34(7):3910-33.

[217] Castro-Hernandez D, Paranjape R. Dynamic analysis of load balancing algorithms in LTE/LTE-A HetNets. Wireless Personal Communications. 2017 Oct;96:3297-315.

[218] Zhang J, Guo H, Liu J, Zhang Y. Task offloading in vehicular edge computing networks: A load-balancing solution. IEEE Transactions on Vehicular Technology. 2019 Dec 12;69(2):2092-104.

[219] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[220] Gu B, Wei Y, Liu X, Song M, Han Z. Traffic offloading and power allocation for green HetNets using reinforcement learning method. In2019 IEEE Global Communications Conference (GLOBECOM) 2019 Dec 9 (pp. 1-6). IEEE.

[221] Moubayed A, Ahmed T, Haque A, Shami A. Machine learning towards enabling spectrum-as-a-service dynamic sharing. In2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) 2020 Aug 30 (pp. 1-6). IEEE.

[222] Alhammadi A, Roslee M, Alias MY, Shayea I, Alriah S, Abas AB. Advanced handover self-optimization approach for 4G/5G HetNets using weighted fuzzy logic control. In2019 15th international conference on telecommunications (ConTEL) 2019 Jul 3 (pp. 1-6). IEEE.

[223] Li Y, Zhang Y, Luo K, Jiang T, Li Z, Peng W. Ultra-dense hetnets meet big data: Green frameworks, techniques, and approaches. IEEE Communications Magazine. 2018 Jun 18;56(6):56-63.

[224] Zhao X, Cao Y, Chen H, Huang Z, Wang D. Multi-objective resource allocation based on deep reinforcement learning in hetnets. In2022 IEEE 8th International Conference on Computer and Communications (ICCC) 2022 Dec 9 (pp. 574-578). IEEE.

[225] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[226] Darwish T, Kurt GK, Yanikomeroglu H, Senarath G, Zhu P. A vision of self-evolving network management for future intelligent vertical HetNet. IEEE Wireless Communications. 2021 Aug;28(4):96-105.

[227] Li Z, Yu P, Li W, Qiu X. Modeling and optimization of self-organizing energy-saving mechanism for HetNets. InNOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium 2016 Apr 25 (pp. 146-152). IEEE.

[228] Ebrahimzadeh A, Maier M. Cooperative computation offloading in FiWi enhanced 4G HetNets using self-organizing MEC. IEEE Transactions on Wireless Communications. 2020 Apr 6;19(7):4480-93.

[229] Mabrouk MB, Garandeau JP, Tabani T, Gateau M. A Self Organizing OneM2M IoT Network. In2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR) 2021 Jun 7 (pp. 1-7). IEEE.

[230] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[231] Wang J, Ma X, Chen Z, Zheng L, Xie W, Wang X. Secrecy Wireless Information and Power Transfer in Ultra-Dense Cloud Radio Access Networks. IEEE Transactions on Wireless Communications. 2024 Feb 6.

[232] Shin C, Park SH, Kim J, Park H. Cloud Radio Random-Access Networks with Multi-Packet Reception Capability. IEEE Access. 2024 Jun 26.

[233] Alhumaima RS, Al-Raweshidy HS. Evaluating the energy efficiency of software defined-based cloud radio access networks. IET communications. 2016 May;10(8):987-94.

[234] Azariah W, Bimo FA, Lin CW, Cheng RG, Nikaein N, Jana R. A survey on open radio access networks: Challenges, research directions, and open source approaches. Sensors. 2024 Feb 5;24(3):1038.

[235] Makhanbet M, Zhang X, Gao H, Suraweera HA. An overview of cloud RAN: Architecture, issues and future directions. InEmerging Trends in Electrical, Electronic and Communications Engineering: Proceedings of the First International Conference on Electrical, Electronic and Communications Engineering (ELECOM 2016), Bagatelle, Mauritius, November 25-27, 2016 2017 (pp. 44-60). Springer International Publishing.

[236] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[237] Raghunandan K. Wireless Standards and National Licenses. InIntroduction to Wireless Communications and Networks: A Practical Perspective 2022 Apr 1 (pp. 75-93). Cham: Springer International Publishing.

[238] Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, Ladid L. Internet of things in the 5G era: Enablers, architecture, and business models. IEEE journal on selected areas in communications. 2016 Feb 3;34(3):510-27.

[239] Lee E, Seo YD, Oh SR, Kim YG. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials. 2021 Mar 19;23(2):1020-47.

[240] Saha C, Afshang M, Dhillon HS. 3GPP-inspired HetNet model using Poisson cluster process: Sum-product functionals and downlink coverage. IEEE Transactions on Communications. 2017 Dec 12;66(5):2219-34.

[241] Narmadha R, Anitha U. Authentication Analysis in HETNETS: Interworking Performance. Wireless Personal Communications. 2023 Mar;129(2):1229-48.

[242] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[243] Rong B, Qiu X, Kadoch M, Sun S, Li W, Rong B, Qiu X, Kadoch M, Sun S, Li W. Intelligent SDN and NFV for 5G HetNet dynamics. 5G Heterogeneous Networks: Self-organizing and Optimization. 2016:15-40.

[244] Farajzadeh A, Khoshkholgh MG, Yanikomeroglu H, Ercetin O. Self-evolving integrated vertical heterogeneous networks. IEEE Open Journal of the Communications Society. 2023 Feb 9;4:552-80.

[245] Alhammadi A, Hassan WH, El-Saleh AA, Shayea I, Mohamad H, Saad WK. Intelligent coordinated self-optimizing handover scheme for 4G/5G heterogeneous networks. ICT Express. 2023 Apr 1;9(2):276-81.

[246] Moazeni A, Khorsand R, Ramezanpour M. Dynamic resource allocation using an adaptive multi-objective teaching-learning based optimization algorithm in cloud. IEEE Access. 2023 Feb 22;11:23407-19.

[247] Almahmoud Z, Yoo PD, Alhussein O, Farhat I, Damiani E. A holistic and proactive approach to forecasting cyber threats. Scientific Reports. 2023 May 17;13(1):8049.

[248] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[249] Nelakuditi NC, Namburi NK, Sayyad J, Rudraraju DV, Govindan R, Rao PV. Secure File Operations: Using Advanced Encryption Standard for Strong Data Protection. International Journal of Safety & Security Engineering. 2024 Jun 1;14(3).

[250] Rabbani M, Wang Y, Khoshkangini R, Jelodar H, Zhao R, Bagheri Baba Ahmadi S, Ayobi S. A review on machine learning approaches for network malicious behavior detection in emerging technologies. Entropy. 2021 Apr 25;23(5):529.

[251] Mohammed T, Albeshri A, Katib I, Mehmood R. UbiPriSEQ—Deep reinforcement learning to manage privacy, security, energy, and QoS in 5G IoT hetnets. Applied Sciences. 2020 Oct 13;10(20):7120.

[252] Su G, Wang J, Xu X, Wang Y, Wang C. The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology. 2024 Mar 13;2(1):52-8.

[253] Chukwurah EG. Agile privacy in practice: integrating CCPA and GDPR within agile frameworks in the US tech scene. International Journal of Scientific Research Updates. 2024;7(2):024-36.